

A Complete Bibliography of Publications in the *Journal of Computer Security*

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148

E-mail: =beebe@math.utah.edu=, =beebe@acm.org=, =beebe@computer.org= (Internet)
WWW URL: =http://www.math.utah.edu/beebe/=

14 October 2017
Version 1.04

Title word cross-reference

₂ [QJ97]. *k* [LWZZ15]. Ω [RFLW96]. π [SV03].

-jump [LWZZ15].

5PM [BEM⁺13].

9798 [BCM13].

Abadi [MW04]. **Abelian** [MS05a, MS05b]. **abstract**
[GM10, GTZ04, MMHS13, PG09]. **abstractions** [CDF⁺08]. **Accelerated**
[Elb08]. **access**
[AJS12, AHB08, ASL96, ACDS08, ACK⁺10, AR12, BBFR00, BDP10, BS02,
BGS06, Bro02, DFP⁺13, HSR08, HTS00, HPS03, KNS08, LKAJ16, LCL⁺15,
RW97, SAsC11, TR11, TL07, UAV⁺14, VAGL09, YGSY15, YSD13, ZRG08].
Accountable [BBS⁺15, BLL02]. **Achieving** [AJB93, HH09]. **Action** [Sin97].

active [BPS08, KGA03]. **activity** [TC16]. **Ad** [ZSXJ06, AJS12, RCBM07, RH07, ZDM07]. **Ad-Hoc** [ZSXJ06, AJS12]. **adaptation** [Bis12]. **adaptive** [KB11]. **Address** [XC09, PSJ⁺13]. **Address-space** [XC09]. **Adjoining** [GM10]. **administration** [SB99, YGSY15]. **administrative** [AR12, VAGL09, YGSY15]. **Advances** [Vis13]. **AES** [Elb08]. **against** [BCFK15, HSR08, LHM⁺10, PV05, RCBM07, SPS⁺14]. **agenda** [Pri06]. **agent** [DB11]. **agents** [BR04]. **Aggregating** [HZO⁺13]. **Aggregation** [Fol92, CPPS07]. **agreement** [PQ03, PQ06]. **ahead** [SM05]. **aid** [BS04]. **aided** [NTU11]. **algebra** [RS01]. **algebraic** [ABG04, CDL06]. **Algebras** [FG95, BCLM05]. **Algorithm** [AJJ95, HDC95]. **algorithms** [AGHP14, LWZZ15, MM96, SAE⁺05]. **Aligning** [BBK14]. **Allocation** [Mii93b]. **Amongst** [CGM95]. **analyses** [Pau01]. **Analysing** [KL11, Low04a]. **Analysis** [HDC95, Mea92, NS06, Syv92, Wra92, ABG04, AS15, AR12, AH00b, BBDLM14, BBI15, BCLM05, BDGS16, BR05b, BHC04, CFL13, CDL⁺05, CYC17, CHM07, CS05, CEHM07, CS13, CW17, DKS10, DMV15, ES06, GEL98, GTZ04, JKK10, KM10, KK16, LOS16, LT17, LLA15, Low98, Mea01, MSC04, MS05a, MS05b, MVB10, PV05, RS02, RTWH11, Shm04, SBP01, SKEG14, TR11, UC07, UAV⁺14, VVB⁺09, VIS96, WYSJ08, War05, YGSY15, ZZW⁺11, BDP05]. **Analytic** [MM96]. **analyzed** [TvdRO03]. **Analyzer** [MSC04]. **Analyzing** [CAFL10, CCP⁺17, Weh07, ABK⁺11]. **Android** [CLD⁺17, JAH⁺16, MMF15]. **announced** [CGLZ03]. **Anomaly** [SAE⁺05, LWWJ02, VVB⁺09]. **anomaly-based** [VVB⁺09]. **Anonymity** [BMS95, HO05, CMS97, HS04, LS02, PSJ⁺13, Shm04]. **anonymity-revoking** [CMS97]. **anonymization** [DRRW11, SVA11]. **Anonymizing** [ACM15, PS14]. **anonymous** [SBS05]. **answers** [BH09]. **Antigone** [MP06]. **APIs** [HBS16]. **applets** [BCG⁺02]. **application** [BHC04, NZS05, QJ97, VC05]. **Applications** [GG92, BHSV14, BLL02, CZ16, DB11, DT97, GEL98, JKK10, KTV12]. **applied** [DKR10]. **Applying** [BFGS08, BFGS09, Mea92]. **Approach** [BY95, WL93, ABG04, ALP11, BBFR00, BFM05, BFO05, CLD⁺17, CDF⁺12, FF11, HS04, KSS13, MS03, Pau98, SBP01]. **approaches** [BDG⁺10]. **Approximate** [DHW04, NG08]. **Architecture** [AXR12, TS93, ABFK03, DPV09, HTS00, MM96, dACD⁺16]. **architectures** [LLA15]. **area** [AFHS09]. **argument** [LZ13]. **ARM** [GNDB16]. **aspects** [CMP14]. **assessment** [BT06, Mal10, SSBW12]. **assignment** [SB99]. **assignments** [VAGL09]. **association** [VC05]. **associations** [DFJ⁺15]. **Assurance** [BMBS10, EMO⁺93, CT09]. **asymmetric** [GJ04]. **Asynchronous** [Yah93]. **Athena** [SBP01]. **ATM** [Chu96]. **attack** [EVK02, HZO⁺13, Kre13, NG08, OMSH04, WYSJ08]. **attackers** [RCBM07]. **Attacking** [CS13]. **attacks** [BPS08, BBDLM14, BWA10, BR04, BCFK15, CS05, DPV09, DS99, Han11, HLS03, HNS⁺14, KB11, LHM⁺10, Low04a, M0105, OMSH04, PQ03, PV05, SPS⁺14, SVSM07, VVB⁺09, ZGDS13].

attempt [Mat98]. **attribute** [LCL⁺15, PTMW10]. **attribute-based** [LCL⁺15, PTMW10]. **attribution** [TC16]. **auction** [DDL15]. **audio** [SKEG14]. **audit** [DS99]. **Auditable** [FM98]. **augmented** [SZP⁺12]. **Authentic** [DGMS03]. **authenticated** [PQ03, PQ06]. **Authentication** [CGM95, GLP93, Gut04b, HP00, NR11, QJ97, TA92, ATI⁺10, BCM13, BCL97, BSSM⁺07, BFM07, DGK⁺04, DMV15, GTY08, GTZ04, HSH11, HCM11, JHS96, MvO11, SKEG14]. **Authenticity** [GJ03]. **Author** [Ano92a, Ano93, Ano95a, Ano96a, Ano97, Ano98, Ano01, Ano02, Ano03, Ano04, Ano05, Ano06, Ano07a, Ano08, Ano09, Ano10, Ano11, Ano12, Ano13, Ano14, Ano15a, Ano16]. **authorities** [MG08]. **Authorization** [BOS95, DS97, DFJ⁺11, Kar00, WL93, AH00b, BBDLM14, BBK14, BFG10, BBFS00, CCF98, GP12, MP06, SWC07]. **authorizations** [CDF97]. **authors** [Ano96b]. **Automated** [BHSV14, CDF97, KK16, AR12, CDE⁺10, SHM02, ZGD04]. **Automatic** [Bla09, RTWH11, UC07, SBP01, ZF12]. **Automatically** [KB11, dSRCP17]. **Automating** [Gue09]. **autoregressive** [NG08]. **availability** [BW08]. **aware** [ACDS08, BDGS16, RS16]. **awareness** [MSas13].

ballot [CS13]. **bandwidth** [DMM04, NR11]. **based** [AJS12, AHB08, ATI⁺10, AR12, AH00b, AHB00, BGJ03, BBI15, BBFR00, BY95, BFO05, BGS06, CG06, CMMV07, CFL13, CWT14, CLK04, CCP⁺17, DHRS11, DR16, DPV09, DLYZ11, Dug04, ES06, EVK02, GMR⁺11, GGS⁺09, HTS00, HSH11, KR03, KNS08, KTV12, LS02, LHM⁺10, LCL⁺15, LT17, LKWB06, LSMR16, MMHS13, Mea01, MMF15, MVB10, NR11, NTU11, PTMW10, PGK14, PG09, RS02, RAJ98, RW97, SB99, SVA11, ST05, SKEG14, TR11, UAV⁺14, VAGL09, VPZ16, VK99, VVB⁺09, WWJ04, WLJW07, WD08, WMF⁺17, YGSY15, YSD13, vOT11, NZS05]. **bases** [BF99, BBFS00]. **Basic** [Jac92]. **batch** [AGHP14]. **Bayes** [CPP08]. **Beacons** [JHS96]. **been** [GLZ11]. **Behavior** [YSD13, RTWH11, WDDN00]. **Behavior-based** [YSD13]. **Belief** [Syv92]. **beliefs** [CMS09]. **Bell** [Mil96]. **between** [CDL⁺05, Pau01]. **BGV** [GHPS13]. **BGV-style** [GHPS13]. **bi** [CGKW17]. **bi-objective** [CGKW17]. **bilinear** [KM10]. **Biometric** [ATI⁺10]. **biometrics** [BSSM⁺07]. **bisimulation** [DKR10]. **Black** [MSas13]. **Black-box** [MSas13]. **Blind** [ABO06, BFPV13]. **boots** [MS96]. **bounded** [DLMS04, TBEB08]. **bounding** [ABK⁺11, BMV15, YT11]. **bounds** [KB11]. **box** [MSas13, SV03]. **Brandt** [DDL15]. **breaches** [CGLZ03, GLZ11]. **Broadcast** [BMS95]. **browser** [ABR13, BCFK15]. **browsers** [BCL97]. **browsing** [SRG97]. **BRSIM** [BPS08]. **BRSIM/UC** [BPS08]. **BRSIM/UC-soundness** [BPS08]. **buffer** [ZZW⁺11]. **building** [PQ06]. **business** [BBK14].

C [DGJN14]. **CA** [BVC⁺14]. **calculus** [AACP13, BGS06, DKR10, HM10, MS96]. **Calibrating** [HM10]. **Call** [Ano92b, Ano95b]. **calls** [HFS98]. **Can** [KNTU13, BBS⁺15]. **capability**

[MG08]. **capable** [TEML08]. **CAPTCHA** [SKEG14]. **CAPTCHA-based** [SKEG14]. **CAPTCHAs** [MGS⁺17]. **capture** [SST08]. **card** [Bel03, BCG⁺02]. **Cardinality** [WWJ04, VC05]. **Cardinality-based** [WWJ04]. **cards** [SRS⁺02]. **Cascade** [HCH⁺93, BFO05, DPV09]. **case** [GP12]. **cases** [ABHS09]. **Casper** [Low98]. **causal** [dC96]. **causality** [SV03]. **CCA1** [MSas13]. **cellular** [HCM11, TEML08]. **centers** [CDE⁺10]. **centric** [RW97]. **centricity** [BSCGS07]. **Certificate** [CEE⁺01, HTML09, BLL02, CAB10, LHM⁺10, WLM01, WLM02]. **certificate-based** [LHM⁺10]. **Certificates** [TA92, LKWB06]. **certified** [NZS05]. **chain** [CEE⁺01, LWM03]. **challenge** [TC16]. **change** [HJT⁺96]. **channel** [KSWH00, KB11]. **Channels** [BMS95, Hu92, Wra92, DMV15, GT17, NR11]. **check** [ST15, T̄BEB08]. **checked** [MCB13]. **checkers** [RB99]. **Checking** [BCG⁺02, BDP05, BJLT01, DHRS11, DR16, JR04, Low99, ZRG08]. **checks** [DFJ⁺16]. **checksum** [BGJ03]. **checksum-based** [BGJ03]. **Chinese** [ACM04]. **ciphers** [KSWH00]. **ciphertxts** [NMP⁺13]. **circuit** [CMTB16]. **Classification** [FG95, BFGS08, BFGS09]. **classified** [GM10]. **click** [vOT11]. **click-based** [vOT11]. **Cliques** [PQ06]. **Cliques-type** [PQ06]. **cloud** [ABR13, CWT14, DFJ⁺16, LT17, ST15, ZGDS13]. **cloud-based** [CWT14]. **cloud1** [YY15]. **code** [PG09, SV03, WS02, XC09]. **codes** [ATI⁺10, SVSM07]. **coercion** [KTV12]. **cognitive** [MGS⁺17]. **collaboration** [AJS12]. **Collaborative** [FJ95, SZP⁺12]. **collection** [BF99]. **collective** [CCBE13]. **colluding** [RCBM07]. **combined** [VVB⁺09]. **combiners** [Her09]. **Commerce** [ABO06, BKA⁺97]. **Communication** [Vis13, JAH⁺16, LSMR16, SBS05, Xu07]. **communications** [DMM10]. **community** [CYC17]. **comparative** [IBS03, NR11, SAE⁺05]. **comparing** [TL07]. **comparison** [CDL⁺05, MM96]. **compiled** [WS02]. **compiler** [CDF⁺08, Low98, LSMR16, ZZW⁺11]. **complete** [T̄BEB08]. **Completeness** [MW04, ABHS09, Low99]. **complex** [TC16]. **complexity** [DLMS04, OMSH04]. **Composability** [ZL95, BU16]. **composition** [BDF09, CDM12, SV03]. **Compositional** [BPR07, DDMP05, DMP03]. **compression** [Weh07]. **computation** [BA12]. **Computational** [BU10, BWA10, RDDM10, War05]. **Computationally** [KM10, CB15, LZ13]. **Computer** [Ano92b, BR09, FJ95, LBF⁺93, BS04, HSR08, Mat98, SVSM07]. **computers** [MvO11]. **computing** [ABR13, SV15, ZGDS13]. **concrete** [BBDLM14]. **Concurrency** [AJJ95, DFP⁺13]. **concurrent** [BN07, BPR07, VS99]. **conditional** [Hal17]. **confidentiality** [CDF⁺12, NSH14]. **configuration** [FF11, RS02]. **configurations** [UC07]. **Configuring** [AFHS09]. **confinement** [LJM00]. **Conspiracy** [Bis96]. **constant** [YY15]. **constant-cost** [YY15]. **constrained** [DMV15]. **Constraint** [AHB08, MVB10, BFO05]. **constraint-based** [BFO05, MVB10]. **constraints** [CCF98, CDF⁺12]. **construction** [HLVA11, MCB13, MSas13]. **Constructions** [LHM⁺10, CGKO11]. **constructs** [Mal10]. **consumption** [MMF15]. **contactless** [Sin11]. **Content** [DTG16]. **Context**

[BDGS16, RS05]. **Context-aware** [BDGS16]. **context-explicit** [RS05]. **contexts** [BMPr05, FR06]. **contingency** [HLVA11]. **contract** [NS06]. **Control** [AJJ95, AHB08, ASL96, ACDS08, ACK⁺10, AR12, BBFR00, BJLT01, BDJP10, Bis12, BGS06, Bro02, HTS00, HPS03, HH09, KNS08, LCL⁺15, RW97, SPS⁺14, SAsC11, TR11, TL07, UAV⁺14, VAGL09, WWJ04, WLJW07, YGSY15, YSD13, ZRG08, BDP05]. **controlled** [BW08]. **Controlling** [dC96]. **CookiExt** [BCFK15]. **cooperative** [BFM05, LKAJ16]. **Coordinated** [OMSH04, ZGDS13]. **Coprocessor** [WD08]. **Coprocessor-based** [WD08]. **CORBA** [Bro02, Kar00]. **core** [AACP13]. **correct** [DJLP10, FHG99]. **Correctability** [Mil95b]. **correcting** [ATI⁺10]. **Correctness** [AJB93, McL92]. **correspondences** [Bla09]. **corruption** [BGJ03]. **Cost** [IBS04, ALP11, CGLZ03, LKAJ16, LFM⁺02, MBK⁺15, Mea01, SSBW12, YY15]. **cost-based** [Mea01]. **cost-sensitive** [LFM⁺02, SSBW12]. **costs** [GLZ11]. **counterevidence** [BLL02]. **coupon** [AS15]. **coverage** [JBH13]. **Covert** [Wra92]. **creation** [ASL96]. **credential** [LWM03]. **credentials** [WCJS97]. **crime** [HSR08]. **cryptanalysis** [KSWH00]. **Cryptographic** [Syv92, BR05b, CFL13, Coh03, CDL06, Dug04, DGJN14, GJ04, GEL98, KAM08, Pau98, YSM14]. **cryptography** [ACK⁺10, Lop06, Mat98]. **cubes** [WWJ04]. **curves** [BGH⁺13]. **CWASAR** [BKA⁺97]. **Cyberspace** [GOvdR99]. **cycle** [LKWB06]. **cycles** [ABHS09, BPS08].

Data [NBM95, Yah93, AXR12, BDF⁺12, BT06, BLB⁺09, CDE⁺10, CDF⁺11, CDF⁺12, Cli00, DS99, DFP⁺13, DFJ⁺15, DGMS03, DRRW11, DRD11, HLVA11, LWZZ15, RB99, SPS⁺14, ST15, SM05, VPZ16, WWJ04, ZMHT07]. **Data-Exchange** [Yah93]. **Database** [AJJ95, AJB93, HDC95, CDF97, DS97, DCMP16, LKAJ16, MM96, VPZ16, YWW⁺09]. **Databases** [BOS95, KK95, Mot92, TS93, CT09, SC00, TvdRO03, WYSJ08]. **datasets** [ACM15]. **DDoS** [PSJ⁺13, SM05]. **decentralized** [ACM04, BFG10]. **Decidability** [RS05]. **decision** [HS05]. **Declassification** [MSZ06, SS09, MB09, RS16]. **declassification-aware** [RS16]. **decoys** [BKP⁺12]. **defense** [PSJ⁺13]. **Defining** [Low04b]. **definition** [KTV12]. **definitions** [CGKO11, HMQU09]. **definitive** [DT97]. **delegatable** [MG08]. **Delegated** [ST15]. **deletion** [BF99]. **delivery** [Nzs05, ZMHT07]. **Denial** [Mil93b, Mea01, M0l05]. **Dependencies** [BC92, SST08, dC96]. **dependent** [BPS08]. **Depender** [WLM01, WLM02]. **deploy** [dSRCP17]. **derivation** [CDF97, DDMP05]. **deriving** [KB11]. **Design** [BFG10, LLA15, ABFK03, Gut04b, KSS13, LWZZ15, RW97, ZAF08]. **Designing** [WMF⁺17]. **detect** [BR04, DS99]. **Detecting** [BBDG10, CYC17, HDC95, RCBM07, SG96, JKK10, WDDN00]. **Detection** [Mil99, BGJ03, BHSV14, DPV09, EVK02, HFS98, IBS03, IBS04, KPS16, KSZ02, LFM⁺02, LWWJ02, MMF15, NG08, SM05, SVSM07, SG02, SHM02, UC07, VK99, VVB⁺09, XVW⁺06, Yas02, SAE⁺05]. **detectors** [KSZ02]. **determinism** [RWW96]. **develop** [Lot97]. **devices**

[BDJP10, CMTB16, CFL13, MvO11]. **Diet** [MGK⁺17]. **Diet-ESP** [MGK⁺17]. **differentially** [AAC⁺15]. **differentially-private** [AAC⁺15]. **differentiation** [MVB10]. **Diffie** [MS05a, MS05b]. **Digital** [CMS97, AGHP14, BSSB06, WD08, WCJS97]. **dimensional** [CT09, WLJW07]. **Dimensions** [SS09]. **directories** [LKWB06]. **disclosure** [BH09, LWZZ15, MB09]. **Discovering** [BBDLM14]. **discovery** [CYC17, CEE⁺01, LWM03]. **discretionary** [AH97]. **disjoint** [Gut04b]. **disjointness** [BHM14]. **display** [KNTU13]. **display-equipped** [KNTU13]. **dissemination** [BLB⁺09]. **distance** [ABK⁺11, BMV15]. **distance-bounding** [BMV15]. **Distributed** [GLP93, LWM03, WL93, BFM05, BGS06, DFJ⁺11, HLVA11, HVL12, JHS96, MS03, MS96, SWC07, YSD13, YLZ05, ZDM07]. **Distributing** [CGM95]. **Distribution** [BMS95, CCD06, SPD⁺10, WLM01, WLM02]. **distributions** [BDF⁺12]. **diversity** [PS10b]. **DNSSEC** [Gue09]. **document** [KPS16]. **documents** [BFM05, DGK⁺04]. **Dolev** [BPS08]. **Domain** [MSC04, CS05, KM98, SG02]. **domain-specific** [SG02]. **downward** [GLZ11]. **driven** [AJS12, BGT15]. **DRM** [DTG16]. **Duty** [NBM95]. **Dynamic** [Bis12, BFM07, MMHS13, NBM95, BM99, FR06, MGS⁺17, PSJ⁺13, SST08]. **dynamically** [LOS16].

e-mail [NZS05]. **e-Passports** [LG10]. **E-voting** [CW17]. **eavesdropping** [Han11]. **economic** [CGLZ03]. **Edge** [VAGL09]. **Edge-RMP** [VAGL09]. **editor** [AH00a, BEN96, BMK97, Cup02, DM00, Foc05, Fol98, Fol99, Fri02, Gor05, Gut04a, JG02, LZ11, Lin99, Lin00, Mer97, SS97, Sch03, Sch04, Syv01, Syv03, TvdR03, Gon95, Gri11, Li12, Mil93a, Mil95a, Mil96, San92a]. **Editorial** [Dam08, Foc10, JM10]. **Editors** [Ano07b, BZ14, BR05a, JM92a, JM92b, JM93, JM95a, JM95b, JM96a, JM96b, JM97, LM92, MK93, YGH08, YRY08]. **Effective** [NSH14, XVW⁺06, BFGS08, BFGS09, IBS04]. **effects** [GJ04, HH09]. **Efficient** [ASV08, BDG14, DFJ⁺16, MCB13, ZSXJ06, CGKO11, HVL12, KSS13, LYW⁺10, LZ13, LLA15, SBP01, Zúq05]. **Efficiently** [SAsC11]. **Electronic** [ABO06, BKA⁺97, DKR09, Sin11]. **Eliminating** [BLL02]. **elliptic** [BGH⁺13]. **email** [BDG⁺10]. **embedded** [KSZ02]. **Embedding** [BR04]. **empirical** [CGLZ03]. **eMRTD** [BB14]. **encrypted** [DRD11, MW04]. **Encryption** [NZS05, ABHS09, BPS08, CG06, CGKO11, GHPS13, Gut04b, LCL⁺15, MSas13, SP03, WMF⁺17]. **energy** [MMF15]. **energy-based** [MMF15]. **enforce** [CDF⁺12]. **enforcement** [ASV08, BBK14, BM12, CDE⁺10, DS97, DFJ⁺11, LKAJ16, MBK⁺15, MMHS13, MT08, ZAF08]. **Enforcing** [AH97, CCF98, MP06, MSZ06, BFR00, CDF⁺11, SAsC11, WS02]. **engineering** [GEL98]. **enhanced** [ACK⁺10, BDP05, DTG16, GHRS05]. **Enhancing** [LWWJ02]. **enterprise** [HZO⁺13]. **enterprises** [HSR08, MT08]. **entity** [BCM13]. **environment** [ASV08, IBS03, Yas02]. **equipped** [KNTU13]. **equivalence** [BWA10]. **error** [ATI⁺10]. **errors** [VVB⁺09]. **ESP**

[MGK⁺17]. **EsPRESSO** [BDG14]. **Establishing** [BSSB06, Gut14]. **establishment** [GT17, ZMHT07]. **estimating** [MMF15]. **EU** [CLM⁺10, Cam10]. **EU-funded** [CLM⁺10, Cam10]. **European** [Ano92b, BKA⁺97]. **evaluable** [CZ16]. **Evaluating** [PS14, YWW⁺09]. **evaluation** [BW08, BDG14, CMTB16, CMMV07, DFJ⁺11, IBS03, KSS13, SAE⁺05]. **Event** [BGT15]. **Event-driven** [BGT15]. **events** [JPSS16]. **evidence** [CGLZ03]. **exact** [GEL98]. **Exchange** [Yah93, BHČ04, KR03]. **execution** [AHB00, DDNP14, RS16, dSRCP17]. **existence** [HS05]. **Expected** [DMV15]. **Experimental** [PV05, IBS03]. **experts** [BFGS08, BFGS09]. **explicit** [RS05]. **Exploiting** [ACK⁺10, TEML08, vOT11]. **Exploring** [DRRW11, SA16]. **exponentiation** [MS05a, MS05b]. **exposure** [Cli00]. **expressions** [MW04]. **Expressive** [San92b, ASL96, TL07]. **Extended** [AS92, BOS95, BCG⁺02]. **extension** [LYW⁺10]. **extensions** [DKS10, Elb08].

factor [BSSM⁺07]. **fair** [KR03]. **faithfulness** [GTZ04]. **Fast** [HDC95, ZF12]. **Fault** [HL01, WLM01, WLM02]. **Fault-preserving** [HL01]. **fault-tolerant** [WLM01, WLM02]. **feasible** [CLD⁺17]. **feature** [BFGS08, BFGS09]. **federated** [BMBS10, DS97, GTY08]. **Federation** [SS10, BSSB06]. **federations** [CDF97]. **Field** [GHPS13]. **filtering** [BDG⁺10]. **Finding** [PS10a, dSRCP17]. **Fine** [RS16]. **Fine-grained** [RS16]. **Finite** [GL10]. **firewall** [UC07]. **First** [Coh03, Hal17]. **First-order** [Coh03, Hal17]. **Fixed** [WDDN00]. **Fixed-** [WDDN00]. **fixing** [CS13]. **flaw** [HLS03]. **flaws** [BBDG10]. **Flexible** [DGK⁺04]. **Flow** [BDP05, Gra92, Kre13, AAP12, BN07, Bec12, BJLT01, Bis96, BMPR05, BPR07, CHM07, CMS09, DHRS11, DR16, FR06, GHRS05, HH09, HBS16, LOS16, Low04b, SST08, VIS96, YT11, dACD⁺16]. **Folklore** [Her09]. **Forcing** [HM13]. **forensic** [BS04]. **Foreword** [Cam10, LaP96]. **Formal** [CCBE13, DKS10, Mea92, MSC04, NRW14, ABHS09, AS15, BBDLM14, BHČ04, CW17, GL10, Pau01, SRS⁺02]. **formalization** [TR11]. **formally** [Lot97]. **Forward** [Mil95b]. **forwarded** [BGSW11]. **Foundation** [Gra92]. **Foundational** [CMPP14]. **frame** [LSMR16]. **framework** [AHB08, AS15, ABK⁺11, BS02, DLYZ11, JAH⁺16, KNS08, LVA14, Mea01, PS10b, ZMHT07]. **frameworks** [IBS04]. **free** [BBK14, DTX09]. **frequency** [CS05, Han11]. **freshness** [TBEB08]. **fully** [DDL15]. **function** [HS05, KSS13, QJ97]. **Functional** [McL92]. **functionality** [TEML08]. **functions** [CZ16]. **funded** [CLM⁺10, Cam10]. **fusion** [BT06, SM05]. **future** [HP00]. **Fuzzy** [Hu92, Tro93].

game [KR03, KTV12, LT17, MGS⁺17, SKEG14]. **game-based** [KR03, KTV12]. **game-theoretic** [SKEG14]. **garbage** [BF99]. **garbled** [CMTB16]. **general** [DGJN14, KSS13]. **general-purpose** [DGJN14]. **generalized** [Elb08, MSAV15]. **generated** [AGHP14]. **generating** [BKP⁺12]. **generation** [CB15, ZF12]. **generator** [Zúq05]. **Generic** [Wan06].

gigabit [IBS03]. **GKMPAN** [ZSXJ06]. **Global** [DLRS01, TA92, CDF97, KK16]. **Globally** [LG10]. **goals** [GHRS05, Gut14]. **GPU** [LLA15]. **grained** [RS16]. **Grant** [Bis95, Bis96]. **granularities** [LWWJ02]. **Graph** [FF11]. **graphical** [vOT11]. **graphs** [BBI15, BJLT01, CAFL10, HZO⁺13, WYSJ08, WLM01, WLM02]. **Group** [ZSXJ06, CLK04, CCBE13, DTX09, MS05a, MS05b, PQ03, PQ06, Xu07, MSC04]. **groups** [CYC17]. **Guessing** [BWA10, Low04a]. **Guest** [AH00a, BEN96, BMK97, Cup02, Dam08, DM00, Foc05, Fol98, Fol99, Fri02, Gor05, Gut04a, JG02, LZ11, Lin99, Lin00, Mer97, SS97, Sch03, Sch04, Syv01, Syv03, TvdR03, Ano07b, BZ14, BR05a, Gon95, Gri11, Li12, LM92, MK93, San92a, YGH08, YRY08]. **Guest-editor** [BEN96]. **Guiding** [DGJN14].

hash [QJ97]. **hashing** [BGH⁺13, LLA15]. **haystack** [PS10a]. **HB** [HSH11]. **healthcare** [YSD13]. **hear** [BBS⁺15]. **Helios** [CS13]. **Hellman** [MS05a, MS05b]. **Hermes** [ZMHT07]. **heterogeneous** [BSS97]. **hiding** [CPP08, HO05, HS04]. **hierarchical** [BFGS08, BFGS09, KAM08, ST15, WD08]. **Hierarchies** [DMM10]. **hierarchy** [BBI15, CLK04]. **High** [EMO⁺93, DMM04, Han11, MR97, SV15, Zúq05]. **high-frequency** [Han11]. **high-throughput** [MR97]. **hijacking** [BCFK15]. **history** [KNS08]. **history-based** [KNS08]. **Hoc** [ZSXJ06, AJS12, RCBM07, RH07, ZDM07]. **homomorphic** [GHPS13, WMF⁺17]. **Hordes** [LS02]. **host** [DS99]. **Human** [Mat98]. **Hyperproperties** [CS10].

ICT [CLM⁺10, Cam10]. **ID** [GTY08]. **Identification** [DS99]. **Identity** [PSJ⁺13, SS10, BMBS10, BSSB06, CG06, MT08, WD08]. **identity-based** [CG06]. **IDS** [BT06]. **IEEE** [RCBM07]. **II** [LB96]. **illicit** [SG96]. **impact** [GLZ11]. **imperative** [CHM07]. **Implementation** [CS05, AXR12, SB99]. **implementations** [BHM14, CB15, Elb08]. **Implementing** [WYSJ08, GOvdR99]. **impossibility** [PQ06]. **Improved** [CGKO11, Smi06]. **in-browser** [ABR13]. **incidents** [BT06]. **increase** [DFJ⁺15]. **incremental** [BLB⁺09]. **indeed** [vdM15]. **Independence** [PS10b, RB99]. **Index** [Ano92a, Ano93, Ano95a, Ano96a, Ano97, Ano98, Ano01, Ano02, Ano03, Ano04, Ano05, Ano06, Ano07a, Ano08, Ano09, Ano10, Ano11, Ano12, Ano13, Ano14, Ano15a, Ano16]. **indexes** [DFP⁺13]. **indifferentiable** [BGH⁺13]. **indistinguishability** [YWW⁺09]. **indistinguishable** [BKP⁺12]. **individual** [RCBM07]. **Inductive** [Bel03, RDDM10, Pau98]. **Inference** [BGSW11, HDC95, Bis12, WWJ04, WLJW07]. **Inference-proof** [BGSW11]. **inferences** [BDF⁺12]. **infinite** [DR16]. **infinite-state** [DR16]. **Information** [Ano96b, Bec12, Bis95, BMPR05, BH09, FR06, Gra92, HBS16, HS04, LOS16, SM95, ABHS09, AAP12, AAC⁺15, BN07, Bis96, Bis12, BS02, BPR07, BS04, CGLZ03, CPPS07, CPP08, Cho12, CHM07, CMS09, CCP⁺17, DHRS11, DR16, DCMP16, GM10, GLZ11, GHRS05, HO05, HH09, KB11, LJM00, Low04b, SG96, SAsC11, SST08, SVSM07, YT11, dACD⁺16].

Information-flow [HBS16, dACD⁺16]. **information-hiding** [CPP08]. **information-theoretic** [KB11]. **infrastructure** [BKA⁺97, DLRS01, LG10]. **Infrastructures** [CMMV07, Pri06]. **injecting** [BKP⁺12]. **injection** [KPS16]. **inline** [DJLP10]. **Instant** [CAB10]. **instruction** [Elb08]. **integer** [ZZW⁺11]. **integer-overflow-to-buffer-overflow** [ZZW⁺11]. **integration** [BBFS00]. **Integrity** [Mot92, NBM95, SM95, DFJ⁺16, ST15, WD08]. **Inter** [GLP93, JAH⁺16, LSMR16]. **inter-frame** [LSMR16]. **inter-process** [JAH⁺16]. **Inter-Realm** [GLP93]. **interactions** [BCG⁺02]. **interactive** [AAP12, BDP10, LZ13, WYSJ08]. **Interference** [ZL95, BR05b, DHW04, RWW96, RS01]. **internal** [KSZ02]. **Internet** [GMR⁺11, DGMS03, OMSH04, PS10a, SKEG14]. **Interoperable** [LG10]. **Interpretation** [MSC04, GM10, MMHS13, PG09]. **intersection** [BHM14, VC05]. **interval** [WMF⁺17]. **intradomain** [PV05]. **intransitive** [vdM15]. **Introduction** [Gut09, VG11, YGH08, YRY08]. **intruder** [BR04]. **Intrusion** [HFS98, LJM00, Mil99, SG02, EVK02, IBS03, IBS04, KSZ02, LFM⁺02, MMF15, SSBW12, UC07, VK99, Yas02, YLZ05, ZGD04]. **investigations** [BS04]. **IoT** [MGK⁺17]. **IP** [DS99, MGK⁺17]. **iris** [BA12]. **islands** [XC09]. **ISO** [BCM13]. **ISO/IEC** [BCM13]. **isolation** [GNDB16, LJM00]. **Issue** [Vis13, BSR97, CLM⁺10, Cam10, SV15]. **issues** [BSCGS07]. **Iterative** [BM12].

Jannie [KNTU13]. **Java** [DJLP10]. **Java-like** [DJLP10]. **JavaScript** [HBS16]. **JCS** [CLM⁺10, Cam10]. **Johnny** [HM13]. **join** [DFJ⁺16]. **Journal** [BR09]. **jump** [LWZZ15].

Keccak [LLA15]. **Kernelized** [TS93]. **Key** [BPS08, BMS95, CMMV07, DMM04, LG10, Mea92, Pri06, TA92, ABHS09, ABR13, CFL13, CLK04, CCD06, GT17, Gue09, HJT⁺96, KAM08, KM98, LHM⁺10, LYW⁺10, Lop06, PQ03, PQ06, RFLW96, SPD⁺10]. **Key-dependent** [BPS08]. **keys** [DMM10, KAM08]. **know** [BBS⁺15]. **Knowledge** [Syv92, BU10, DLYZ11, LZ13, MMHS13]. **knowledge-based** [MMHS13]. **known** [LWZZ15].

Language

[ES06, BN07, BFG10, CHM07, EVK02, LOS16, MW04, Smi06, SG02, VS99]. **LaPadula** [Mil96]. **Large** [GLP93, SA16, ZDM07]. **large-scale** [ZDM07]. **layer** [JAH⁺16, MGK⁺17, RCBM07]. **layered** [GRKL15]. **layout** [XC09]. **LDAP** [LKWB06]. **Leak** [DTX09]. **Leak-free** [DTX09]. **leakage** [ABHS09, AAC⁺15, SG96]. **leakages** [VPZ16]. **learning** [RTWH11]. **length** [PB13, WDDN00]. **LESS** [SA16]. **level** [DS99, ZAF08]. **Leveraging** [HCM11, MvO11]. **Life** [LKWB06]. **Life-cycle** [LKWB06]. **lightweight** [FM98]. **like** [DJLP10]. **limit** [Cli00]. **limited** [JPSS16]. **line** [Wan06]. **linear** [HVL12]. **Linguistic** [BDGS16]. **linked** [Aba98, HvdM01]. **Linux** [GNDB16, GHRS05]. **lists** [PB13]. **lived** [ZDM07]. **liveness** [BPWS04].

local [Aba98, HvdM01]. **location** [SAsC11, SVA11]. **location-based** [SVA11]. **logic** [BBFR00, DDMP05, DMP03, GP12, HvdM01, Hal17, JH09, JPSS16]. **logic-based** [BBFR00]. **Logical** [BC92, SP03, CLK04, HvdM03, KNS08]. **login** [HM13]. **logs** [BT06]. **long** [ZDM07]. **long-lived** [ZDM07]. **looping** [Mal10]. **Loose** [DFJ⁺15]. **loss** [DMV15]. **low** [ALP11, DS99, NR11]. **low-bandwidth** [NR11]. **low-cost** [ALP11]. **low-level** [DS99]. **Lowe** [War05].

MAC [RCBM07]. **Machine** [AGHP14, MCB13, RTWH11]. **machine-checked** [MCB13]. **Machine-generated** [AGHP14]. **mail** [NZS05]. **Maintaining** [BMS95]. **malleable** [MSas13]. **malware** [RTWH11]. **Manageable** [Bro02]. **Management** [AJB93, ES06, FF11, KK95, Mea92, NBM95, AJS12, AH97, ACM04, BMBS10, Bec12, BVC⁺14, BLL02, CG06, CFL13, CDM04, CCBE13, DMM04, GTY08, IBS04, KAM08, LWM03, LT17, LKWB06, MT08, NRW14, RFLW96, ST05, SWC07, SZP⁺12, WD08]. **managing** [GMR⁺11]. **mandatory** [AH97, AFHS09]. **MANETs** [ZMHT07]. **market** [CGLZ03]. **Mashic** [LSMR16]. **Mashup** [LSMR16]. **masking** [YLZ05]. **matching** [BEM⁺13, BA12]. **Mathematical** [Gra92]. **means** [LG10, Lot97]. **measure** [KPS16]. **Measures** [LBF⁺93]. **Measuring** [MMF15]. **mechanism** [CLK04, PSJ⁺13, WS02]. **mechanisms** [AAC⁺15, BDGS16]. **mediated** [CG06, DTX09]. **mediating** [JAH⁺16]. **mediation** [ABFK03]. **memory** [GNDB16]. **Merging** [BSS97, NBM95]. **Message** [Ano07b, BZ14, GTZ04, BPS08]. **metaprogramming** [LOS16]. **metering** [FM98]. **method** [Gut04b, HJT⁺96, WLM01, WLM02]. **methodology** [CMMV07]. **Methods** [Mea92]. **Metric** [CMMV07]. **metrics** [HZO⁺13]. **micro** [LWZZ15]. **micro-data** [LWZZ15]. **Minimizing** [VAGL09]. **Minimum** [LKAJ16]. **mining** [Cli00, LVA14, MSAV15, VC05]. **misbehavior** [RCBM07]. **mitigate** [ZZW⁺11]. **Mitigating** [Möl05]. **MITRE** [LB96]. **mix** [JBH13]. **mix-zone** [JBH13]. **mixtures** [BFGS08, BFGS09]. **mobile** [AS15, ASV08, BDP10, CMTB16, HP00]. **Model** [AS92, BOS95, BJLT01, Bis95, DHRS11, DR16, JR04, Mil93b, Mot92, RS02, San92b, AHB00, BHČ04, CCD06, KL11, Low99, LHY⁺15, Mil96, RAJ98, RB99, SB99, SVA11, TR11, ZRG08, Bis96]. **Model-based** [RS02]. **Model-checking** [DHRS11, DR16]. **Modeling** [BDF⁺12, LFM⁺02, NG08]. **Modelling** [GOvdR99, Tro93]. **Models** [NBM95, ASL96, AH00b, GL10, SRS⁺02, TL07, YLZ05]. **Modular** [CDM12, SPS⁺14, HS04, KSS13]. **monadic** [HH09]. **monitoring** [DJLP10, JPSS16]. **monotonic** [ASL96]. **multi** [ASL96, BSSM⁺07, CDE⁺10, CT09, DB11, DDNP14, DRRW11, JAH⁺16, MS03, NSH14, RS16, Smi06, WLJW07, ZAF08, Zúq05]. **multi-agent** [DB11]. **multi-dimensional** [CT09, WLJW07]. **multi-execution** [DDNP14, RS16]. **multi-factor** [BSSM⁺07]. **multi-layer** [JAH⁺16]. **multi-level** [ZAF08]. **multi-objective** [DRRW11]. **multi-parent** [ASL96]. **multi-programmed**

[Zúq05]. **multi-tenant** [CDE⁺10]. **multi-threaded** [MS03, NSH14, Smi06]. **multiagent** [HO05]. **multiapplicative** [SRS⁺02]. **Multicast** [ZSXJ06, DMM04, DMM10, LS02, MR97]. **Multilevel** [AXR12, AJJ95, AJB93, JAK⁺01, KK95, TS93, AHB00, BF99, RAJ98]. **multimodal** [ATI⁺10]. **Multiple** [BMS95, CGM95, DFP⁺13, KM98]. **multisensor** [SM05]. **Multiset** [DLMS04, BCLM05, CDL⁺05]. **multithreaded** [DJLP10].

name [Aba98, HvdM01, SC00]. **name-spaces** [SC00]. **Needham** [War05]. **needles** [PS10a]. **net** [AH00b]. **NetSTAT** [VK99]. **network** [BKP⁺12, Gei13, NG08, RW97, UC07, VK99, Weh07, dC96]. **network-based** [VK99]. **network-centric** [RW97]. **Networks** [Vis13, ZSXJ06, AFHS09, CPPS07, Chu96, GT17, HZO⁺13, HCM11, JBH13, KGA03, Lop06, Mea01, PS14, RCBM07, RH07, SPD⁺10, TC16, TEMPL08, ZDM07]. **Neural** [Gei13]. **NEXPTIME** [T̄BEB08]. **NEXPTIME-complete** [T̄BEB08]. **NFC** [AS15]. **no** [CLD⁺17]. **no-root** [CLD⁺17]. **noisy** [GT17]. **Non** [BR05b, MG08, RWW96, ZL95, DHW04, KR03, LZ13, MB09, MSas13, RS01, SPS⁺14, Wan06]. **non-control** [SPS⁺14]. **Non-delegatable** [MG08]. **non-disclosure** [MB09]. **non-interactive** [LZ13]. **Non-Interference** [ZL95, BR05b, RWW96, DHW04, RS01]. **non-malleable** [MSas13]. **non-repudiation** [KR03, Wan06]. **Noninterference** [BY95, Fol92, McL92, ABG04, Smi06, VS99, vdM15]. **Norwegian** [CW17, HSR08]. **Notarized** [GTY08]. **note** [BM99]. **novel** [SBP01]. **NPATRL** [MSC04]. **NRL** [MSC04]. **number** [Zúq05].

OBDD [CDF⁺12]. **obfuscation** [PS14, PG09, PS10b]. **Object** [BOS95, TS93, BF99, DT97, HTS00]. **Object-Oriented** [TS93, DT97]. **objective** [CGKW17, DRRW11]. **objectives** [BBK14]. **obligations** [CCBE13]. **Obstruction** [BBK14]. **Obstruction-free** [BBK14]. **off** [Wan06]. **off-line** [Wan06]. **offs** [DRRW11]. **One** [SM05, PB13]. **open** [BSCGS07, TEMPL08]. **operating** [SG96]. **Operational** [LBF⁺93]. **operations** [Dug04, WMF⁺17, YLZ05]. **operator** [MS05a, MS05b]. **opinion** [CYC17]. **opportunities** [BHSV14]. **optimal** [JPSS16]. **Optimality** [Yah93]. **optimization** [DRRW11, LVA14]. **Optimizing** [JBH13]. **Oracle** [SB99]. **order** [Coh03, Hal17]. **orderings** [BSS97]. **Oriented** [TS93, DT97, LHY⁺15]. **origin** [BS04]. **outsourced** [BA12, CMTB16, CT09, DFP⁺13, LCL⁺15]. **outsourcing** [CDF⁺11]. **overflow** [ZZW⁺11]. **ownership** [NSMSN11].

P5 [SBS05]. **packet** [ZMHT07]. **pairings** [KM10]. **Panoptis** [SG02]. **Paper** [Ano15b]. **Papers** [Ano92b, Ano95b]. **paradigm** [DT97]. **parallel** [BR04]. **parameter** [BHSV14]. **parent** [ASL96]. **Parity** [WLJW07]. **Parity-based** [WLJW07]. **partial** [ABHS09]. **Party** [Yah93, KSS13]. **passive** [CMS97]. **passports** [Sin11, LG10]. **password** [HJT⁺96, MvO11]. **passwords** [vOT11]. **Patching** [BCFK15]. **Paths** [HDC95]. **pattern** [BEM⁺13].

patterns [WDDN00]. **payment** [CMS97, HP00]. **PCPOR** [YY15]. **IEC** [BCM13]. **MC** [CAFL10]. **SDSI** [CEE⁺01, JR04]. **subscribe** [YSM14]. **UC-soundness** [BPS08]. **Penetration** [GG92]. **Penetration-Resistant** [GG92]. **performance** [DTG16, IBS03, LLA15, MM96, SV15]. **Performing** [BT06]. **persistent** [TC16]. **personal** [MvO11]. **pervasive** [JBH13]. **Petri** [AH00b]. **phishing** [BDG⁺10]. **pi** [DKR10]. **pie** [HNS⁺14]. **PKCS#11** [CFL13, DKS10]. **PKI** [BVC⁺14, BB14, NTU11, PS10a]. **PKI-based** [NTU11]. **plaintext** [MSas13]. **Planning** [BDF09]. **plans** [CDM12]. **platform** [GMR⁺11]. **policies** [AR12, BDP05, CCBE13, HTML09, MBK⁺15, MMHS13, WS02]. **Policy** [AJS12, YGSY15, ASV08, BBI15, BW08, Bis12, CDE⁺10, CMMV07, ES06, FF11, MB09, MP06, MT08, NRW14, ZAF08]. **policy-based** [CMMV07]. **Policy-driven** [AJS12]. **Polynomial** [BPWS04, HMQU09, HM10]. **polynomial-time** [HM10]. **portscans** [SHM02]. **Power** [San92b, ASL96, HM10, MMF15, TL07]. **Practical** [BMV15, DCMP16, Han11, NSMSN11, SHM02, BM12]. **practically** [KSS13]. **practice** [DDNP14, Her09]. **predictability** [vOT11]. **Preface** [AL12, Atl11, BBW07, BCLP12, DG13, DJLS14, Foc06, Gon95, GP10, Got06, Got07, Got10, Gri11, JM92a, JM92b, JM93, JM95a, JM95b, Li12, LM92, MK93, Mil93a, Mil95a, MB12, PJ09, Sab08, Sab10, San92a, ZK06, AH00a, BR05a, BEN96, BMK97, Cup02, DM00, Foc05, Fol98, Fol99, Fri02, Gor05, Gut04a, JM96a, JM96b, JM97, JG02, LZ11, Lin99, Lin00, Mer97, Mil96, SS97, Sch03, Sch04, Syv01, Syv03, TvdR03]. **Preprocessing** [BW08]. **preservation** [DTG16]. **Preserving** [CWT14, BSSM⁺07, BDG14, BLB⁺09, DCMP16, Gut14, HSH11, HL01, LWZZ15, WMF⁺17]. **prevent** [HLS03]. **preventing** [BDF⁺12, BBDG10, SKEG14]. **Prevention** [SVSM07]. **PRIME** [ACK⁺10]. **principles** [SS09]. **Privacy** [ABR13, BSSM⁺07, BLB⁺09, MT08, SWH⁺08, ACDS08, ACK⁺10, BCL15, BCL97, BDG14, CWT14, CDF⁺11, DTG16, DKR09, DLYZ11, DRRW11, DCMP16, HSH11, HS04, LYW⁺10, LWZZ15, PS14, SZP⁺12, TvdRO03, WMF⁺17, YWW⁺09]. **privacy-aware** [ACDS08]. **privacy-enhanced** [ACK⁺10]. **Privacy-preserving** [BLB⁺09, BDG14, DCMP16, HSH11, WMF⁺17]. **Privacy-supporting** [ABR13]. **privacy-type** [DKR09]. **Private** [SRG97, AAC⁺15, DFP⁺13, DDL15]. **Probabilistic** [MBK⁺15, Shm04, VS99, ABG04, HM10, JPSS16, MMHS13, NS06, Smi06]. **Problem** [HCH⁺93, BCL15, BFO05, CGKW17, MSAV15, TC16]. **problems** [YT11]. **procedure** [HS05]. **Process** [FG95, RS01, ABG04, BCLM05, BS04, JAH⁺16, WDDN00, YLZ05]. **process-algebraic** [ABG04]. **processes** [APRR14]. **processing** [AXR12, JAK⁺01, MM96, RAJ98]. **product** [KSWH00]. **profile** [SVA11]. **profiles** [LWWJ02]. **Programmable** [HPS03]. **programmed** [Zúq05]. **programming** [HVL12]. **programs** [BPR07, DJLP10, MS03, NSH14]. **Project** [ACK⁺10]. **Prometheus** [CCP⁺17]. **Proof** [GP12, BGSW11, BR05b]. **proofs**

[AGHP14, BU10, GL10, Hal17, MCB13, YY15]. **Properties** [FG95, Fol92, BJLT01, CDL06, DHRS11, DR16, DKR09, DMP03, Hal17, NRW14, RDDM10]. **propositional** [Bis12]. **proprietary** [DKS10]. **protecting** [BSSB06]. **Protection** [AS92, Bis95, Bis96, HSR08, Mil93b, San92b, ATI⁺10, CAFL10, DLRS01, WD08]. **protections** [SPS⁺14]. **Protocol** [Mea92, MSC04, BHM14, BCLM05, BHČ04, CB15, CDL⁺05, CW17, DDL15, GT17, GTZ04, Gut14, LS02, MR97, MCB13, MS05a, MS05b, Pau01, SBS05, SBP01, War05, Yas02, ZF12, MSC04]. **Protocols** [SM95, Syv92, Yah93, AS15, ABK⁺11, Bel03, Bla09, BBD⁺05, BR05b, CPP08, Coh03, CEHM07, CDL06, DDMP05, DKR09, DGJN14, DMP03, DLMS04, FHG99, GRKL15, GJ03, GJ04, GEL98, Gut04b, HSH11, HLS03, HL01, JH09, KSS13, KR03, KM10, KK16, Low98, Low99, Low04a, MVB10, NR11, PB13, Pau98, PQ03, PQ06, PV05, RS05, RB99, TBEB08, Wan06]. **Prototype** [EMO⁺93]. **Provable** [GEL98]. **Provably** [BCM13, DJLP10, GNDB16, BMV15]. **prove** [DGJN14]. **Proved** [CB15]. **provenance** [AACP13]. **Providing** [BS04]. **Proving** [McL92, RB99, DMP03, FHG99]. **provisioning** [MP06]. **pseudonym** [CG06]. **pseudorandom** [CZ16]. **Public** [CMMV07, LG10, Pri06, TA92, YY15, Lop06]. **public-key** [Lop06]. **publicly** [CAB10, DGMS03, HLVA11]. **Publicly** [CZ16, NMP⁺13, CGLZ03, LWZZ15]. **publicly-known** [LWZZ15]. **publish** [YSM14]. **publish/subscribe** [YSM14]. **publishing** [CDF⁺12, DFJ⁺15]. **purpose** [DGJN14]. **purposes** [KNTU13].

Qualified [MSZ06]. **qualitative** [Hal17]. **quality** [DRRW11, Zúq05]. **quantification** [VPZ16]. **Quantifying** [CMS09, CHM07]. **Quantitative** [AAP12, Hal17, YT11, ZMHT07]. **quantity** [Low04b]. **quantum** [SPD⁺10]. **queries** [Bis12, BH09, DFJ⁺16, VVB⁺09, WLJW07]. **Query** [CT09, BW08, CWT14, DFJ⁺11, PS14].

random [Zúq05]. **randomization** [XC09]. **randomness** [BM99]. **range** [WLJW07]. **rank** [HS05]. **rational** [BHČ04]. **RBAC** [BGT15, LHY⁺15]. **reader** [NTU11]. **real** [BT06]. **real-time** [BT06]. **Realm** [GLP93]. **Reasoning** [KGA03, BHM14]. **Reconstructing** [CDM04]. **reconstruction** [HvdM03]. **Recoverable** [NZS05]. **recovery** [CLK04, KM98]. **redirection** [Kre13]. **Reducing** [Hu92, VVB⁺09]. **reduction** [MVB10]. **refinement** [BHM14, ZAF08]. **reflection** [WS02]. **refreshments** [BGSW11]. **Registry** [SAE⁺05]. **Regular** [Ano15b]. **regulating** [BS02]. **Rekeying** [ZSXJ06]. **Relating** [BCLM05]. **Relational** [Mot92, WYSJ08]. **Relations** [Pau01, SP03]. **relationship** [RW97]. **relationship-based** [RW97]. **release** [BDF⁺12, BS02, Cho12, HTML09]. **released** [YWW⁺09]. **reliability** [LT17]. **reliable** [MR97, ZMHT07]. **remapping** [PSJ⁺13]. **repairing** [BCM13]. **repeater** [SPD⁺10]. **replacement** [LHM⁺10]. **replacing** [KAM08]. **Replicated** [KK95, MM96]. **replicated-architecture** [MM96]. **replication**

[SVSM07]. **Report** [LB96]. **represent** [BBI15]. **reproducibility** [SA16].
reputation [KR03, Wan06]. **Reputation** [ST05, KNS08].
Reputation-based [ST05]. **requests** [VVB⁺09]. **Required** [Cho12].
Requirements [AJB93, ABFK03]. **Research**
 [Ano92b, ZGD04, CLM⁺10, Cam10, Pri06]. **resiliency** [CGKW17].
resistance [KTV12]. **Resistant** [GG92]. **Resource** [Mil93b, BDP10].
resources [JPSS16]. **responding** [OMSH04]. **response**
 [LFM⁺02, SSBW12, ZGD04]. **result** [ACK⁺10, Low99]. **retrievability**
 [YY15]. **retrieval** [DCMP16]. **revisited** [DDL15]. **revocation**
 [CAB10, HTML09, NTU11]. **revoking** [CMS97]. **rewriting**
 [BCLM05, CDL⁺05, DLMS04]. **RFID**
 [ALP11, ABK⁺11, DLYZ11, HSH11, Han11, KNTU13, NSMSN11, NTU11].
ring [LYW⁺10]. **Risk** [Mal10, SWC07, CPP08]. **RMP** [VAGL09]. **Robust**
 [HJT⁺96, MSZ06, RCBM07, ZDM07, Her09]. **Robustness** [MSZ06].
Rogaway [MW04]. **Role** [BGS06, SB99, SM95, AJS12, AHB08, AR12,
 BBI15, LVA14, MSAV15, TR11, UAV⁺14, VAGL09, YGSY15]. **Role-based**
 [BGS06, SB99, AJS12, AR12, BBI15, TR11, VAGL09]. **rollbackability**
 [ZGD04]. **rollover** [Gue09]. **root** [CLD⁺17]. **routing** [PV05]. **RSA**
 [NZZ05, ZDM07]. **RSA-based** [NZZ05]. **rule** [LKAJ16, VC05]. **run**
 [SVSM07]. **run-time** [SVSM07]. **runtime** [HMQU09].

safely [HM13]. **safety** [AH00b]. **sample** [BDG14, Cli00]. **sandboxes**
 [PGK14]. **sandboxing** [LSMR16]. **satisfiability** [CGKW17]. **Scalable**
 [AR12, BB14, SBS05]. **scale** [SA16, ZDM07]. **scan** [XVW⁺06]. **scenarios**
 [Lot97, dSRCP17]. **Scheduler** [ZGDS13]. **schedulers** [HM10]. **scheduling**
 [BN07]. **Schematic** [AS92, San92b]. **Scheme**
 [ZSXJ06, LYW⁺10, MSas13, NSMSN11, SZP⁺12]. **schemes**
 [AGHP14, BM99, DTG16, Xu07]. **Schroeder** [War05]. **Scriptless** [HNS⁺14].
scripts [DDNP14]. **SDSI** [Aba98, HvdM01]. **Search** [MVB10, KM98, PS14].
Search-space [MVB10]. **Searchable** [CGKO11, DRD11]. **Second** [HDC95].
SecPAL [BFG10]. **Secrecy** [TBEB08, CS13, KGA03]. **secret**
 [GT17, WMF⁺17]. **secrets** [Pau01]. **SECTET** [AHB08].
SECTET-framework [AHB08]. **Section** [Ano15b, Mil99]. **Secure**
 [ABFK03, AJJ95, AJB93, BEM⁺13, BN07, BF99, BC92, BA12, CG06,
 CMTB16, CPPS07, DDNP14, HLVA11, HVL12, KK95, PTMW10, RS16,
 SV03, TS93, VC05, Yah93, ZSXJ06, AXR12, ALP11, AHB00, BHM14,
 BCG⁺02, BMPR05, BMV15, BKA⁺97, BB14, CB15, CCD06, CDF⁺08,
 CDM12, DMM04, DMM10, GNDB16, HJT⁺96, JAK⁺01, KSS13, LHM⁺10,
 Lot97, MR97, PQ06, SC00, VIS96, ZAF08, dC96]. **Securing**
 [ALP11, Chu96, RH07, SST08]. **Security**
 [BSR97, CLM⁺10, Cam10, DB11, FG95, FJ95, Gra92, Jac92, Kar00, LBF⁺93,
 Mot92, SPD⁺10, UAV⁺14, Vis13, ZAF08, AS15, AH97, ACM04, ASV08,
 AFHS09, BPS08, BBK14, BBI15, BCL15, BJLT01, BCLM05, Bla09, BT06,
 BDP05, BBD⁺05, BDGS16, BSS97, BPR07, CDE⁺10, CGLZ03, CMMV07,

CDL⁺⁰⁵, CMPP14, CWT14, CEHM07, CCBE13, DDMP05, DKS10, DT97, DMP03, DLMS04, FHG99, FR06, FF11, FM98, GRKL15, GJ03, GLZ11, GL10, GEL98, GOvdR99, Gut04b, Gut14, Hal17, HH09, HLS03, HBS16, HL01, JH09, JPSS16, JAH⁺¹⁶, KNTU13, KK16, Low98, Low99, Mal10, MBK⁺¹⁵, MS03, MMHS13, MS96, MCB13, MGK⁺¹⁷, MVB10, MGS⁺¹⁷, NRW14, PB13, RS05, RW97, RB99, RDDM10, SRS⁺⁰², Sin97, Sin11, SA16, SBP01, SV15, TvdRO03, TBEB08, WS02, Xu07, Yas02, ZF12, dSRCP17]. **Security** [Ano92b, GHRS05, BR09]. **Security-Enhanced** [GHRS05]. **security-sensitive** [dSRCP17]. **selection** [BFGS08, BFGS09, SSBW12]. **Selective** [CDF⁺¹¹]. **self** [SVSM07]. **self-replication** [SVSM07]. **semantic** [AHB00, PS10b, RAJ98, FF11]. **semantic-based** [AHB00, RAJ98]. **Semantics** [JH09, PG09, Syv92, BFG10]. **Semantics-based** [PG09]. **sensitive** [BDF⁺¹², LFM⁺⁰², SSBW12, dSRCP17]. **sensor** [CPPS07, Lop06]. **sensors** [KSZ02]. **sentiment** [CYC17]. **separate** [YGSY15]. **Separation** [Fol92, NBM95]. **sequences** [HFS98, QJ97]. **Server** [ATW97]. **Server-supported** [ATW97]. **Servers** [CGM95, DRD11]. **Service** [BCL15, Mil93b, BDF09, BS02, CDM12, Mea01, M0l05, RFLW96]. **services** [CWT14, SVA11]. **session** [BCFK15, CDF⁺⁰⁸]. **set** [BDG14, Elb08, VC05]. **severity** [VPZ16]. **severity-based** [VPZ16]. **Shared** [DRD11]. **sharing** [DTG16, WMF⁺¹⁷]. **shift** [GLZ11]. **Short** [BFPV13]. **shuffle** [LZ13]. **SIA** [CPPS07]. **Side** [KSWH00, KB11]. **side-channel** [KB11]. **signature** [AGHP14, LHM⁺¹⁰]. **signatures** [ATW97, BFPV13, DTX09, ZDM07, NZS05]. **signcryption** [LYW⁺¹⁰]. **signing** [NS06]. **sill** [HNS⁺¹⁴]. **similarity** [BDG14, KPS16]. **simple** [CHM07]. **simplifying** [HL01]. **simulatability** [HMQU09]. **simulator** [SA16]. **SINTRA** [MM96]. **SIP** [GMR⁺¹¹]. **SIP-based** [GMR⁺¹¹]. **size** [Cli00]. **skimming** [Han11]. **smart** [Bel03, BCG⁺⁰², SRS⁺⁰²]. **SMS** [TEML08]. **SMS-capable** [TEML08]. **SMT** [AR12]. **Snapshot** [AJJ95]. **socio** [BCL15]. **socio-technical** [BCL15]. **soft** [BFO05]. **Software** [CS05, AGHP14, WD08]. **solutions** [MT08]. **solving** [AR12]. **Some** [PQ03]. **sound** [KM10, LZ13, VIS96]. **Soundness** [ABHS09, BPS08, BU10, BWA10]. **space** [MVB10, XC09]. **spaces** [Aba98, CDL⁺⁰⁵, FHG99, HvdM01, KL11, SC00, SWH⁺⁰⁸]. **spam** [BFGS08, BFGS09, CYC17, SKEG14, GMR⁺¹¹]. **spammer** [CYC17]. **spatio** [TR11]. **spatio-temporal** [TR11]. **spatiotemporal** [SAsC11]. **Special** [BSR97, Mil99, SV15, Vis13, CLM⁺¹⁰, Cam10]. **specific** [SG02]. **specification** [BBFS00, CCBE13, DS97, MSC04, Sin97]. **specifications** [CB15]. **Specifying** [FJ95, YLZ05, GOvdR99]. **SPIDER** [GMR⁺¹¹]. **SPIT** [GMR⁺¹¹]. **SPKI** [CEE⁺⁰¹, ES06, HvdM03, JR04]. **SPKI/SDSI** [CEE⁺⁰¹, JR04]. **Spread** [PSJ⁺¹³]. **SPX** [TA92]. **SQL** [KPS16, VVB⁺⁰⁹]. **SQLiDDS** [KPS16]. **staged** [LOS16]. **standard** [BCM13, BCL97]. **State** [BY95, DR16, EVK02, KK16]. **State-based** [BY95, EVK02]. **Stateful** [GP12, APRR14]. **Static** [BBD⁺⁰⁵, JKK10, BWA10, BBDG10, BDGS16, CHM07]. **STATL** [EVK02].

StatVerif [APRR14]. **stealers** [CCP⁺17]. **Stealing** [HNS⁺14, Kre13]. **stealthy** [SHM02]. **steganography** [GGS⁺09]. **step** [SM05]. **stock** [CGLZ03]. **storage** [AFHS09, LT17]. **storage-area** [AFHS09]. **Strand** [FHG99, CDL⁺05, KL11]. **strategies** [RCBM07]. **Strategy** [LT17, LWZZ15]. **stream** [AXR12]. **Stricter** [AJB93]. **Strong** [BCL97]. **stronger** [MvO11]. **Structured** [SC00]. **study** [CLD⁺17, GP12, IBS03]. **style** [BPS08, GHPS13, JKK10]. **subject** [Low04a]. **sum** [WLJW07]. **support** [MMF15]. **Supported** [FJ95, ATW97]. **Supporting** [DFP⁺13, TS93, ABR13, Wan06]. **suppression** [BM12]. **surveillance** [TC16]. **surveilled** [SWH⁺08]. **survey** [CDL06, NR11, Sin11]. **suspicious** [WDDN00]. **switching** [GHPS13]. **Symbolic** [BU16, DKR10, MS05a, MS05b, AR12, BU10, MCB13]. **symmetric** [CGKO11, YWW⁺09]. **Symposium** [Ano92b]. **Synthesising** [ZRG08].

System [ES06, EMO⁺93, Tro93, ACDS08, Bis12, BKP⁺12, DDMP05, DLRS01, HFS98, IBS03, MP06, MM96, Shm04, Sin11, SA16, UC07, VK99, VIS96]. **systematic** [KSS13]. **Systems** [AJB93, GLP93, GG92, WL93, ALP11, AAP12, ATI⁺10, AH97, ACM04, Bec12, BFM05, BSSB06, CMS97, DR16, DTG16, DB11, DS97, DT97, HTS00, HO05, HP00, IBS04, JHS96, KAM08, KNS08, LCL⁺15, LJM00, Lot97, MS96, MG08, NTU11, PTMW10, SS10, SG96, Sin97, SV15, VPZ16, YSD13, YSM14, ZRG08, ZAF08, Zúq05]. **Syverson** [BHČ04].

table [DCMP16]. **tables** [HLVA11]. **tags** [HSH11, KNTU13]. **taint** [JKK10]. **taint-style** [JKK10]. **Take** [Bis95, Bis96]. **Take-Grant** [Bis95, Bis96]. **tampering** [BHSV14]. **targets** [CYC17]. **taxonomy** [BSCGS07]. **Technical** [LB96, BCL15]. **technique** [BGJ03]. **techniques** [BFGS08, BFGS09, BR05b, DRRW11, RB99, WMF⁺17, XVW⁺06]. **Telephony** [GMR⁺11, SKEG14]. **template** [ATI⁺10]. **Temporal** [BBFS00, JPSS16, MSAV15, TR11, UAV⁺14]. **tenant** [CDE⁺10]. **tests** [Gut04b]. **TG** [CAFL10]. **TG/MC** [CAFL10]. **Theft** [Bis95]. **their** [CZ16, KSS13]. **Theorems** [Jac92, MW04]. **theoretic** [KB11, SKEG14]. **theories** [BM12]. **Theory** [DDNP14, GG92, GP12, Her09, LT17, TL07]. **there** [GLZ11]. **threaded** [MS03, NSH14, Smi06]. **Threat** [FF11, Lot97, BT06, ZZW⁺11]. **threats** [Mal10, YWW⁺09]. **threshold** [BM99]. **throughput** [MR97]. **ticket** [HTS00]. **ticket-based** [HTS00]. **Time** [Hu92, Tro93, BT06, BBDG10, HM10, LWWJ02, SVSM07]. **Timed** [CEHM07, Kre13]. **Timing** [Hu92, Wra92]. **TLS** [KL11]. **tokens** [Han11]. **tolerant** [WLM01, WLM02]. **touching** [HNS⁺14]. **trace** [DHRS11, DR16, RDDM10]. **trace-based** [DHRS11, DR16]. **Traces** [McL92]. **trade** [DRRW11]. **trade-offs** [DRRW11]. **traffic** [Weh07]. **Transaction** [KK95, JAK⁺01, MM96, RAJ98]. **transactional** [ACM15]. **transactions** [BGSW11, RAJ98]. **transfer** [NSMSN11]. **transform** [DPV09]. **transformations** [HL01]. **Translation** [GGS⁺09, ABR13].

Translation-based [GG⁺09]. **transparent** [RS16, Wan06]. **trapping** [MS96]. **treatment** [YSM14]. **Tree** [HSH11, LLA15]. **Tree-based** [HSH11]. **triggers** [CCF98]. **TripleMon** [JAH⁺16]. **Trojan** [Gei13]. **Trust** [CLM⁺10, Cam10, CGM95, ES06, SM95, Bec12, BVC⁺14, CDM04, DB11, LWM03, NRW14, ST05, SZP⁺12, WD08, ZMHT07]. **trust-augmented** [SZP⁺12]. **Trusted** [NBM95, Gue09, SPD⁺10]. **trustees** [CMS97]. **TTP** [Wan06]. **tutorial** [Mö105]. **Two** [AJJ95, Yah93, KSS13, Pau01, SAE⁺05]. **Two-Party** [Yah93, KSS13]. **Two-Snapshot** [AJJ95]. **Type** [CFL13, Dug04, BHM14, BBDG10, DKR09, HLS03, PQ06, VIS96, ZZW⁺11]. **Type-based** [CFL13, Dug04]. **Typed** [PGK14, LOS16]. **Typed-based** [PGK14]. **Types** [GJ04, BHM14, BFM07, SV03]. **typing** [GJ03]. **typings** [Smi06].

unauthorized [HSR08]. **unbounded** [PB13]. **uncertain** [SAsC11]. **uncertainty** [CAFL10]. **unclassified** [GM10]. **unconditionally** [ALP11, CCD06]. **Unified** [Mot92, CCD06]. **uniform** [BS02]. **unifying** [MS03]. **Union** [BHM14]. **universal** [BU16]. **Unleashing** [Lop06]. **unspoofable** [NR11]. **untrusted** [DRD11, MvO11, SV03]. **Unwinding** [Mil95b]. **update** [BGSW11]. **updates** [BFM05]. **upon** [PQ03]. **URA97** [SB99]. **usability** [MGS⁺17, KNTU13]. **used** [CDL06]. **User** [BSCGS07, BMS95, NTU11, CWT14, LHY⁺15, SB99, TC16]. **User-aided** [NTU11]. **user-oriented** [LHY⁺15]. **user-role** [SB99]. **Using** [Cli00, JPSS16, KSZ02, McL92, TA92, WS02, WCJS97, ZZW⁺11, AFHS09, BT06, CG06, CCF98, CAB10, DRRW11, FF11, GT17, Hal17, HFS98, HZO⁺13, KPS16, KM10, LWVJ02, MMHS13, MSC04, RTWH11, SG02, TvdRO03, WYSJ08, Weh07, XC09, YLZ05]. **utility** [DFJ⁺15].

validation [BBD⁺05]. **value** [BDF⁺12]. **variable** [WDDN00]. **variable-length** [WDDN00]. **various** [XVW⁺06]. **vehicular** [RH07]. **Verifiable** [NZS05, NMP⁺13]. **Verification** [APRR14, PB13, AGHP14, Bel03, Bla09, CT09, Coh03, KR03, NSH14, NRW14, PGK14]. **Verified** [BGH⁺13, SRS⁺02, ZRG08, dACD⁺16]. **verifier** [DGJN14]. **verify** [KNTU13]. **Verifying** [BDJP10, DKR09, GRKL15, GHRS05, BDF09, BB14, Pau98]. **version** [BCG⁺02]. **versus** [DRRW11]. **via** [AJJ95, BMS95, Elb08, SST08, SKEG14]. **video** [QJ97, SWH⁺08]. **View** [BC92, BGSW11]. **views** [YWW⁺09]. **virtual** [CDE⁺10]. **visibility** [CDF⁺12]. **VoIP** [SS10]. **Volume** [Ano95a, Ano96a, Ano97, Ano98, Ano01, Ano02, Ano03, Ano04, Ano05, Ano06, Ano07a, Ano08, Ano09, Ano10, Ano11, Ano12, Ano13, Ano14, Ano15a, Ano16, LB96]. **voting** [CW17, DKR09, SZP⁺12]. **vs** [WDDN00]. **vulnerabilities** [BHSV14, DS99, JKK10, RS02, ZGDS13]. **Vulnerability** [HCH⁺93, BFO05, HZO⁺13].

wall [ACM04]. **watermarking** [CS05]. **wavelet** [DPV09]. **Web**

[BSR97, BHSV14, DDNP14, JKK10, VVB⁺09, BS02, BVC⁺14, HCM11, PS14, PGK14, SRG97, WCJS97]. **web-based** [VVB⁺09]. **WebCallerID** [HCM11]. **WebDAV** [CAB10]. **WebInject** [CCP⁺17]. **WebInject-based** [CCP⁺17]. **website** [BBDLM14]. **well** [Kre13]. **well-timed** [Kre13]. **Wide** [BSR97, WCJS97]. **Window** [EMO⁺93]. **Windows** [SAE⁺05]. **wireless** [GT17, JBH13, Lop06]. **wiretapping** [BBS⁺15]. **within** [BR04]. **without** [HNS⁺14, YGSY15]. **workflow** [AH97, AH00b, ACM04, CCF98, CGKW17, GOvdR99, TvdRO03]. **workflows** [AHB00, dSRCP17]. **Working** [FJ95]. **World** [BSR97, WCJS97]. **worm** [XVW⁺06]. **worms** [Weh07]. **wrappers** [SV03]. **Write** [TS93]. **Write-Up** [TS93]. **WWW** [BSR97].

X.509 [LKWB06]. **XML** [BFM05, DGK⁺04]. **XPath** [BH09].

Yahalom [Pau01]. **Yao** [BPS08]. **Yao-style** [BPS08].

zero [BU10, DLYZ11, LZ13]. **zero-knowledge** [BU10, DLYZ11, LZ13]. **zone** [JBH13].

References

Alvim:2015:ILD

[AAC⁺15] Mário S. Alvim, Miguel E. Andrés, Konstantinos Chatzizokolakis, Pierpaolo Degano, and Catuscia Palamidessi. On the information leakage of differentially-private mechanisms. *Journal of Computer Security*, 23(4):427–469, ??? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Acar:2013:CCP

[AACP13] Umut A. Acar, Amal Ahmed, James Cheney, and Roly Perera. A core calculus for provenance. *Journal of Computer Security*, 21(6): 919–969, ??? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Alvim:2012:QIF

[AAP12] Mário S. Alvim, Miguel E. Andrés, and Catuscia Palamidessi. Quantitative information flow in interactive systems. *Journal of Computer Security*, 20(1):3–50, ??? 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Abadi:1998:SLL

- [Aba98] Martín Abadi. On SDSI's linked local name spaces. *Journal of Computer Security*, 6(1-2):3–21, ??? 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Altenschmidt:2003:SMR

- [ABFK03] C. Altenschmidt, J. Biskup, U. Flegel, and Y. Karabulut. Secure mediation: requirements, design, and architecture. *Journal of Computer Security*, 11(3):365–398, ??? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Aldini:2004:PAA

- [ABG04] Alessandro Aldini, Mario Bravetti, and Roberto Gorrieri. A process-algebraic approach for the analysis of probabilistic non-interference. *Journal of Computer Security*, 12(2):191–245, ??? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Adao:2009:SCF

- [ABHS09] Pedro Adão, Gergei Bana, Jonathan Herzog, and Andre Scedrov. Soundness and completeness of formal encryption: The cases of key cycles and partial information leakage. *Journal of Computer Security*, 17(5):737–797, ??? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Avoine:2011:FAR

- [ABK⁺11] Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardaş, Cédric Lauradoux, and Benjamin Martin. A framework for analyzing RFID distance bounding protocols. *Journal of Computer Security*, 19(2):289–317, ??? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Aimeur:2006:BEC

- [ABO06] Esma Aïmeur, Gilles Brassard, and Flavien Serge Mani Onana. Blind electronic commerce. *Journal of Computer Security*, 14(6):535–559, ??? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Arapinis:2013:PSC

- [ABR13] Myrto Arapinis, Sergiu Bursuc, and Mark Ryan. Privacy-supporting cloud computing by in-browser key translation. *Jour-*

Journal of Computer Security, 21(6):847–880, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ardagna:2008:PAA

- [ACDS08] C. A. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati. A privacy-aware access control system. *Journal of Computer Security*, 16(4):369–397, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ardagna:2010:ECP

- [ACK⁺10] Claudio A. Ardagna, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer, and Mario Verdicchio. Exploiting cryptography for privacy-enhanced access control: A result of the PRIME Project. *Journal of Computer Security*, 18(1):123–160, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Atluri:2004:CWS

- [ACM04] Vijayalakshmi Atluri, Soon Ae Chun, and Pietro Mazzoleni. Chinese wall security for decentralized workflow management systems. *Journal of Computer Security*, 12(6):799–840, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

AlBouna:2015:ATD

- [ACM15] Bechara Al Bouna, Chris Clifton, and Qutaibah Malluhi. Anonymizing transactional datasets. *Journal of Computer Security*, 23(1):89–106, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Aziz:2009:CSA

- [AFHS09] Benjamin Aziz, Simon N. Foley, John Herbert, and Garret Swart. Configuring storage-area networks using mandatory security. *Journal of Computer Security*, 17(2):191–210, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Akinyele:2014:MGA

- [AGHP14] Joseph A. Akinyele, Matthew Green, Susan Hohenberger, and Matthew Pagano. Machine-generated algorithms, proofs and software for the batch verification of digital signature schemes. *Journal of Computer Security*, 22(6):867–912, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

- Atluri:1997:EMD**
- [AH97] Vijayalakshmi Atluri and Wei-Kuang Huang. Enforcing mandatory and discretionary security in workflow management systems. *Journal of Computer Security*, 5(4):303–339, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).
- Atluri:2000:GEP**
- [AH00a] Vijay Atluri and John Hale. Guest editor’s preface. *Journal of Computer Security*, 8(4):241–242, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).
- Atluri:2000:PNB**
- [AH00b] Vijayalakshmi Atluri and Wei-Kuang Huang. A Petri net based safety analysis of workflow authorization models. *Journal of Computer Security*, 8(2–3):209–240, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).
- Atluri:2000:SBE**
- [AHB00] Vijayalakshmi Atluri, Wei-Kuang Huang, and Elisa Bertino. A semantic-based execution model for multilevel secure workflows. *Journal of Computer Security*, 8(1):3–41, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).
- Alam:2008:CBR**
- [AHB08] Muhammad Alam, Michael Hafner, and Ruth Breu. Constraint based role based access control in the SECTET-framework. *Journal of Computer Security*, 16(2):223–260, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).
- Atluri:1993:ASC**
- [AJB93] Vijayalakshmi Atluri, Sushil Jajodia, and Elisa Bertino. Achieving stricter correctness requirements in multilevel secure database management systems. *Journal of Computer Security*, 2(4):311–351, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).
- Ammann:1995:CCS**
- [AJJ95] Paul Ammann, Frank Jaeckle, and Sushil Jajodia. Concurrency control in a secure multilevel database via a two-snapshot algorithm. *Journal of Computer Security*, 3(2–3):87–113, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ahn:2012:PDR

- [AJS12] Gail-Joon Ahn, Jing Jin, and Mohamed Shehab. Policy-driven role-based access management for ad-hoc collaboration. *Journal of Computer Security*, 20(2–3):223–257, 2012. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Armando:2012:P

- [AL12] Alessandro Armando and Gavin Lowe. Preface. *Journal of Computer Security*, 20(1):1, 2012. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Alomair:2011:SLC

- [ALP11] Basel Alomair, Loukas Lazos, and Radha Poovendran. Securing low-cost RFID systems: An unconditionally secure approach. *Journal of Computer Security*, 19(2):229–257, 2011. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:1992:AI

- [Ano92a] Anonymous. Author index. *Journal of Computer Security*, 1(3–4):413, 1992. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:1992:CPE

- [Ano92b] Anonymous. Call for papers: European Symposium on Research in Computer Security. *Journal of Computer Security*, 1(1):131, 1992. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:1993:AI

- [Ano93] Anonymous. Author index. *Journal of Computer Security*, 2(4):353–354, 1993. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:1995:AIV

- [Ano95a] Anonymous. Author index volume 3. *Journal of Computer Security*, 3(4):325–326, 1995. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:1995:CP

- [Ano95b] Anonymous. Call for papers. *Journal of Computer Security*, 3(4):323–324, 1995. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:1996:AIV

- [Ano96a] Anonymous. Author index volume 4 (1996). *Journal of Computer Security*, 4(4):361–362, ????. 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:1996:IA

- [Ano96b] Anonymous. Information for authors. *Journal of Computer Security*, 4(1):113–119, ????. 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:1997:AIV

- [Ano97] Anonymous. Author index volume 5 (1997). *Journal of Computer Security*, 5(4):383–384, ????. 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:1998:AIV

- [Ano98] Anonymous. Author index volume 6 (1998). *Journal of Computer Security*, 6(4):287, ????. 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2001:AIV

- [Ano01] Anonymous. Author index volume 9 (2001). *Journal of Computer Security*, 9(4):339–340, ????. 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2002:AIV

- [Ano02] Anonymous. Author index volume 10 (2002). *Journal of Computer Security*, 10(4):433–434, ????. 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2003:AIV

- [Ano03] Anonymous. Author index volume 11 (2003). *Journal of Computer Security*, 11(4):723–725, ????. 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2004:AIV

- [Ano04] Anonymous. Author index volume 12 (2004). *Journal of Computer Security*, 12(6):933–935, ????. 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2005:AIV

- [Ano05] Anonymous. Author index volume 13 (2005). *Journal of Computer Security*, 13(6):905–907, ??? 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2006:AIV

- [Ano06] Anonymous. Author index volume 14 (2006). *Journal of Computer Security*, 14(6):625–626, ??? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2007:AIV

- [Ano07a] Anonymous. Author index volume 15 (2007). *Journal of Computer Security*, 15(6):717–719, ??? 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2007:MGE

- [Ano07b] Anonymous. Message from the Guest Editors. *Journal of Computer Security*, 15(1):1–2, ??? 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2008:AIV

- [Ano08] Anonymous. Author index volume 16 (2008). *Journal of Computer Security*, 16(6):791–793, ??? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2009:AIV

- [Ano09] Anonymous. Author index volume 17 (2009). *Journal of Computer Security*, 17(6):969–971, ??? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2010:AIV

- [Ano10] Anonymous. Author index volume 18 (2010). *Journal of Computer Security*, 18(6):1301–1305, ??? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2011:AIV

- [Ano11] Anonymous. Author index volume 19 (2011). *Journal of Computer Security*, 19(6):1173–1176, ??? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2012:AIV

- [Ano12] Anonymous. Author index volume 20 (2012). *Journal of Computer Security*, 20(6):765–767, ??? 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2013:AIV

- [Ano13] Anonymous. Author index volume 21 (2013). *Journal of Computer Security*, 21(6):1009–1012, ??? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2014:AIV

- [Ano14] Anonymous. Author index volume 22 (2014). *Journal of Computer Security*, 22(6):1051–1054, ??? 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2015:AIV

- [Ano15a] Anonymous. Author index volume 23 (2015). *Journal of Computer Security*, 23(6):789–791, ??? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2015:RPS

- [Ano15b] Anonymous. Regular paper section. *Journal of Computer Security*, 23(5):639, ??? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Anonymous:2016:AIV

- [Ano16] Anonymous. Author index volume 24 (2016). *Journal of Computer Security*, 24(6):839–841, ??? 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Arapinis:2014:SVS

- [APRR14] Myrto Arapinis, Joshua Phillips, Eike Ritter, and Mark D. Ryan. StatVerif: Verification of stateful processes. *Journal of Computer Security*, 22(5):743–821, ??? 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Armando:2012:SAS

- [AR12] Alessandro Armando and Silvio Ranise. Scalable automated symbolic analysis of administrative role-based access control policies by SMT solving. *Journal of Computer Security*, 20(4):309–352, ??? 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ammann:1992:ESP

- [AS92] Paul E. Ammann and Ravi S. Sandhu. The extended schematic protection model. *Journal of Computer Security*, 1(3–4):335–383, ??? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Alshehri:2015:FFS

- [AS15] Ali Alshehri and Steve Schneider. A formal framework for security analysis of NFC mobile coupon protocols. *Journal of Computer Security*, 23(6):685–707, ??? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ammann:1996:EPM

- [ASL96] Paul Ammann, Ravi S. Sandhu, and Richard Lipton. The expressive power of multi-parent creation in monotonic access control models. *Journal of Computer Security*, 4(2–3):149–165, ??? 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Atluri:2008:ESP

- [ASV08] Vijayalakshmi Atluri, Heechang Shin, and Jaideep Vaidya. Efficient security policy enforcement for the mobile environment. *Journal of Computer Security*, 16(4):439–475, ??? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Argyropoulos:2010:BTP

- [ATI⁺10] Savvas Argyropoulos, Dimitrios Tzovaras, Dimosthenis Ioannidis, Yannis Damousis, Michael G. Strintzis, Martin Braun, and Serge Boverie. Biometric template protection in multimodal authentication systems based on error correcting codes. *Journal of Computer Security*, 18(1):161–185, ??? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Atluri:2011:P

- [Atl11] Vijay Atluri. Preface. *Journal of Computer Security*, 19(3):365, ??? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Asokan:1997:SSS

- [ATW97] N. Asokan, G. Tsudik, and M. Waidner. Server-supported signatures. *Journal of Computer Security*, 5(1):91–108, ??? 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Adaikkalavan:2012:MSD

- [AXR12] Raman Adaikkalavan, Xing Xie, and Indrakshi Ray. Multilevel secure data stream processing: Architecture and implementation. *Journal of Computer Security*, 20(5):547–581, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Blanton:2012:SOC

- [BA12] Marina Blanton and Mehrdad Aliasgari. Secure outsourced computation of iris matching. *Journal of Computer Security*, 20(2–3):259–305, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Buchmann:2014:TMS

- [BB14] Nicolas Buchmann and Harald Baier. Towards a more secure and scalable verifying PKI of eMRTD. *Journal of Computer Security*, 22(6):1025–1049, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bodei:2005:SVS

- [BBD⁺05] Chiara Bodei, Mikael Buchholtz, Pierpaolo Degano, Flemming Nielson, and Hanne Riis Nielson. Static validation of security protocols. *Journal of Computer Security*, 13(3):347–390, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bodei:2010:DPT

- [BBDG10] Chiara Bodei, Linda Brodo, Pierpaolo Degano, and Han Gao. Detecting and preventing type flaws at static time. *Journal of Computer Security*, 18(2):229–264, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bansal:2014:DCA

- [BBDLM14] Chetan Bansal, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, and Sergio Maffei. Discovering concrete attacks on website authorization by formal analysis. *Journal of Computer Security*, 22(4):601–657, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bertino:2000:LBA

- [BBFR00] Elisa Bertino, Francesco Buccafurri, Elena Ferrari, and Pasquale Rullo. A logic-based approach for enforcing access control. *Journal of Computer Security*, 8(2–3):109–139, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bertino:2000:TAB

- [BBFS00] Elisa Bertino, Piero Andrea Bonatti, Elena Ferrari, and Maria Luisa Sapino. Temporal authorization bases: From specification to integration. *Journal of Computer Security*, 8(4):309–353, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Belim:2015:AGR

- [BBI15] Sergey Belim, Nadezda Bogachenko, and Evgeniy Ilushechkin. An analysis of graphs that represent a role-based security policy hierarchy. *Journal of Computer Security*, 23(5):641–657, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Basin:2014:OFA

- [BBK14] David Basin, Samuel J. Burri, and Günter Karjoth. Obstruction-free authorization enforcement: Aligning security and business objectives. *Journal of Computer Security*, 22(5):661–698, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bates:2015:AWK

- [BBS⁺15] Adam Bates, Kevin R. B. Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable wiretapping — or — I know they can hear you now. *Journal of Computer Security*, 23(2):167–195, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Backes:2007:P

- [BBW07] Michael Backes, David Basin, and Michael Waidner. Preface. *Journal of Computer Security*, 15(6):561, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bieber:1992:LVS

- [BC92] Pierre Bieber and Frédéric Cuppens. A logical view of secure dependencies. *Journal of Computer Security*, 1(1):99–129, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bugliesi:2015:CPB

- [BCFK15] Michele Bugliesi, Stefano Calzavara, Riccardo Focardi, and Wilayat Khan. CookieExt: Patching the browser against session hijacking attacks. *Journal of Computer Security*, 23(4):509–537, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bieber:2002:CSI

- [BCG⁺02] P. Bieber, J. Cazin, P. Girard, J.-L. Lanet, V. Wiels, and G. Zanon. Checking secure interactions of smart card applets: extended version. *Journal of Computer Security*, 10(4):369–398, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bergadano:1997:SAP

- [BCL97] F. Bergadano, B. Crispo, and M. Lomas. Strong authentication and privacy with standard browsers. *Journal of Computer Security*, 5(3):191–212, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bella:2015:SSP

- [BCL15] Giampaolo Bella, Paul Curzon, and Gabriele Lenzini. Service security and privacy as a socio-technical problem. *Journal of Computer Security*, 23(5):563–585, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bistarelli:2005:RMR

- [BCLM05] Stefano Bistarelli, Iliano Cervesato, Gabriele Lenzini, and Fabio Martinelli. Relating multiset rewriting and process algebras for security protocol analysis. *Journal of Computer Security*, 13(1):3–47, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Barthe:2012:P

- [BCLP12] Gilles Barthe, Jorge Cuellar, Javier Lopez, and Alexander Pretschner. Preface. *Journal of Computer Security*, 20(4):307–308, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Basin:2013:PRI

- [BCM13] David Basin, Cas Cremers, and Simon Meier. Provably repairing the ISO/IEC 9798 standard for entity authentication. *Journal of Computer Security*, 21(6):817–846, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bartoletti:2009:PVS

- [BDF09] Massimo Bartoletti, Pierpaolo Degano, and Gian Luigi Ferrari. Planning and verifying service composition. *Journal of Computer Security*, 17(5):799–837, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bezzi:2012:MPI

- [BDF⁺12] Michele Bezzi, Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, Pierangela Samarati, and Roberto Sassi. Modeling and preventing inferences from sensitive value distributions in data release. *Journal of Computer Security*, 20(4):393–436, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bergholz:2010:NFA

- [BDG⁺10] André Bergholz, Jan De Beer, Sebastian Glahn, Marie-Francine Moens, Gerhard Paaß, and Siehyun Strobel. New filtering approaches for phishing email. *Journal of Computer Security*, 18(1):7–35, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Blundo:2014:EEP

- [BDG14] Carlo Blundo, Emiliano De Cristofaro, and Paolo Gasti. EsPRESSO: Efficient privacy-preserving evaluation of sample set similarity. *Journal of Computer Security*, 22(3):355–381, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bodei:2016:CAS

- [BDGS16] Chiara Bodei, Pierpaolo Degano, Letterio Galletta, and Francesco Salvatori. Context-aware security: Linguistic mechanisms and static analysis. *Journal of Computer Security*, 24(4):427–477, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Besson:2010:VRA

- [BDJP10] Frédéric Besson, Guillaume Dufay, Thomas Jensen, and David Pichardie. Verifying resource access control on mobile interactive devices. *Journal of Computer Security*, 18(6):971–998, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bodei:2005:CSP

- [BDP05] Chiara Bodei, Pierpaolo Degano, and Corrado Priami. Checking security policies through an enhanced Control Flow Analysis. *Journal of Computer Security*, 13(1):49–85, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Becker:2012:IFT

- [Bec12] Moritz Y. Becker. Information flow in trust management systems. *Journal of Computer Security*, 20(6):677–708, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bella:2003:IVS

- [Bel03] Giampaolo Bella. Inductive verification of smart card protocols. *Journal of Computer Security*, 11(1):87–132, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Baron:2013:SPM

- [BEM⁺13] Joshua Baron, Karim El Defrawy, Kirill Minkovich, Rafail Ostrovsky, and Eric Tressler. 5PM: Secure pattern matching. *Journal of Computer Security*, 21(5):601–625, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bertino:1996:GEP

- [BEN96] Elisa Bertino, Gérard Eizenberg, and Roger M. Needham. Guest-editors' preface. *Journal of Computer Security*, 4(1):1–2, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bertino:1999:SOD

- [BF99] Elisa Bertino and Elena Ferrari. Secure object deletion and garbage collection in multilevel object bases. *Journal of Computer Security*, 7(4):257–285, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Becker:2010:SDS

- [BFG10] Moritz Y. Becker, Cédric Fournet, and Andrew D. Gordon. SecPAL: Design and semantics of a decentralized authorization language. *Journal of Computer Security*, 18(4):619–665, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Belsis:2008:AEF

- [BFGS08] Petros Belsis, Kostas Fragos, Stefanos Gritzalis, and Christos Skourlas. Applying effective feature selection techniques with hierarchical mixtures of experts for spam classification. *Journal of Computer Security*, 16(6):761–790, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Belsis:2009:AEF

- [BFGS09] Petros Belsis, Kostas Fragos, Stefanos Gritzalis, and Christos Skourlas. Applying effective feature selection techniques with hierarchical mixtures of experts for spam classification. *Journal of Computer Security*, 17(3):239–268, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bertino:2005:ACU

- [BFM05] E. Bertino, E. Ferrari, and G. Mella. An approach to cooperative updates of XML documents in distributed systems. *Journal of Computer Security*, 13(2):191–242, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bugliesi:2007:DTA

- [BFM07] Michele Bugliesi, Riccardo Focardi, and Matteo Maffei. Dynamic types for authentication. *Journal of Computer Security*, 15(6):563–617, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bistarelli:2005:SCB

- [BFO05] Stefano Bistarelli, Simon N. Foley, and Barry O’Sullivan. A soft constraint-based approach to the cascade vulnerability problem. *Journal of Computer Security*, 13(5):699–720, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Blazy:2013:SBS

- [BFPV13] Olivier Blazy, Georg Fuchsbaauer, David Pointcheval, and Damien Vergnaud. Short blind signatures. *Journal of Computer Security*, 21(5):627–661, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Barthe:2013:VIH

- [BGH⁺13] Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, Federico Olmedo, and Santiago Zanella-Béguelin. Verified indifferentially hashing into elliptic curves. *Journal of Computer Security*, 21(6):881–917, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Barbara:2003:CBC

- [BGJ03] Daniel Barbará, Rajni Goel, and Sushil Jajodia. A checksum-based corruption detection technique. *Journal of Computer Secu-*

urity, 11(3):315–329, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Braghin:2006:RBA

- [BGS06] Chiara Braghin, Daniele Gorla, and Vladimiro Sassone. Role-based access control for a distributed calculus. *Journal of Computer Security*, 14(2):113–155, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Biskup:2011:IPV

- [BGSW11] Joachim Biskup, Christian Gogolin, Jens Seiler, and Torben Weibert. Inference-proof view update transactions with forwarded refreshments. *Journal of Computer Security*, 19(3):487–529, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bonatti:2015:EDR

- [BGT15] Piero Bonatti, Clemente Galdi, and Davide Torres. Event-driven RBAC. *Journal of Computer Security*, 23(6):709–757, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Böttcher:2009:IDA

- [BH09] Stefan Böttcher and Rita Hartel. Information disclosure by answers to XPath queries. *Journal of Computer Security*, 17(1):69–99, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Buttyan:2004:FMR

- [BHČ04] Levente Buttyán, Jean-Pierre Hubaux, and Srdjan Čapkun. A formal model of rational exchange and its application to the analysis of Syverson’s protocol. *Journal of Computer Security*, 12(3–4):551–587, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Backes:2014:UIR

- [BHM14] Michael Backes, Cătălin Hrițcu, and Matteo Maffei. Union, intersection and refinement types and reasoning about type disjointness for secure protocol implementations. *Journal of Computer Security*, 22(2):301–353, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bisht:2014:ADP

- [BHSV14] Prithvi Bisht, Timothy Hinrichs, Nazari Skrupsky, and V. N. Venkatakrishnan. Automated detection of parameter tampering opportunities and vulnerabilities in web applications. *Journal of Computer Security*, 22(3):415–465, ??? 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bishop:1995:TIT

- [Bis95] Matt Bishop. Theft of information in the take-Grant protection model. *Journal of Computer Security*, 3(4):283–308, ??? 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bishop:1996:CIF

- [Bis96] Matt Bishop. Conspiracy and information flow in the Take-Grant Protection Model. *Journal of Computer Security*, 4(4):331–359, ??? 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Biskup:2012:DPA

- [Bis12] Joachim Biskup. Dynamic policy adaptation for inference control of queries to a propositional information system. *Journal of Computer Security*, 20(5):509–546, ??? 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Besson:2001:MCS

- [BJLT01] Frédéric Besson, Thomas Jensen, Daniel Le Métayer, and Tommy Thorn. Model checking security properties of control flow graphs. *Journal of Computer Security*, 9(3):217–250, ??? 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bryce:1997:CEI

- [BKA⁺97] Ciarán Bryce, Winfried Kühnhauser, Rémy Amouroux, Mauricio López, and Harry Rudnik. CWASAR: a European infrastructure for secure electronic commerce. *Journal of Computer Security*, 5(3):225–235, ??? 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bowen:2012:SGI

- [BKP⁺12] Brian M. Bowen, Vasileios P. Kemerlis, Pratap Prabhu, Angelos D. Keromytis, and Salvatore J. Stolfo. A system for generating and injecting indistinguishable network decoys. *Journal of Computer*

Security, 20(2–3):199–221, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Blanchet:2009:AVC

- [Bla09] Bruno Blanchet. Automatic verification of correspondences for security protocols. *Journal of Computer Security*, 17(4):363–434, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Byun:2009:PPI

- [BLB⁺09] Ji-Won Byun, Tiancheng Li, Elisa Bertino, Ninghui Li, and Yonglak Sohn. Privacy-preserving incremental data dissemination. *Journal of Computer Security*, 17(1):43–68, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Buldas:2002:ECA

- [BLL02] Ahto Buldas, Peeter Laud, and Helger Lipmaa. Eliminating counter-evidence with applications to accountable certificate management. *Journal of Computer Security*, 10(3):273–296, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Blundo:1999:NRD

- [BM99] Carlo Blundo and Barbara Masucci. A note on the randomness in dynamic threshold schemes. *Journal of Computer Security*, 7(1):73–85, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bielova:2012:IES

- [BM12] Nataliia Bielova and Fabio Massacci. Iterative enforcement by suppression: Towards practical enforcement theories. *Journal of Computer Security*, 20(1):51–79, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Baldwin:2010:AFI

- [BMBS10] Adrian Baldwin, Marco Casassa Mont, Yolanta Beres, and Simon Shiu. Assurance for federated identity management. *Journal of Computer Security*, 18(4):541–572, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bertino:1997:GEP

- [BMK97] Elisa Bertino, Emilio Montolivo, and Helmut Kurth. Guest editors' preface. *Journal of Computer Security*, 5(1):1–2, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bossi:2005:IFS

- [BMPR05] Annalisa Bossi, Damiano Macedonio, Carla Piazza, and Sabina Rossi. Information flow in secure contexts. *Journal of Computer Security*, 13(3):391–422, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Blundo:1995:MKD

- [BMS95] C. Blundo, Luiz A. Frota Mattos, and D. R. Stinson. Multiple key distribution maintaining user anonymity via broadcast channels. *Journal of Computer Security*, 3(4):309–322, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Boureau:2015:PPS

- [BMV15] Ioana Boureau, Aikaterini Mitrokotsa, and Serge Vaudenay. Practical and provably secure distance-bounding. *Journal of Computer Security*, 23(2):229–257, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Barthe:2007:SIF

- [BN07] Gilles Barthe and Leonor Prensa Nieto. Secure information flow for a concurrent language with scheduling. *Journal of Computer Security*, 15(6):647–689, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bertino:1995:EAM

- [BOS95] Elisa Bertino, Fabio Origgi, and Pierangela Samarati. An extended authorization model for object databases. *Journal of Computer Security*, 3(2–3):169–206, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bossi:2007:CIF

- [BPR07] Annalisa Bossi, Carla Piazza, and Sabina Rossi. Compositional information flow security for concurrent programs. *Journal of Computer Security*, 15(3):373–416, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Backes:2008:KDM

- [BPS08] Michael Backes, Birgit Pfitzmann, and Andre Scedrov. Key-dependent message security under active attacks — BRSIM/UC-soundness of Dolev–Yao-style encryption with key cycles. *Journal of Computer Security*, 16(5):497–530, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Backes:2004:PL

- [BPWS04] Michael Backes, Birgit Pfitzmann, Michael Waidner, and Michael Steiner. Polynomial liveness. *Journal of Computer Security*, 12(3–4):589–617, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Broadfoot:2004:EAW

- [BR04] P. J. Broadfoot and A. W. Roscoe. Embedding agents within the intruder to detect parallel attacks. *Journal of Computer Security*, 12(3–4):379–408, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bella:2005:GEP

- [BR05a] Giampaolo Bella and Peter Ryan. Guest Editors' preface. *Journal of Computer Security*, 13(5):697, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bugliesi:2005:NIP

- [BR05b] Michele Bugliesi and Sabina Rossi. Non-interference proof techniques for the analysis of cryptographic protocols. *Journal of Computer Security*, 13(1):87–113, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bella:2009:JCS

- [BR09] Giampaolo Bella and Peter Y. A. Ryan. *Journal of Computer Security*. *Journal of Computer Security*, 17(3):237, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Brose:2002:MAC

- [Bro02] Gerald Brose. Manageable access control for CORBA. *Journal of Computer Security*, 10(4):301–337, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bonatti:2002:UFR

- [BS02] Piero A. Bonatti and Pierangela Samarati. A uniform framework for regulating service access and information release on the Web. *Journal of Computer Security*, 10(3):241–271, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Buchholz:2004:PPO

- [BS04] Florian P. Buchholz and Clay Shields. Providing process origin information to aid in computer forensic investigations. *Journal of*

Computer Security, 12(5):753–776, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bhargav-Spantzel:2007:UCT

- [BSCGS07] Abhilasha Bhargav-Spantzel, Jan Camenisch, Thomas Gross, and Dieter Sommer. User centrality: A taxonomy and open issues. *Journal of Computer Security*, 15(5):493–527, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bertino:1997:SIS

- [BSR97] Elisa Bertino, Pierangela Samarati, and Gian Paolo Rossi. Special issue on security in the World Wide Web (WWW). *Journal of Computer Security*, 5(3):189–190, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bonatti:1997:MHS

- [BSS97] P. A. Bonatti, M. L. Sapino, and V. S. Subrahmanian. Merging heterogeneous security orderings. *Journal of Computer Security*, 5(1):3–29, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bhargav-Spantzel:2006:EPD

- [BSSB06] Abhilasha Bhargav-Spantzel, Anna C. Squicciarini, and Elisa Bertino. Establishing and protecting digital identity in federation systems. *Journal of Computer Security*, 14(3):269–300, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bhargav-Spantzel:2007:PPM

- [BSSM⁺07] Abhilasha Bhargav-Spantzel, Anna C. Squicciarini, Shimon Modi, Matthew Young, Elisa Bertino, and Stephen J. Elliott. Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security*, 15(5):529–560, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Blyth:2006:PRT

- [BT06] Andrew Blyth and Paula Thomas. Performing real-time threat assessment of security incidents using data fusion of IDS logs. *Journal of Computer Security*, 14(6):513–534, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Backes:2010:CSS

- [BU10] Michael Backes and Dominique Unruh. Computational soundness of symbolic zero-knowledge proofs. *Journal of Computer Security*,

18(6):1077–1155, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bohl:2016:SUC

[BU16] Florian Böhl and Dominique Unruh. Symbolic universal composability. *Journal of Computer Security*, 24(1):1–38, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Braun:2014:CTM

[BVC⁺14] Johannes Braun, Florian Volk, Jiska Classen, Johannes Buchmann, and Max Mühlhäuser. CA trust management for the Web PKI. *Journal of Computer Security*, 22(6):913–959, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Biskup:2008:PCQ

[BW08] Joachim Biskup and Lena Wiese. Preprocessing for controlled query evaluation with availability policy. *Journal of Computer Security*, 16(4):477–494, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Baudet:2010:GAC

[BWA10] Mathieu Baudet, Bogdan Warinschi, and Martín Abadi. Guessing attacks and the computational soundness of static equivalence. *Journal of Computer Security*, 18(5):909–968, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Bevier:1995:SBA

[BY95] William R. Bevier and William D. Young. A state-based approach to noninterference. *Journal of Computer Security*, 3(1):55–70, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Backes:2014:MGE

[BZ14] Michael Backes and Steve Zdancewic. Message from the Guest Editors. *Journal of Computer Security*, 22(5):659–660, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chadwick:2010:ICR

[CAB10] David W. Chadwick, Sean Antony, and Rune Bjerik. Instant certificate revocation and publication using WebDAV. *Journal of Computer Security*, 18(3):475–496, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Conrad:2010:AUT

- [CAFL10] James R. Conrad, Jim Alves-Foss, and Sauchi Stephen Lee. Analyzing uncertainty in TG protection graphs with TG/MC. *Journal of Computer Security*, 18(5):667–699, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Campolargo:2010:JSI

- [Cam10] Mário Campolargo. JCS special issue on EU-funded ICT research on trust and security: Foreword. *Journal of Computer Security*, 18(1):??, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cade:2015:PGI

- [CB15] David Cadé and Bruno Blanchet. Proved generation of implementations from computationally secure protocol specifications. *Journal of Computer Security*, 23(3):331–402, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cuppens:2013:FSM

- [CCBE13] Frédéric Cuppens, Nora Cuppens-Boulahia, and Yehia Elrakaiby. Formal specification and management of security policies with collective group obligations. *Journal of Computer Security*, 21(1):149–190, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cimato:2006:UMU

- [CCD06] Stelvio Cimato, Antonella Cresti, and Paolo D’Arco. A unified model for unconditionally secure key distribution. *Journal of Computer Security*, 14(1):45–64, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Casati:1998:EWA

- [CCF98] Fabio Casati, Silvana Castano, and Maria Grazia Fugini. Enforcing workflow authorization constraints using triggers. *Journal of Computer Security*, 6(4):257–285, 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Continella:2017:PAW

- [CCP⁺17] Andrea Continella, Michele Carminati, Mario Polino, Andrea Lanzi, Stefano Zanero, and Federico Maggi. Prometheus: Analyzing WebInject-based information stealers. *Journal of Computer*

Security, 25(2):117–137, 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cabuk:2010:TAS

- [CDE⁺10] Serdar Cabuk, Chris I. Dalton, Konrad Eriksson, Dirk Kuhlmann, HariGovind V. Ramasamy, Gianluca Ramunno, Ahmad-Reza Sadeghi, Matthias Schunter, and Christian Stübke. Towards automated security policy enforcement in multi-tenant virtual data centers. *Journal of Computer Security*, 18(1):89–121, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Castano:1997:ADG

- [CDF97] S. Castano, S. De Capitani di Vimercati, and M. G. Fugini. Automated derivation of global authorizations for database federations. *Journal of Computer Security*, 5(4):271–301, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Corin:2008:SCS

- [CDF⁺08] Ricardo Corin, Pierre-Malo Deniérou, Cédric Fournet, Karthikeyan Bhargavan, and James Leifer. A secure compiler for session abstractions. *Journal of Computer Security*, 16(5):573–636, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ciriani:2011:SDO

- [CDF⁺11] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Selective data outsourcing for enforcing privacy. *Journal of Computer Security*, 19(3):531–566, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ciriani:2012:OAE

- [CDF⁺12] Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, and Pierangela Samarati. An OBDD approach to enforce confidentiality and visibility constraints in data publishing. *Journal of Computer Security*, 20(5):463–508, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cervesato:2005:CBS

- [CDL⁺05] Iliano Cervesato, Nancy A. Durgin, Patrick D. Lincoln, John C. Mitchell, and Andre Scedrov. A comparison between strand spaces and multiset rewriting for security protocol analysis. *Journal of*

Computer Security, 13(2):265–316, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cortier:2006:SAP

- [CDL06] Véronique Cortier, Stéphanie Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chander:2004:RTM

- [CDM04] Ajay Chander, Drew Dean, and John C. Mitchell. Reconstructing trust management. *Journal of Computer Security*, 12(1):131–164, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Costa:2012:MPS

- [CDM12] Gabriele Costa, Pierpaolo Degano, and Fabio Martinelli. Modular plans for secure service composition. *Journal of Computer Security*, 20(1):81–117, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Clarke:2001:CCD

- [CEE⁺01] Dwaine Clarke, Jean-Emile Elie, Carl Ellison, Matt Fredette, Alexander Morcos, and Ronald L. Rivest. Certificate chain discovery in SPKI/SDSI. *Journal of Computer Security*, 9(4):285–322, 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Corin:2007:TAS

- [CEHM07] R. Corin, S. Etalle, P. H. Hartel, and A. Mader. Timed analysis of security protocols. *Journal of Computer Security*, 15(6):619–645, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Centenaro:2013:TBA

- [CFL13] Matteo Centenaro, Riccardo Focardi, and Flaminia L. Luccio. Type-based analysis of key management in PKCS#11 cryptographic devices. *Journal of Computer Security*, 21(6):971–1007, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Candebat:2006:SPM

- [CG06] Thibault Candebat and David Gray. Secure pseudonym management using mediated identity-based encryption. *Journal of Computer Security*, 14(3):249–267, ??? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Curtmola:2011:SSE

- [CGKO11] Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. *Journal of Computer Security*, 19(5):895–934, ??? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Crampton:2017:BOW

- [CGKW17] Jason Crampton, Gregory Gutin, Daniel Karapetyan, and Rémi Watrigant. The bi-objective workflow satisfiability problem and workflow resiliency. *Journal of Computer Security*, 25(1):83–115, ??? 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Campbell:2003:ECP

- [CGLZ03] Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3):431–448, ??? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chen:1995:DTA

- [CGM95] Liqun Chen, Dieter Gollmann, and Christopher J. Mitchell. Distributing trust amongst multiple authentication servers. *Journal of Computer Security*, 3(4):255–267, ??? 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Clark:2007:SAQ

- [CHM07] David Clark, Sebastian Hunt, and Pasquale Malacaria. A static analysis for quantifying information flow in a simple imperative language. *Journal of Computer Security*, 15(3):321–371, ??? 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chong:2012:RIR

- [Cho12] Stephen Chong. Required information release. *Journal of Computer Security*, 20(6):637–676, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chuang:1996:SAN

- [Chu96] Shaw-Cheng Chuang. Securing ATM networks. *Journal of Computer Security*, 4(4):289–329, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cheng:2017:SFN

- [CLD⁺17] Yao Cheng, Yingjiu Li, Robert Deng, Lingyun Ying, and Wei He. A study on a feasible no-root approach on Android. *Journal of Computer Security*, 25(3):231–253, 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Clifton:2000:USS

- [Cli00] Chris Clifton. Using sample size to limit exposure to data mining. *Journal of Computer Security*, 8(4):281–307, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cho:2004:GKR

- [CLK04] Taenam Cho, Sang-Ho Lee, and Won Kim. A group key recovery mechanism based on logical key hierarchy. *Journal of Computer Security*, 12(5):711–736, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Camenisch:2010:JSI

- [CLM⁺10] Jan Camenisch, Javier Lopez, Fabio Massacci, Massimo Ciccato, and Thomas Skordas. JCS special issue on EU-funded ICT research on trust and security. *Journal of Computer Security*, 18(1):1–5, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Casola:2007:PBM

- [CMMV07] Valentina Casola, Antonino Mazzeo, Nicola Mazzocca, and Valeria Vittorini. A policy-based methodology for security evaluation: A security metric for public key infrastructures. *Journal of Computer Security*, 15(2):197–229, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chatzikokolakis:2014:FAS

- [CMPP14] Konstantinos Chatzikokolakis, Sebastian Alexander Mödersheim, Catuscia Palamidessi, and Jun Pang. Foundational aspects of security. *Journal of Computer Security*, 22(2):201–202, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Camenisch:1997:DPS

- [CMS97] Jan Camenisch, Ueli Maurer, and Markus Stadler. Digital payment systems with passive anonymity-revoking trustees. *Journal of Computer Security*, 5(1):69–89, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Clarkson:2009:QIF

- [CMS09] Michael R. Clarkson, Andrew C. Myers, and Fred B. Schneider. Quantifying information flow with beliefs. *Journal of Computer Security*, 17(5):655–701, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Carter:2016:SOG

- [CMTB16] Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure outsourced garbled circuit evaluation for mobile devices. *Journal of Computer Security*, 24(2):137–180, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cohen:2003:FOV

- [Coh03] Ernie Cohen. First-order verification of cryptographic protocols. *Journal of Computer Security*, 11(2):189–216, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chatzikokolakis:2008:BRI

- [CPP08] Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Prakash Panangaden. On the Bayes risk in information-hiding protocols. *Journal of Computer Security*, 16(5):531–571, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chan:2007:SSI

- [CPPS07] Haowen Chan, Adrian Perrig, Bartosz Przydatek, and Dawn Song. SIA: Secure information aggregation in sensor networks. *Journal of Computer Security*, 15(1):69–102, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Collberg:2005:SWF

- [CS05] Christian Collberg and Tapas Ranjan Sahoo. Software watermarking in the frequency domain: Implementation, analysis, and attacks. *Journal of Computer Security*, 13(5):721–755, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Clarkson:2010:H

- [CS10] Michael R. Clarkson and Fred B. Schneider. Hyperproperties. *Journal of Computer Security*, 18(6):1157–1210, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cortier:2013:AFH

- [CS13] Véronique Cortier and Ben Smyth. Attacking and fixing Helios: An analysis of ballot secrecy. *Journal of Computer Security*, 21(1):89–148, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cheng:2009:QAV

- [CT09] Weiwei Cheng and Kian-Lee Tan. Query assurance verification for outsourced multi-dimensional databases. *Journal of Computer Security*, 17(1):101–126, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cuppens:2002:GEP

- [Cup02] Frédéric Cuppens. Guest editor’s preface. *Journal of Computer Security*, 10(4):299–300, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Cortier:2017:FAN

- [CW17] Véronique Cortier and Cyrille Wiedling. A formal analysis of the Norwegian E-voting protocol. *Journal of Computer Security*, 25(1):21–57, 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chen:2014:PUQ

- [CWT14] Yen-Chung Chen, Yu-Sung Wu, and Wen-Guey Tzeng. Preserving user query privacy in cloud-based security services. *Journal of Computer Security*, 22(6):997–1024, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Choo:2017:DOS

- [CYC17] Euijin Choo, Ting Yu, and Min Chi. Detecting opinion spammer groups and spam targets through community discovery and sentiment analysis. *Journal of Computer Security*, 25(3):283–318, ??? 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Chen:2016:PEP

- [CZ16] Yu Chen and Zongyang Zhang. Publicly evaluable pseudorandom functions and their applications. *Journal of Computer Security*, 24(2):289–320, ??? 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

deAmorim:2016:VIF

- [dACD⁺16] Arthur Azevedo de Amorim, Nathan Collins, André DeHon, Delphine Demange, Cătălin Hrițcu, David Pichardie, Benjamin C. Pierce, Randy Pollack, and Andrew Tolmach. A verified information-flow architecture. *Journal of Computer Security*, 24(6):689–734, ??? 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Damiani:2008:GE

- [Dam08] Ernesto Damiani. Guest editorial. *Journal of Computer Security*, 16(4):367–368, ??? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DeAngelis:2011:SAT

- [DB11] David DeAngelis and K. Suzanne Barber. Security applications of trust in multi-agent systems. *Journal of Computer Security*, 19(1):57–99, ??? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

dAusbourg:1996:CCD

- [dC96] Bruno d’Ausbourg and Christel Calas. Controlling causal dependencies over a secure network. *Journal of Computer Security*, 4(1):3–25, ??? 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DiCrescenzo:2016:PPP

- [DCMP16] Giovanni Di Crescenzo, Debra L. Cook, Allen McIntosh, and Euthimios Panagos. Practical and privacy-preserving information retrieval from a database table. *Journal of Computer Security*, 24(4):

479–506, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dreier:2015:BFP

- [DDL15] Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. Brandt’s fully private auction protocol revisited. *Journal of Computer Security*, 23(5):587–610, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Datta:2005:DSC

- [DDMP05] Anupam Datta, Ante Derek, John C. Mitchell, and Dusko Pavlovic. A derivation system and compositional logic for security protocols. *Journal of Computer Security*, 13(3):423–482, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DeGroef:2014:SME

- [DDNP14] Willem De Groef, Dominique Devriese, Nick Nikiforakis, and Frank Piessens. Secure multi-execution of web scripts: Theory and practice. *Journal of Computer Security*, 22(4):469–509, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DeCapitanidiVimercati:2011:AED

- [DFJ⁺11] Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Authorization enforcement in distributed query evaluation. *Journal of Computer Security*, 19(4):751–794, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DeCapitanidiVimercati:2015:LAI

- [DFJ⁺15] Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Giovanni Livraga, Stefano Paraboschi, and Pierangela Samarati. Loose associations to increase utility in data publishing. *Journal of Computer Security*, 23(1):59–88, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DeCapitanidiVimercati:2016:EIC

- [DFJ⁺16] Sabrina De Capitani di Vimercati, Sara Foresti, Sushil Jajodia, Stefano Paraboschi, and Pierangela Samarati. Efficient integrity checks for join queries in the cloud. *Journal of Computer Security*, 24(3):347–378, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DeCapitanidiVimercati:2013:SCM

- [DFP⁺13] Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Gerardo Pelosi, and Pierangela Samarati. Supporting concurrency and multiple indexes in private access to outsourced data. *Journal of Computer Security*, 21(3):425–461, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Degano:2013:P

- [DG13] Pierpaolo Degano and Joshua D. Guttman. Preface. *Journal of Computer Security*, 21(6):779–780, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dupressoir:2014:GGP

- [DGJN14] François Dupressoir, Andrew D. Gordon, Jan Jürjens, and David A. Naumann. Guiding a general-purpose C verifier to prove cryptographic protocols. *Journal of Computer Security*, 22(5):823–866, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Devanbu:2004:FAX

- [DGK⁺04] Premkumar Devanbu, Michael Gertz, April Kwong, Charles Martel, Glen Nuckolls, and Stuart G. Stubblebine. Flexible authentication of XML documents. *Journal of Computer Security*, 12(6):841–864, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Devanbu:2003:ADP

- [DGMS03] Premkumar Devanbu, Michael Gertz, Charles Martel, and Stuart G. Stubblebine. Authentic data publication over the Internet. *Journal of Computer Security*, 11(3):291–314, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DSouza:2011:MCT

- [DHRS11] Deepak D’Souza, Raveendra Holla, K. R. Raghavendra, and Barbara Sprick. Model-checking trace-based information flow properties. *Journal of Computer Security*, 19(1):101–138, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DiPierro:2004:ANI

- [DHW04] Alessandra Di Pierro, Chris Hankin, and Herbert Wiklicky. Approximate non-interference. *Journal of Computer Security*, 12(1):

37–81, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dam:2010:PCI

- [DJLP10] Mads Dam, Bart Jacobs, Andreas Lundblad, and Frank Piessens. Provably correct inline monitoring for multithreaded Java-like programs. *Journal of Computer Security*, 18(1):37–59, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Desmet:2014:P

- [DJLS14] Lieven Desmet, Martin Johns, Benjamin Livshits, and Andrei Sabelfeld. Preface. *Journal of Computer Security*, 22(4):467–468, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Delaune:2009:VPT

- [DKR09] Stéphanie Delaune, Steve Kremer, and Mark Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4):435–487, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Delaune:2010:SBA

- [DKR10] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Symbolic bisimulation for the applied pi calculus. *Journal of Computer Security*, 18(2):317–377, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Delaune:2010:FSA

- [DKS10] Stéphanie Delaune, Steve Kremer, and Graham Steel. Formal security analysis of PKCS#11 and proprietary extensions. *Journal of Computer Security*, 18(6):1211–1245, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Durgin:2004:MRC

- [DLMS04] Nancy Durgin, Patrick Lincoln, John Mitchell, and Andre Scedrov. Multiset rewriting and the complexity of bounded security protocols. *Journal of Computer Security*, 12(2):247–311, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DeCapitanidiVimercati:2001:GIP

- [DLRS01] Sabrina De Capitani di Vimercati, Patrick Lincoln, Livio Ricciulli, and Pierangela Samarati. Global infrastructure protection system.

Journal of Computer Security, 9(4):251–283, 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Deng:2011:ZKB

- [DLYZ11] Robert H. Deng, Yingjiu Li, Moti Yung, and Yunlei Zhao. A zero-knowledge based framework for RFID privacy. *Journal of Computer Security*, 19(6):1109–1146, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Deswarte:2000:GEP

- [DM00] Yves Deswarte and Catherine Meadows. Guest editors' preface. *Journal of Computer Security*, 8(2–3):87, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DiPietro:2004:KMH

- [DMM04] Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei. Key management for high bandwidth secure multicast. *Journal of Computer Security*, 12(5):693–709, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DiPietro:2010:HKS

- [DMM10] Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei. Hierarchies of keys in secure multicast communications. *Journal of Computer Security*, 18(5):839–860, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Durgin:2003:CLP

- [DMP03] Nancy Durgin, John Mitchell, and Dusko Pavlovic. A compositional logic for proving security properties of protocols. *Journal of Computer Security*, 11(4):677–721, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dimitrakakis:2015:ELA

- [DMV15] Christos Dimitrakakis, Aikaterini Mitrokotsa, and Serge Vaudenay. Expected loss analysis for authentication in constrained channels. *Journal of Computer Security*, 23(3):309–329, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dainotti:2009:CAA

- [DPV09] Alberto Dainotti, Antonio Pescapé, and Giorgio Ventre. A cascade architecture for DoS attacks detection based on the wavelet transform. *Journal of Computer Security*, 17(6):945–968, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DSouza:2016:MCT

- [DR16] Deepak D'Souza and K. R. Raghavendra. Model-checking trace-based information flow properties for infinite-state systems. *Journal of Computer Security*, 24(5):617–643, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dong:2011:SSE

- [DRD11] Changyu Dong, Giovanni Russello, and Naranker Dulay. Shared and searchable encrypted data for untrusted servers. *Journal of Computer Security*, 19(3):367–397, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Dewri:2011:EPV

- [DRRW11] Rinku Dewri, Indrajit Ray, Indrakshi Ray, and Darrell Whitley. Exploring privacy versus data quality trade-offs in anonymization techniques using multi-objective optimization. *Journal of Computer Security*, 19(5):935–974, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

DeCapitanidiVimercati:1997:ASE

- [DS97] Sabrina De Capitani di Vimercati and Pierangela Samarati. Authorization specification and enforcement in federated database systems. *Journal of Computer Security*, 5(2):155–188, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Daniels:1999:IHA

- [DS99] Thomas E. Daniels and Eugene H. Spafford. Identification of host audit data to detect attacks on low-level IP vulnerabilities. *Journal of Computer Security*, 7(1):3–35, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

dosSantos:2017:AFE

- [dSRCP17] Daniel Ricardo dos Santos, Silvio Ranise, Luca Compagna, and Serena Elisa Ponta. Automatically finding execution scenarios to deploy security-sensitive workflows. *Journal of Computer Security*, 25(3):255–282, 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Demurjian:1997:TDP

- [DT97] S. A. Demurjian Sr. and T. C. Ting. Towards a definitive paradigm for security in object-oriented systems and applications. *Journal*

of *Computer Security*, 5(4):341–382, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Davidson:2016:CSS

- [DTG16] Michal Davidson, Tamir Tassa, and Ehud Gudes. Content sharing schemes in DRM systems with enhanced performance and privacy preservation. *Journal of Computer Security*, 24(6):667–688, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ding:2009:LFM

- [DTX09] Xuhua Ding, Gene Tsudik, and Shouhuai Xu. Leak-free mediated group signatures. *Journal of Computer Security*, 17(4):489–514, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Duggan:2004:TBC

- [Dug04] Dominic Duggan. Type-based cryptographic operations. *Journal of Computer Security*, 12(3–4):485–550, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Elbirt:2008:AAI

- [Elb08] A. J. Elbirt. Accelerated AES implementations via generalized instruction set extensions. *Journal of Computer Security*, 16(3):265–288, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Epstein:1993:HAW

- [EMO⁺93] Jeremy Epstein, John McHugh, Hilarie Orman, Rita Pascale, Ann Marmor-Squires, Bonnie Danner, Charles R. Martin, Martha Branstad, Glenn Benson, and Doug Rothnie. A high assurance window system prototype. *Journal of Computer Security*, 2(2–3):159–190, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Eamani:2006:LBP

- [ES06] Arun K. Eamani and A. Prasad Sistla. Language based policy analysis in a SPKI trust management system. *Journal of Computer Security*, 14(4):327–357, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Eckmann:2002:SAL

- [EVK02] Steven T. Eckmann, Giovanni Vigna, and Richard A. Kemmerer. STATL: An attack language for state-based intrusion detection. *Journal of Computer Security*, 10(1–2):71–103, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Foley:2011:MSP

- [FF11] Simon N. Foley and William M. Fitzgerald. Management of security policy configuration using a Semantic Threat Graph approach. *Journal of Computer Security*, 19(3):567–605, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Focardi:1995:CSP

- [FG95] Riccardo Focardi and Roberto Gorrieri. A classification of security properties for process algebras. *Journal of Computer Security*, 3(1):5–33, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Fabrega:1999:SSP

- [FHG99] F. Javier Thayer Fábrega, Jonathan C. Herzog, and Joshua D. Guttman. Strand spaces: proving security protocols correct. *Journal of Computer Security*, 7(2–3):191–230, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Foley:1995:SSC

- [FJ95] Simon N. Foley and Jeremy L. Jacob. Specifying security for computer supported collaborative working. *Journal of Computer Security*, 3(4):233–253, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Franklin:1998:AML

- [FM98] Matthew K. Franklin and Dahlia Malkhi. Auditable metering with lightweight security. *Journal of Computer Security*, 6(4):237–255, 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Focardi:2005:GEP

- [Foc05] Riccardo Focardi. Guest editor’s preface. *Journal of Computer Security*, 13(3):345, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Focardi:2006:P

- [Foc06] Riccardo Focardi. Preface. *Journal of Computer Security*, 14(2):111, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Focardi:2010:E

- [Foc10] Riccardo Focardi. Editorial. *Journal of Computer Security*, 18(6):969, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Foley:1992:ASN

- [Fol92] Simon N. Foley. Aggregation and separation as noninterference properties. *Journal of Computer Security*, 1(2):159–188, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Foley:1998:GEP

- [Fol98] Simon N. Foley. Guest editors' preface. *Journal of Computer Security*, 6(1–2):1, 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Foley:1999:GEP

- [Fol99] Simon N. Foley. Guest editor's preface. *Journal of Computer Security*, 7(2–3):87, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Focardi:2006:IFS

- [FR06] Riccardo Focardi and Sabina Rossi. Information flow security in dynamic contexts. *Journal of Computer Security*, 14(1):65–110, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Frincke:2002:GEP

- [Fri02] Deborah Frincke. Guest editor's preface. *Journal of Computer Security*, 10(1–2):1–3, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Geigel:2013:NNT

- [Gei13] Arturo Geigel. Neural network Trojan. *Journal of Computer Security*, 21(2):191–232, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gray:1998:PSC

- [GEL98] James W. Gray III, Kin Fai Epsilon Ip, and King-Shan Lui. Provable security for cryptographic protocols — exact analysis and engineering applications. *Journal of Computer Security*, 6(1–2): 23–52, 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gupta:1992:TTP

- [GG92] Sarbari Gupta and Virgil D. Gligor. Towards a theory of penetration-resistant systems and its applications. *Journal of Computer Security*, 1(2):133–158, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Grothoff:2009:TBS

- [GGS⁺09] Christian Grothoff, Krista Grothoff, Ryan Stutsman, Ludmila Alkhutova, and Mikhail Atallah. Translation-based steganography. *Journal of Computer Security*, 17(3):269–303, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gentry:2013:FSB

- [GHPS13] Craig Gentry, Shai Halevi, Chris Peikert, and Nigel P. Smart. Field switching in BGV-style homomorphic encryption. *Journal of Computer Security*, 21(5):663–684, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guttman:2005:VIF

- [GHR05] Joshua D. Guttman, Amy L. Herzog, John D. Ramsdell, and Clement W. Skorupka. Verifying information flow goals in Security-Enhanced Linux. *Journal of Computer Security*, 13(1): 115–134, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gordon:2003:ATS

- [GJ03] Andrew D. Gordon and Alan Jeffrey. Authenticity by typing for security protocols. *Journal of Computer Security*, 11(4):451–519, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gordon:2004:TEA

- [GJ04] Andrew D. Gordon and Alan Jeffrey. Types and effects for asymmetric cryptographic protocols. *Journal of Computer Security*, 12

(3–4):435–483, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Goubault-Larrecq:2010:FMF

[GL10] Jean Goubault-Larrecq. Finite models for formal security proofs. *Journal of Computer Security*, 18(6):1247–1299, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gligor:1993:IRA

[GLP93] Virgil D. Gligor, Shyh-Wei Luan, and Joseph N. Pato. On inter-realm authentication in large distributed systems. *Journal of Computer Security*, 2(2–3):137–157, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gordon:2011:IIS

[GLZ11] Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1):33–56, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Giacobazzi:2010:ACU

[GM10] Roberto Giacobazzi and Isabella Mastroeni. Adjoining classified and unclassified information by abstract interpretation. *Journal of Computer Security*, 18(5):751–797, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gritzalis:2011:SPM

[GMR⁺11] Dimitris Gritzalis, Giannis Marias, Yacine Rebahi, Yannis Soupionis, and Sven Ehlert. SPIDER: A platform for managing SIP-based Spam over Internet Telephony (SPIT). *Journal of Computer Security*, 19(5):835–867, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guanciale:2016:PSM

[GNDB16] Roberto Guanciale, Hamed Nemati, Mads Dam, and Christoph Baumann. Provably secure memory isolation for Linux on ARM. *Journal of Computer Security*, 24(6):793–837, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gong:1995:GEP

[Gon95] Li Gong. Guest Editor’s preface. *Journal of Computer Security*, 3(1):3, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gorrieri:2005:GEP

- [Gor05] Roberto Gorrieri. Guest editor's preface. *Journal of Computer Security*, 13(1):1–2, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Goto:2006:P

- [Got06] Atsuhiko Goto. Preface. *Journal of Computer Security*, 14(3):247, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Goto:2007:P

- [Got07] Atsuhiko Goto. Preface. *Journal of Computer Security*, 15(5):491, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Goto:2010:P

- [Got10] Atsuhiko Goto. Preface. *Journal of Computer Security*, 18(4):497, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gudes:1999:MSI

- [GOvdR99] Ehud Gudes, Martin S. Olivier, and Reind P. van de Riet. Modelling, specifying and implementing workflow security in Cyberspace. *Journal of Computer Security*, 7(4):287–315, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gorla:2010:P

- [GP10] Daniele Gorla and Catuscia Palamidessi. Preface. *Journal of Computer Security*, 18(2):189, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Garg:2012:SAL

- [GP12] Deepak Garg and Frank Pfenning. Stateful authorization logic — proof theory and a case study. *Journal of Computer Security*, 20(4):353–391, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gray:1992:TMF

- [Gra92] James W. Gray III. Toward a mathematical foundation for information flow security. *Journal of Computer Security*, 1(3–4):255–294, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gritzalis:2011:GEP

- [Gri11] Dimitris Gritzalis. Guest Editor’s preface. *Journal of Computer Security*, 19(6):1027–1028, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Gibson-Robinson:2015:VLS

- [GRKL15] Thomas Gibson-Robinson, Allaa Kamil, and Gavin Lowe. Verifying layered security protocols. *Journal of Computer Security*, 23(3):259–307, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guan:2017:SKE

- [GT17] Albert Guan and Wen-Guey Tzeng. A secret key establishment protocol for wireless networks using noisy channels. *Journal of Computer Security*, 25(2):139–151, 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Goodrich:2008:NFI

- [GTY08] Michael T. Goodrich, Roberto Tamassia, and Danfeng (Daphne) Yao. Notarized federated ID management and authentication. *Journal of Computer Security*, 16(4):399–418, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guttman:2004:FAP

- [GTZ04] Joshua D. Guttman, F. Javier Thayer, and Lenore D. Zuck. The faithfulness of abstract protocol analysis: Message authentication. *Journal of Computer Security*, 12(6):865–891, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guette:2009:ATK

- [Gue09] Gilles Guette. Automating trusted key rollover in DNSSEC. *Journal of Computer Security*, 17(6):839–854, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guttman:2004:GEP

- [Gut04a] Joshua Guttman. Guest editor’s preface. *Journal of Computer Security*, 12(1):1, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guttman:2004:ATD

- [Gut04b] Joshua D. Guttman. Authentication tests and disjoint encryption: A design method for security protocols. *Journal of Computer Se-*

curity, 12(3–4):409–433, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guttman:2009:I

- [Gut09] Joshua D. Guttman. Introduction. *Journal of Computer Security*, 17(5):515, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Guttman:2014:EPP

- [Gut14] Joshua D. Guttman. Establishing and preserving protocol security goals. *Journal of Computer Security*, 22(2):203–267, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Halpern:2017:QQP

- [Hal17] Joseph Y. Halpern. From qualitative to quantitative proofs of security properties using first-order conditional logic. *Journal of Computer Security*, 25(1):1–19, 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hancke:2011:PES

- [Han11] Gerhard P. Hancke. Practical eavesdropping and skimming attacks on high-frequency RFID tokens. *Journal of Computer Security*, 19(2):259–288, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hedin:2016:IFS

- [HBS16] Daniel Hedin, Luciano Bello, and Andrei Sabelfeld. Information-flow security for JavaScript and its APIs. *Journal of Computer Security*, 24(2):181–234, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Horton:1993:CVP

- [HCH⁺93] J. D. Horton, R. H. Cooper, W. F. Hyslop, B. G. Nickerson, O. K. Ward, Robert Harland, Elton Ashby, and W. M. Stewart. The cascade vulnerability problem. *Journal of Computer Security*, 2(4):279–290, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hsu:2011:WLC

- [HCM11] Francis Hsu, Hao Chen, and Sridhar Machiraju. WebCallerID: Leveraging cellular networks for Web authentication. *Journal of Computer Security*, 19(5):869–893, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hinke:1995:FAD

- [HDC95] Thomas H. Hinke, Harry S. Delugach, and Asha Chandrasekhar. A fast algorithm for detecting second paths in database inference analysis. *Journal of Computer Security*, 3(2–3):147–168, ??? 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Herzberg:2009:FPT

- [Her09] Amir Herzberg. Folklore, practice and theory of robust combiners. *Journal of Computer Security*, 17(2):159–189, ??? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hofmeyr:1998:IDU

- [HFS98] Steven A. Hofmeyr, Stephanie Forrest, and Anil Somayaji. Intrusion detection using sequences of system calls. *Journal of Computer Security*, 6(3):151–180, ??? 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Harrison:2009:AIF

- [HH09] William L. Harrison and James Hook. Achieving information flow security through monadic control of effects. *Journal of Computer Security*, 17(5):599–653, ??? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hauser:1996:RSP

- [HJT+96] Ralf Hauser, Philippe Janson, Gene Tsudik, Els Van Herreweghen, and Refik Molva. Robust and secure password and key change method. *Journal of Computer Security*, 4(1):97–111, ??? 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hui:2001:FPS

- [HL01] Mei Lin Hui and Gavin Lowe. Fault-preserving simplifying transformations for security protocols. *Journal of Computer Security*, 9(1–2):3–46, ??? 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Heather:2003:HPT

- [HLS03] James Heather, Gavin Lowe, and Steve Schneider. How to prevent type flaw attacks on security protocols. *Journal of Computer Security*, 11(2):217–244, ??? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

He:2011:SCP

- [HLVA11] Xiaoyun He, Haibing Lu, Jaideep Vaidya, and Nabil Adam. Secure construction and publication of contingency tables from distributed data. *Journal of Computer Security*, 19(3):453–484, ??? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hamadou:2010:CPS

- [HM10] Sardaouna Hamadou and John Mullins. Calibrating the power of schedulers for probabilistic polynomial-time calculus. *Journal of Computer Security*, 18(2):265–316, ??? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Herzberg:2013:FJL

- [HM13] Amir Herzberg and Ronen Margulies. Forcing Johnny to login safely. *Journal of Computer Security*, 21(3):393–424, ??? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hofheinz:2009:PRS

- [HMQU09] Dennis Hofheinz, Jörn Müller-Quade, and Dominique Unruh. Polynomial runtime in simulatability definitions. *Journal of Computer Security*, 17(5):703–735, ??? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Heiderich:2014:SAS

- [HNS⁺14] M. Heiderich, M. Niemietz, F. Schuster, T. Holz, and J. Schwenk. Scriptless attacks: Stealing more pie without touching the sill. *Journal of Computer Security*, 22(4):567–599, ??? 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Halpern:2005:AIH

- [HO05] Joseph Y. Halpern and Kevin R. O’Neill. Anonymity and information hiding in multiagent systems. *Journal of Computer Security*, 13(3):483–514, ??? 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Horn:2000:APF

- [HP00] Günther Horn and Bart Preneel. Authentication and payment in future mobile systems. *Journal of Computer Security*, 8(2–3):183–207, ??? 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hale:2003:PAC

- [HPS03] John Hale, Mauricio Papa, and Sujeet Shenoi. Programmable access control. *Journal of Computer Security*, 11(3):331–351, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hughes:2004:IHA

- [HS04] Dominic Hughes and Vitaly Shmatikov. Information hiding, anonymity and privacy: a modular approach. *Journal of Computer Security*, 12(1):3–36, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Heather:2005:DPE

- [HS05] James Heather and Steve Schneider. A decision procedure for the existence of a rank function. *Journal of Computer Security*, 13(2):317–344, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Halevi:2011:TBH

- [HSH11] Tzipora Halevi, Nitesh Saxena, and Shai Halevi. Tree-based HB protocols for privacy-preserving authentication of RFID tags. *Journal of Computer Security*, 19(2):343–363, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hagen:2008:PAU

- [HSR08] Janne Merete Hagen, Tormod Kalberg Sivertsen, and Chunming Rong. Protection against unauthorized access and computer crime in Norwegian enterprises. *Journal of Computer Security*, 16(3):341–366, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hu:2009:CRR

- [HTML09] Nan Hu, Giri K. Tayi, Chengyu Ma, and Yingjiu Li. Certificate revocation release policies. *Journal of Computer Security*, 17(2):127–157, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hale:2000:TBA

- [HTS00] John Hale, Jody Threet, and Sujeet Shenoi. A ticket-based access control architecture for object systems. *Journal of Computer Security*, 8(1):43–65, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hu:1992:RTC

- [Hu92] Wei-Ming Hu. Reducing timing channels with fuzzy time. *Journal of Computer Security*, 1(3–4):233–254, ??? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Halpern:2001:LSL

- [HvdM01] Joseph Y. Halpern and Ron van der Meyden. A logic for SDSI's linked local name spaces. *Journal of Computer Security*, 9(1–2):105–142, ??? 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Halpern:2003:LRS

- [HvdM03] Joseph Y. Halpern and Ron van der Meyden. A logical reconstruction of SPKI. *Journal of Computer Security*, 11(4):581–613, ??? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Hong:2012:SED

- [HVL12] Yuan Hong, Jaideep Vaidya, and Haibing Lu. Secure and efficient distributed linear programming. *Journal of Computer Security*, 20(5):583–634, ??? 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Homer:2013:AVM

- [HZO⁺13] John Homer, Su Zhang, Xinming Ou, David Schmidt, Yanhui Du, S. Raj Rajagopalan, and Anoop Singhal. Aggregating vulnerability metrics in enterprise networks using attack graphs. *Journal of Computer Security*, 21(4):561–597, ??? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Iheagwara:2003:CEE

- [IBS03] Charles Iheagwara, Andrew Blyth, and Mukesh Singhal. A comparative experimental evaluation study of intrusion detection system performance in a gigabit environment. *Journal of Computer Security*, 11(1):1–33, ??? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Iheagwara:2004:CEM

- [IBS04] Charles Iheagwara, Andrew Blyth, and Mukesh Singhal. Cost effective management frameworks for intrusion detection systems. *Journal of Computer Security*, 12(5):777–798, ??? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jacob:1992:BTB

- [Jac92] Jeremy Jacob. Basic theorems about security. *Journal of Computer Security*, 1(3–4):385–411, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jing:2016:TML

- [JAH⁺16] Yiming Jing, Gail-Joon Ahn, Hongxin Hu, Haehyun Cho, and Ziming Zhao. TripleMon: A multi-layer security framework for mediating inter-process communication on Android. *Journal of Computer Security*, 24(4):405–426, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:2001:MST

- [JAK⁺01] Sushil Jajodia, Vijayalakshmi Atluri, Thomas F. Keefe, Catherine D. McCollum, and Ravi Mukkamala. Multilevel secure transaction processing. *Journal of Computer Security*, 9(3):165–195, 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jadliwala:2013:OMZ

- [JBH13] Murtuza Jadliwala, Igor Bilogrevic, and Jean-Pierre Hubaux. Optimizing mix-zone coverage in pervasive wireless networks. *Journal of Computer Security*, 21(3):317–346, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:2002:GEP

- [JG02] Sushil Jajodia and Dimitris Gritzalis. Guest editors' preface. *Journal of Computer Security*, 10(3):211, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jacobs:2009:SLS

- [JH09] Bart Jacobs and Ichiro Hasuo. Semantics and logic for security protocols. *Journal of Computer Security*, 17(6):909–944, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jiwa:1996:BAD

- [JHS96] Azad Jiwa, Thomas Hardjono, and Jennifer Seberry. Beacons for authentication in distributed systems. *Journal of Computer Security*, 4(1):81–96, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jovanovic:2010:SAD

- [JKK10] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Static analysis for detecting taint-style vulnerabilities in web applications. *Journal of Computer Security*, 18(5):861–907, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:1992:EPa

- [JM92a] Sushil Jajodia and Jonathan Millen. Editors' preface. *Journal of Computer Security*, 1(1):1–3, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:1992:EPb

- [JM92b] Sushil Jajodia and Jonathan Millen. Editors' preface. *Journal of Computer Security*, 1(3–4):215, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:1993:EPa

- [JM93] Sushil Jajodia and Jonathan Millen. Editors' preface. *Journal of Computer Security*, 2(2–3):85, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:1995:EPa

- [JM95a] Sushil Jajodia and Jonathan Millen. Editors' preface. *Journal of Computer Security*, 3(1):1, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:1995:EPc

- [JM95b] Sushil Jajodia and Jonathan Millen. Editors' preface. *Journal of Computer Security*, 3(4):231, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:1996:EPa

- [JM96a] Sushil Jajodia and Jonathan Millen. Editors' preface. *Journal of Computer Security*, 4(2–3):121, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:1996:EPb

- [JM96b] Sushil Jajodia and Jonathan Millen. Editors' preface. *Journal of Computer Security*, 4(4):265, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:1997:EP

- [JM97] Sushil Jajodia and Jonathan Millen. Editors' preface. *Journal of Computer Security*, 5(2):109, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:2010:E

- [JM10] Sushil Jajodia and Jon Millen. Editorial. *Journal of Computer Security*, 18(2):187, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jajodia:2016:UTP

- [JPSS16] Sushil Jajodia, Noseong Park, Edoardo Serra, and V. S. Subrahmanian. Using temporal probabilistic logic for optimal monitoring of security events with limited resources. *Journal of Computer Security*, 24(6):735–791, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Jha:2004:MCS

- [JR04] S. Jha and T. Reps. Model checking SPKI/SDSI. *Journal of Computer Security*, 12(3–4):317–353, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kayem:2008:RCK

- [KAM08] Anne V. D. M. Kayem, Selim G. Akl, and Patrick Martin. On replacing cryptographic keys in hierarchical key management systems. *Journal of Computer Security*, 16(3):289–309, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Karjoth:2000:ACS

- [Kar00] Günter Karjoth. Authorization in CORBA security. *Journal of Computer Security*, 8(2–3):89–108, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kopf:2011:ADI

- [KB11] Boris Köpf and David Basin. Automatically deriving information-theoretic bounds for adaptive side-channel attacks. *Journal of Computer Security*, 19(1):1–31, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kakkar:2003:RAS

- [KGA03] Pankaj Kakkar, Carl A. Gunter, and Martín Abadi. Reasoning about secrecy for active networks. *Journal of Computer Security*,

11(2):245–287, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kang:1995:TMM

- [KK95] I. E. Kang and T. F. Keefe. Transaction management for multilevel secure replicated databases. *Journal of Computer Security*, 3(2–3):115–145, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kremer:2016:AAS

- [KK16] Steve Kremer and Robert Künnemann. Automated analysis of security protocols with global state. *Journal of Computer Security*, 24(5):583–616, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kamil:2011:ATS

- [KL11] Allaa Kamil and Gavin Lowe. Analysing TLS in the strand spaces model. *Journal of Computer Security*, 19(5):975–1025, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Knudsen:1998:SMD

- [KM98] Lars R. Knudsen and Keith M. Martin. In search of multiple domain key recovery. *Journal of Computer Security*, 6(4):219–235, 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kremer:2010:CSA

- [KM10] Steve Kremer and Laurent Mazaré. Computationally sound analysis of protocols using bilinear pairings. *Journal of Computer Security*, 18(6):999–1033, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Krukow:2008:LFH

- [KNS08] Karl Krukow, Mogens Nielsen, and Vladimiro Sassone. A logical framework for history-based access control and reputation systems. *Journal of Computer Security*, 16(1):63–101, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kobsa:2013:CJV

- [KNTU13] Alfred Kobsa, Rishab Nithyanand, Gene Tsudik, and Ersin Uzun. Can Jannie verify? Usability of display-equipped RFID tags for security purposes. *Journal of Computer Security*, 21(3):347–370,

???? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kar:2016:SSI

- [KPS16] Debabrata Kar, Suvasini Panigrahi, and Srikanth Sundararajan. SQLiDDS: SQL injection detection using document similarity measure. *Journal of Computer Security*, 24(4):507–539, ??? 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kremer:2003:GBV

- [KR03] Steve Kremer and Jean-François Raskin. A game-based verification of non-repudiation and fair exchange protocols. *Journal of Computer Security*, 11(3):399–429, ??? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kreitz:2013:FSW

- [Kre13] Gunnar Kreitz. Flow stealing: A well-timed redirection attack. *Journal of Computer Security*, 21(3):371–391, ??? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kolesnikov:2013:SAP

- [KSS13] Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider. A systematic approach to practically efficient general two-party secure function evaluation protocols and their modular design. *Journal of Computer Security*, 21(2):283–315, ??? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kelsey:2000:SCC

- [KSWH00] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Side channel cryptanalysis of product ciphers. *Journal of Computer Security*, 8(2–3):141–158, ??? 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kerschbaum:2002:UIS

- [KSZ02] Florian Kerschbaum, Eugene H. Spafford, and Diego Zamboni. Using internal sensors and embedded detectors for intrusion detection. *Journal of Computer Security*, 10(1–2):23–70, ??? 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Kusters:2012:GBD

- [KTV12] Ralf Küsters, Tomasz Truderung, and Andreas Vogt. A game-based definition of coercion resistance and its applications. *Jour-*

nal of Computer Security, 20(6):709–764, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

LaPadula:1996:F

- [LaP96] Leonard J. LaPadula. Foreword. *Journal of Computer Security*, 4(2–3):233–238, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

LaPadula:1996:MTR

- [LB96] Leonard J. LaPadula and D. Elliott Bell. MITRE technical report 2547, volume II. *Journal of Computer Security*, 4(2–3):239–263, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Littlewood:1993:TOM

- [LBF⁺93] Bev Littlewood, Sarah Brocklehurst, Norman Fenton, Peter Mellor, Stella Page, David Wright, John Dobson, John McDermid, and Dieter Gollmann. Towards operational measures of computer security. *Journal of Computer Security*, 2(2–3):211–229, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Li:2015:NAC

- [LCL⁺15] Jin Li, Xiaofeng Chen, Jingwei Li, Chunfu Jia, Jianfeng Ma, and Wenjing Lou. New access control systems based on outsourced attribute-based encryption. *Journal of Computer Security*, 23(6):659–683, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lee:2002:TCS

- [LFM⁺02] Wenke Lee, Wei Fan, Matthew Miller, Salvatore J. Stolfo, and Erez Zadok. Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security*, 10(1–2):5–22, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lekkas:2010:PMT

- [LG10] Dimitrios Lekkas and Dimitris Gritzalis. e-Passports as a means towards a Globally Interoperable Public Key Infrastructure. *Journal of Computer Security*, 18(3):379–396, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Li:2010:CCB

- [LHM⁺10] Jiguo Li, Xinyi Huang, Yi Mu, Willy Susilo, and Qianhong Wu. Constructions of certificate-based signature secure against key re-

placement attacks. *Journal of Computer Security*, 18(3):421–449, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lu:2015:TUO

- [LHY⁺15] Haibing Lu, Yuan Hong, Yanjiang Yang, Lian Duan, and Nazia Badar. Towards user-oriented RBAC model. *Journal of Computer Security*, 23(1):107–129, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Li:2012:GEP

- [Li12] Yingjiu Li. Guest Editor’s preface. *Journal of Computer Security*, 20(5):461–462, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lin:1999:GEP

- [Lin99] T. Y. Lin. Guest editor’s preface. *Journal of Computer Security*, 7(4):255, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lin:2000:GEP

- [Lin00] T. Y. Lin. Guest editor’s preface. *Journal of Computer Security*, 8(1):1, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Liu:2000:ICI

- [LJM00] Peng Liu, Sushil Jajodia, and Catherine D. McCollum. Intrusion confinement by isolation in information systems. *Journal of Computer Security*, 8(4):243–279, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Le:2016:MCR

- [LKAJ16] Meixing Le, Krishna Kant, Malek Athamnah, and Sushil Jajodia. Minimum cost rule enforcement for cooperative database access. *Journal of Computer Security*, 24(3):379–403, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lippert:2006:LCM

- [LKWB06] M. Lippert, V. Karatsiolis, A. Wiesmaier, and J. Buchmann. Life-cycle management of X.509 certificates based on LDAP directories. *Journal of Computer Security*, 14(5):419–439, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lowden:2015:DPA

- [LLA15] Jason Lowden, Marcin Lukowiak, and Sonia Lopez Alarcon. Design and performance analysis of efficient Keccak tree hashing on GPU architectures. *Journal of Computer Security*, 23(5):541–562, ??? 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lunt:1992:GEP

- [LM92] Teresa F. Lunt and John McLean. Guest Editors' preface. *Journal of Computer Security*, 1(3–4):217–218, ??? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lopez:2006:UPK

- [Lop06] Javier Lopez. Unleashing public-key cryptography in wireless sensor networks. *Journal of Computer Security*, 14(5):469–482, ??? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lester:2016:IFA

- [LOS16] Martin Lester, Luke Ong, and Max Schäfer. Information flow analysis for a dynamically typed language with staged metaprogramming. *Journal of Computer Security*, 24(5):541–582, ??? 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lotz:1997:TSM

- [Lot97] Volkmar Lotz. Threat scenarios as a means to formally develop secure systems. *Journal of Computer Security*, 5(1):31–67, ??? 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lowe:1998:CCA

- [Low98] Gavin Lowe. Casper: A compiler for the analysis of security protocols. *Journal of Computer Security*, 6(1–2):53–84, ??? 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lowe:1999:TCR

- [Low99] Gavin Lowe. Towards a completeness result for model checking of security protocols. *Journal of Computer Security*, 7(2–3):89–146, ??? 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lowe:2004:APS

- [Low04a] Gavin Lowe. Analysing protocols subject to guessing attacks. *Journal of Computer Security*, 12(1):83–97, 2004. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lowe:2004:DIF

- [Low04b] Gavin Lowe. Defining information flow quantity. *Journal of Computer Security*, 12(3–4):619–653, 2004. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Levine:2002:HMB

- [LS02] Brian Neil Levine and Clay Shields. Hordes: a multicast based protocol for anonymity. *Journal of Computer Security*, 10(3):213–240, 2002. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Luo:2016:MCM

- [LSMR16] Zhengqin Luo, José Fragoso Santos, Ana Almeida Matos, and Tamara Rezk. Mashic compiler: Mashup sandboxing based on inter-frame communication. *Journal of Computer Security*, 24(1):91–136, 2016. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lin:2017:SAC

- [LT17] Chung-Yi Lin and Wen-Guey Tzeng. Strategy analysis for cloud storage reliability management based on game theory. *Journal of Computer Security*, 25(2):153–171, 2017. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lu:2014:OFR

- [LVA14] Haibing Lu, Jaideep Vaidya, and Vijayalakshmi Atluri. An optimization framework for role mining. *Journal of Computer Security*, 22(1):1–31, 2014. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Li:2003:DCC

- [LWM03] Ninghui Li, William H. Winsborough, and John C. Mitchell. Distributed credential chain discovery in trust management. *Journal of Computer Security*, 11(1):35–86, 2003. CODEN JCSJET. ISSN 0926-227X (print), 1875-8924 (electronic).

Li:2002:EPA

- [LWWJ02] Yingjiu Li, Ningning Wu, X. Sean Wang, and Sushil Jajodia. Enhancing profiles for anomaly detection using time granularities. *Journal of Computer Security*, 10(1–2):137–157, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Liu:2015:JSD

- [LWZZ15] Wen Ming Liu, Lingyu Wang, Lei Zhang, and Shunzhi Zhu. k -jump: A strategy to design publicly-known algorithms for privacy preserving micro-data disclosure. *Journal of Computer Security*, 23(2):131–165, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Li:2010:ESS

- [LYW⁺10] Chung Ki Li, Guomin Yang, Duncan S. Wong, Xiaotie Deng, and Sherman S. M. Chow. An efficient signcryption scheme with key privacy and its extension to ring signcryption. *Journal of Computer Security*, 18(3):451–473, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Li:2011:GEP

- [LZ11] Yingjiu Li and Jianying Zhou. Guest editors' preface. *Journal of Computer Security*, 19(2):227–228, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Lipmaa:2013:MEC

- [LZ13] Helger Lipmaa and Bingsheng Zhang. A more efficient computationally sound non-interactive zero-knowledge shuffle argument. *Journal of Computer Security*, 21(5):685–719, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Malacaria:2010:RAS

- [Mal10] Pasquale Malacaria. Risk assessment of security threats for looping constructs. *Journal of Computer Security*, 18(2):191–228, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Matsumoto:1998:HCC

- [Mat98] Tsutomu Matsumoto. Human-computer cryptography: An attempt. *Journal of Computer Security*, 6(3):129–149, 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Matos:2009:DND

- [MB09] Ana Almeida Matos and Gérard Boudol. On declassification and the non-disclosure policy. *Journal of Computer Security*, 17(5):549–597, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Myers:2012:P

- [MB12] Andrew Myers and Michael Backes. Preface. *Journal of Computer Security*, 20(6):635–636, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Mallios:2015:PCE

- [MBK⁺15] Yannis Mallios, Lujjo Bauer, Dilsun Kaynar, Fabio Martinelli, and Charles Morisset. Probabilistic cost enforcement of security policies. *Journal of Computer Security*, 23(6):759–787, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Meier:2013:ECM

- [MCB13] Simon Meier, Cas Cremers, and David Basin. Efficient construction of machine-checked symbolic protocol security proofs. *Journal of Computer Security*, 21(1):41–87, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

McLean:1992:PNF

- [McL92] John McLean. Proving noninterference and functional correctness using traces. *Journal of Computer Security*, 1(1):37–57, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Meadows:1992:AFM

- [Mea92] Catherine Meadows. Applying formal methods to the analysis of a key management protocol. *Journal of Computer Security*, 1(1):5–35, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Meadows:2001:CBF

- [Mea01] Catherine Meadows. A cost-based framework for analysis of denial of service in networks. *Journal of Computer Security*, 9(1–2):143–164, 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Merritt:1997:GEP

- [Mer97] Michael Merritt. Guest editor's preface. *Journal of Computer Security*, 5(2):111–112, ??? 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Murray:2008:NDA

- [MG08] Toby Murray and Duncan Grove. Non-delegatable authorities in capability systems. *Journal of Computer Security*, 16(6):743–759, ??? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Migault:2017:DEI

- [MGK⁺17] Daniel Migault, Tobias Guggemos, Sylvain Killian, Maryline Laurent, Guy Pujolle, and Jean Philippe Wary. Diet-ESP: IP layer security for IoT. *Journal of Computer Security*, 25(2):173–203, ??? 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Mohamed:2017:SUD

- [MGS⁺17] Manar Mohamed, Song Gao, Niharika Sachdeva, Nitesh Saxena, Chengcui Zhang, Ponnurangam Kumaraguru, and Paul C. Van Oorschot. On the security and usability of dynamic cognitive game CAPTCHAs. *Journal of Computer Security*, 25(3):205–230, ??? 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Millen:1993:EPb

- [Mil93a] Jonathan Millen. Editor's preface. *Journal of Computer Security*, 2(4):277, ??? 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Millen:1993:RAM

- [Mil93b] Jonathan K. Millen. A resource allocation model for denial of service protection. *Journal of Computer Security*, 2(2–3):89–106, ??? 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Millen:1995:EPb

- [Mil95a] Jonathan K. Millen. Editor's preface. *Journal of Computer Security*, 3(2–3):85, ??? 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Millen:1995:UFC

- [Mil95b] Jonathan K. Millen. Unwinding forward correctability. *Journal of Computer Security*, 3(1):35–54, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Millen:1996:EPB

- [Mil96] Jonathan Millen. Editor’s preface to the Bell–LaPadula model. *Journal of Computer Security*, 4(2–3):229–231, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Millen:1999:SSI

- [Mil99] Jonathan Millen. Special section on intrusion detection. *Journal of Computer Security*, 7(1):1, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

McLean:1993:GEP

- [MK93] John McLean and Richard Kemmerer. Guest Editors’ preface. *Journal of Computer Security*, 2(2–3):87–88, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

McDermott:1996:APC

- [MM96] John McDermott and Ravi Mukkamala. Analytic performance comparison of transaction processing algorithms for the SINTRA replicated-architecture database system. *Journal of Computer Security*, 4(2–3):189–228, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Merlo:2015:MEP

- [MMF15] Alessio Merlo, Mauro Migliardi, and Paolo Fontanelli. Measuring and estimating power consumption in Android to support energy-based intrusion detection. *Journal of Computer Security*, 23(5):611–637, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Mardziel:2013:DEK

- [MMHS13] Piotr Mardziel, Stephen Magill, Michael Hicks, and Mudhakar Srivatsa. Dynamic enforcement of knowledge-based security policies using probabilistic abstract interpretation. *Journal of Computer Security*, 21(4):463–532, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Molsa:2005:MDS

- [Möl05] Jarmo Mölsä. Mitigating denial of service attacks: A tutorial. *Journal of Computer Security*, 13(6):807–837, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Motro:1992:UMS

- [Mot92] Amihai Motro. A unified model for security and integrity in relational databases. *Journal of Computer Security*, 1(2):189–213, 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

McDaniel:2006:EPA

- [MP06] Patrick McDaniel and Atul Prakash. Enforcing provisioning and authorization policy in the Antigone system. *Journal of Computer Security*, 14(6):483–511, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Malkhi:1997:HTS

- [MR97] Dahlia Malkhi and Michael Reiter. A high-throughput secure reliable multicast protocol. *Journal of Computer Security*, 5(2):113–127, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Maurer:1996:CSB

- [MS96] Ueli M. Maurer and Pierre E. Schmid. A calculus for security boots trapping in distributed systems. *Journal of Computer Security*, 4(1):55–80, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Mantel:2003:UAS

- [MS03] Heiko Mantel and Andrei Sabelfeld. A unifying approach to the security of distributed and multi-threaded programs. *Journal of Computer Security*, 11(4):615–676, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Millen:2005:SPAa

- [MS05a] Jonathan Millen and Vitaly Shmatikov. Symbolic protocol analysis with an Abelian group operator or Diffie–Hellman exponentiation. *Journal of Computer Security*, 13(3):515–564, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Millen:2005:SPAb

- [MS05b] Jonathan Millen and Vitaly Shmatikov. Symbolic protocol analysis with an Abelian group operator or Diffie–Hellman exponentiation. *Journal of Computer Security*, 13(4):695, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Myers:2013:BBC

- [MSas13] Steven Myers, Mona Sergi, and abhi shelat. Black-box construction of a more than non-malleable CCA1 encryption scheme from plaintext awareness. *Journal of Computer Security*, 21(5):721–748, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Mitra:2015:GTR

- [MSAV15] Barsha Mitra, Shamik Sural, Vijayalakshmi Atluri, and Jaideep Vaidya. The generalized temporal role mining problem. *Journal of Computer Security*, 23(1):31–58, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Meadows:2004:FSA

- [MSC04] Catherine Meadows, Paul Syverson, and Iliano Cervesato. Formal specification and analysis of the Group Domain of Interpretation Protocol using NPATRL and the NRL Protocol Analyzer. *Journal of Computer Security*, 12(6):893–931, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Myers:2006:ERD

- [MSZ06] Andrew C. Myers, Andrei Sabelfeld, and Steve Zdancewic. Enforcing robust declassification and qualified robustness. *Journal of Computer Security*, 14(2):157–196, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Mont:2008:PPE

- [MT08] Marco Casassa Mont and Robert Thyne. Privacy policy enforcement in enterprises with identity management solutions. *Journal of Computer Security*, 16(2):133–163, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Modersheim:2010:CDS

- [MVB10] Sebastian Modersheim, Luca Viganò, and David Basin. Constraint differentiation: Search-space reduction for the constraint-based analysis of security protocols. *Journal of Computer Security*, 18(4):

575–618, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Mannan:2011:LPD

- [MvO11] Mohammad Mannan and P. C. van Oorschot. Leveraging personal devices for stronger password authentication from untrusted computers. *Journal of Computer Security*, 19(4):703–750, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Micciancio:2004:CTA

- [MW04] Daniele Micciancio and Bogdan Warinschi. Completeness theorems for the Abadi–Rogaway language of encrypted expressions. *Journal of Computer Security*, 12(1):99–129, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Notargiacomo:1995:MMI

- [NBM95] LouAnna Notargiacomo, Barbara T. Blaustein, and Catherine D. McCollum. Merging models: Integrity, dynamic separation of duty and trusted data management. *Journal of Computer Security*, 3(2–3):207–230, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Nayyar:2008:AAM

- [NG08] Harshit Nayyar and Ali A. Ghorbani. Approximate autoregressive modeling for network attack detection. *Journal of Computer Security*, 16(2):165–197, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Nieto:2013:PVC

- [NMP+13] Juan González Nieto, Mark Manulis, Bertram Poettering, Jothi Rangasamy, and Douglas Stebila. Publicly verifiable ciphertexts. *Journal of Computer Security*, 21(5):749–778, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Nguyen:2011:APB

- [NR11] L. H. Nguyen and A. W. Roscoe. Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey. *Journal of Computer Security*, 19(1):139–201, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Niu:2014:FVS

- [NRW14] Jianwei Niu, Mark Reith, and William H. Winsborough. Formal verification of security properties in trust management policy.

Journal of Computer Security, 22(1):69–153, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Norman:2006:APC

- [NS06] Gethin Norman and Vitaly Shmatikov. Analysis of probabilistic contract signing. *Journal of Computer Security*, 14(6):561–589, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ngo:2014:EVC

- [NSH14] Tri Minh Ngo, Mariëlle Stoelinga, and Marieke Huisman. Effective verification of confidentiality for multi-threaded programs. *Journal of Computer Security*, 22(2):269–300, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ng:2011:PRO

- [NSMSN11] Ching Yu Ng, Willy Susilo, Yi Mu, and Rei Safavi-Naini. Practical RFID ownership transfer scheme. *Journal of Computer Security*, 19(2):319–341, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Nithyanand:2011:UAR

- [NTU11] Rishab Nithyanand, Gene Tsudik, and Ersin Uzun. User-aided reader revocation in PKI-based RFID systems. *Journal of Computer Security*, 19(6):1147–1172, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Nenadic:2005:RBV

- [Nzs05] Aleksandra Nenadić, Ning Zhang, and Qi Shi. RSA-based Verifiable and Recoverable Encryption of Signatures and its application in certified e-mail delivery. *Journal of Computer Security*, 13(5):757–777, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ourston:2004:CIA

- [OMSH04] Dirk Ourston, Sara Matzner, William Stump, and Bryan Hopkins. Coordinated Internet attacks: responding to attack complexity. *Journal of Computer Security*, 12(2):165–190, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Paulson:1998:IAV

- [Pau98] Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6(1–2):85–128,

???? 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Paulson:2001:RBS

- [Pau01] Lawrence C. Paulson. Relations between secrets: two formal analyses of the Yahalom protocol. *Journal of Computer Security*, 9(3):197–216, ??? 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Paiola:2013:VSP

- [PB13] Miriam Paiola and Bruno Blanchet. Verification of security protocols with lists: From length one to unbounded length. *Journal of Computer Security*, 21(6):781–816, ??? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Preda:2009:SBC

- [PG09] Mila Dalla Preda and Roberto Giacobazzi. Semantics-based code obfuscation by abstract interpretation. *Journal of Computer Security*, 17(6):855–908, ??? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Politz:2014:TBV

- [PGK14] Joe Gibbs Politz, Arjun Guha, and Shriram Krishnamurthi. Typed-based verification of Web sandboxes. *Journal of Computer Security*, 22(4):511–565, ??? 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Petkovic:2009:P

- [PJ09] Milan Petković and Willem Jonker. Preface. *Journal of Computer Security*, 17(1):1–3, ??? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Pereira:2003:SAU

- [PQ03] Olivier Pereira and Jean-Jacques Quisquater. Some attacks upon authenticated group key agreement protocols. *Journal of Computer Security*, 11(4):555–580, ??? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Pereira:2006:IBS

- [PQ06] Olivier Pereira and Jean-Jacques Quisquater. On the impossibility of building secure Cliques-type authenticated group key agreement protocols. *Journal of Computer Security*, 14(2):197–246, ???

2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Price:2006:PKI

- [Pri06] Geraint Price. Public key infrastructures: A research agenda. *Journal of Computer Security*, 14(5):391–417, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Pala:2010:FPN

- [PS10a] Massimiliano Pala and Sean W. Smith. Finding the PKI needles in the Internet haystack. *Journal of Computer Security*, 18(3):397–420, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Pucella:2010:IOS

- [PS10b] Riccardo Pucella and Fred B. Schneider. Independence from obfuscation: A semantic framework for diversity. *Journal of Computer Security*, 18(5):701–749, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Peddinti:2014:WSQ

- [PS14] Sai Teja Peddinti and Nitesh Saxena. Web search query privacy: Evaluating query obfuscation and anonymizing networks. *Journal of Computer Security*, 22(1):155–199, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Phatak:2013:SIN

- [PSJ+13] Dhananjay Phatak, Alan T. Sherman, Nikhil Joshi, Bhushan Sonawane, Vivek G. Relan, and Amol Dawalbhakta. Spread identity: A new dynamic address remapping mechanism for anonymity and DDoS defense. *Journal of Computer Security*, 21(2):233–281, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Pirretti:2010:SAB

- [PTMW10] Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure attribute-based systems. *Journal of Computer Security*, 18(5):799–837, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Pescape:2005:EAA

- [PV05] Antonio Pescapè and Giorgio Ventre. Experimental analysis of attacks against intradomain routing protocols. *Journal of Com-*

puter Security, 13(6):877–903, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Quisquater:1997:ASS

- [QJ97] Jean-Jacques Quisquater and Marc Joye. Authentication of sequences with the SL_2 hash function: application to video sequences. *Journal of Computer Security*, 5(3):213–223, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ray:1998:SBT

- [RAJ98] Indrakshi Ray, Paul Ammann, and Sushil Jajodia. A semantic-based transaction processing model for multilevel transactions. *Journal of Computer Security*, 6(3):181–217, 1998. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Roscoe:1999:PSP

- [RB99] A. W. Roscoe and P. J. Broadfoot. Proving security protocols with model checkers by data independence techniques. *Journal of Computer Security*, 7(2–3):147–190, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Radosavac:2007:DIM

- [RCBM07] S. Radosavac, Alvaro A. Cárdenas, John S. Baras, and George V. Moustakides. Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: Robust strategies against individual and colluding attackers. *Journal of Computer Security*, 15(1):103–128, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Roy:2010:ITP

- [RDDM10] Arnab Roy, Anupam Datta, Ante Derek, and John C. Mitchell. Inductive trace properties for computational security. *Journal of Computer Security*, 18(6):1035–1073, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Reiter:1996:KMS

- [RFLW96] Michael K. Reiter, Matthew K. Franklin, John B. Lacy, and Rebecca N. Wright. The Ω key management service. *Journal of Computer Security*, 4(4):267–287, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Raya:2007:SVA

- [RH07] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ryan:2001:PAN

- [RS01] P. Y. A. Ryan and S. A. Schneider. Process algebra and non-interference. *Journal of Computer Security*, 9(1–2):75–103, 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ramakrishnan:2002:MBA

- [RS02] C. R. Ramakrishnan and R. Sekar. Model-based analysis of configuration vulnerabilities. *Journal of Computer Security*, 10(1–2):189–209, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Ramanujam:2005:DCE

- [RS05] R. Ramanujam and S. P. Suresh. Decidability of context-explicit security protocols. *Journal of Computer Security*, 13(1):135–165, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Rafnsson:2016:SME

- [RS16] Willard Rafnsson and Andrei Sabelfeld. Secure multi-execution: Fine-grained, declassification-aware, and transparent. *Journal of Computer Security*, 24(1):39–90, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Rieck:2011:AAM

- [RTWH11] Konrad Rieck, Philipp Trinius, Carsten Willems, and Thorsten Holz. Automatic analysis of malware behavior using machine learning. *Journal of Computer Security*, 19(4):639–668, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Roscheisen:1997:NCD

- [RW97] Martin Röscheisen and Terry Winograd. A network-centric design for relationship-based security and access control. *Journal of Computer Security*, 5(3):249–254, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Roscoe:1996:NIT

- [RWW96] A. W. Roscoe, J. C. P. Woodcock, and L. Wulf. Non-interference through determinism. *Journal of Computer Security*, 4(1):27–53, ??? 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sonchack:2016:ELS

- [SA16] John Sonchack and Adam J. Aviv. Exploring large scale security system reproducibility with the LESS simulator. *Journal of Computer Security*, 24(5):645–665, ??? 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sabelfeld:2008:P

- [Sab08] Andrei Sabelfeld. Preface. *Journal of Computer Security*, 16(5):495, ??? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sabelfeld:2010:P

- [Sab10] Andrei Sabelfeld. Preface. *Journal of Computer Security*, 18(6):1075, ??? 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Stolfo:2005:CET

- [SAE⁺05] Salvatore J. Stolfo, Frank Apap, Eleazar Eskin, Katherine Heller, Shlomo Hershkop, Andrew Honig, and Krysta Svore. A comparative evaluation of two algorithms for Windows Registry Anomaly Detection. *Journal of Computer Security*, 13(4):659–693, ??? 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sandhu:1992:GEP

- [San92a] Ravi Sandhu. Guest Editor’s preface. *Journal of Computer Security*, 1(2):131–132, ??? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sandhu:1992:EPS

- [San92b] Ravi S. Sandhu. Expressive power of the schematic protection model. *Journal of Computer Security*, 1(1):59–98, ??? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Shin:2011:EES

- [SAsC11] Heechang Shin, Vijayalakshmi Atluri, and June suh Cho. Efficiently enforcing spatiotemporal access control under uncertain location information. *Journal of Computer Security*, 19(3):607–637, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sandhu:1999:RBA

- [SB99] Ravi Sandhu and Venkata Bhamidipati. Role-based administration of user-role assignment: The URA97 model and its Oracle implementation. *Journal of Computer Security*, 7(4):317–342, 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Song:2001:ANA

- [SBP01] Dawn Xiaodong Song, Sergey Berezin, and Adrian Perrig. Athena: a novel approach to efficient automatic security protocol analysis. *Journal of Computer Security*, 9(1–2):47–74, 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sherwood:2005:PPS

- [SBS05] Rob Sherwood, Bobby Bhattacharjee, and Aravind Srinivasan. P5: A protocol for scalable anonymous communication. *Journal of Computer Security*, 13(6):839–876, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Spalka:2000:SNS

- [SC00] Adrian Spalka and Armin B. Cremers. Structured name-spaces in secure databases. *Journal of Computer Security*, 8(1):67–86, 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Schneider:2003:GEP

- [Sch03] Steve Schneider. Guest editor’s preface. *Journal of Computer Security*, 11(4):449–450, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Schneider:2004:GEP

- [Sch04] Steve Schneider. Guest editor’s preface. *Journal of Computer Security*, 12(3–4):313–315, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Shieh:1996:DIL

- [SG96] Shiuh-Pyng Shieh and Virgil D. Gligor. Detecting illicit leakage of information in operating systems. *Journal of Computer Security*, 4(2-3):123–148, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic). URL <http://www.cl.cam.ac.uk/~fapp2/steganography/bibliography/061242.html>.

Spinellis:2002:PID

- [SG02] Diomidis Spinellis and Dimitris Gritzalis. Panoptis: Intrusion detection using a domain-specific language. *Journal of Computer Security*, 10(1-2):159–176, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Staniford:2002:PAD

- [SHM02] Stuart Staniford, James A. Hoagland, and Joseph M. McAlerney. Practical automated detection of stealthy portscans. *Journal of Computer Security*, 10(1-2):105–136, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Shmatikov:2004:PAA

- [Shm04] Vitaly Shmatikov. Probabilistic analysis of an anonymity system. *Journal of Computer Security*, 12(3-4):355–377, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sinclair:1997:ASS

- [Sin97] Jane Sinclair. Action systems for security specification. *Journal of Computer Security*, 5(2):129–154, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sinha:2011:SSS

- [Sin11] Anshuman Sinha. A survey of system security in contactless electronic passports. *Journal of Computer Security*, 19(1):203–226, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Soupionis:2014:GTA

- [SKEG14] Yannis Soupionis, Remous-Aris Koutsiamanis, Pavlos Efraimidis, and Dimitris Gritzalis. A game-theoretic analysis of preventing spam over Internet Telephony via audio CAPTCHA-based authentication. *Journal of Computer Security*, 22(3):383–413, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Simmons:1995:RTI

- [SM95] G. J. Simmons and Catherine Meadows. The role of trust in information integrity protocols. *Journal of Computer Security*, 3(1):71–84, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Siaterlis:2005:OSA

- [SM05] Christos Siaterlis and Vasilis Maglaris. One step ahead to multi-sensor data fusion for DDoS detection. *Journal of Computer Security*, 13(5):779–806, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Smith:2006:ITP

- [Smi06] Geoffrey Smith. Improved typings for probabilistic noninterference in a multi-threaded language. *Journal of Computer Security*, 14(6):591–623, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sumii:2003:LRE

- [SP03] Eijiro Sumii and Benjamin C. Pierce. Logical relations for encryption. *Journal of Computer Security*, 11(4):521–554, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Salvail:2010:STR

- [SPD⁺10] Louis Salvail, Momtchil Peev, Eleni Diamanti, Romain Alléaume, Norbert Lütkenhaus, and Thomas Länger. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security*, 18(1):61–87, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Schlesinger:2014:MPA

- [SPS⁺14] Cole Schlesinger, Karthik Pattabiraman, Nikhil Swamy, David Walker, and Benjamin Zorn. Modular protections against non-control data attacks. *Journal of Computer Security*, 22(5):699–742, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Syverson:1997:PWB

- [SRG97] Paul F. Syverson, Michael G. Reed, and David M. Goldschlag. Private Web browsing. *Journal of Computer Security*, 5(3):237–248, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Schellhorn:2002:VFS

- [SRS⁺02] Gerhard Schellhorn, Wolfgang Reif, Axel Schairer, Paul Karger, Vernon Austel, and David Toll. Verified formal security models for multiapplicative smart cards. *Journal of Computer Security*, 10(4):339–367, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Samarati:1997:GEP

- [SS97] Pierangela Samarati and Ravi Sandhu. Guest editors' preface. *Journal of Computer Security*, 5(4):269–270, 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sabelfeld:2009:DDP

- [SS09] Andrei Sabelfeld and David Sands. Declassification: Dimensions and principles. *Journal of Computer Security*, 17(5):517–548, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Saklikar:2010:IFV

- [SS10] Samir Saklikar and Subir Saha. Identity federation for VoIP systems. *Journal of Computer Security*, 18(4):499–540, 2010. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Stakhanova:2012:TCS

- [SSBW12] Natalia Stakhanova, Chris Strasburg, Samik Basu, and Johnny S. Wong. Towards cost-sensitive assessment of intrusion response selection. *Journal of Computer Security*, 20(2–3):169–198, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Shroff:2008:SIF

- [SST08] Paritosh Shroff, Scott F. Smith, and Mark Thober. Securing information flow via dynamic capture of dependencies. *Journal of Computer Security*, 16(5):637–688, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Shmatikov:2005:RBT

- [ST05] Vitaly Shmatikov and Carolyn Talcott. Reputation-based trust management. *Journal of Computer Security*, 13(1):167–190, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Shen:2015:DIC

- [ST15] Shiuan-Tzuo Shen and Wen-Guey Tzeng. Delegated integrity check for hierarchical cloud data. *Journal of Computer Security*, 23(4):471–508, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sewell:2003:SCU

- [SV03] Peter Sewell and Jan Vitek. Secure composition of untrusted code: box π , wrappers, and causality types. *Journal of Computer Security*, 11(2):135–187, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Spalazzi:2015:SIS

- [SV15] Luca Spalazzi and Luca Viganò. Special issue on security and high performance computing systems. *Journal of Computer Security*, 23(5):539–540, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Shin:2011:PAM

- [SVA11] Heechang Shin, Jaideep Vaidya, and Vijayalakshmi Atluri. A profile anonymization model for location-based services. *Journal of Computer Security*, 19(5):795–833, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Skormin:2007:PIA

- [SVSM07] V. Skormin, A. Volynkin, D. Summerville, and J. Moronski. Prevention of information attacks by run-time detection of self-replication in computer codes. *Journal of Computer Security*, 15(2):273–302, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Skalka:2007:RMD

- [SWC07] Christian Skalka, X. Sean Wang, and Peter Chapin. Risk management for distributed authorization. *Journal of Computer Security*, 15(4):447–489, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Spindler:2008:PVS

- [SWH⁺08] Torsten Spindler, Christoph Wartmann, Ludger Hovestadt, Daniel Roth, Luc Van Gool, and Andreas Steffen. Privacy in video surveilled spaces. *Journal of Computer Security*, 16(2):199–222,

???? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Syverson:1992:KBS

[Syv92] Paul F. Syverson. Knowledge, belief, and semantics in the analysis of cryptographic protocols. *Journal of Computer Security*, 1(3–4):317–334, ??? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Syverson:2001:GEP

[Syv01] Paul F. Syverson. Guest editor’s preface. *Journal of Computer Security*, 9(1–2):1–2, ??? 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Syverson:2003:GEP

[Syv03] Paul F. Syverson. Guest editor’s preface. *Journal of Computer Security*, 11(2):133, ??? 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Sun:2012:TAV

[SZP⁺12] Yanjie Sun, Chenyi Zhang, Jun Pang, Baptiste Alcalde, and Sjouke Mauw. A trust-augmented voting scheme for collaborative privacy management. *Journal of Computer Security*, 20(4):437–459, ??? 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Tardo:1992:SGA

[TA92] Joseph J. Tardo and Kannan Alagappan. SPX: Global authentication using public key certificates. *Journal of Computer Security*, 1(3–4):295–316, ??? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Tiplea:2008:SBS

[TBEB08] Ferucio L. Tiplea, Cătălin V. Bîrjoveanu, Constantin Enea, and Ioana Boureanu. Secrecy for bounded security protocols with freshness check is NEXPTIME-complete. *Journal of Computer Security*, 16(6):689–712, ??? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Taglienti:2016:UAP

[TC16] Claudio Taglienti and James Cannady. The user attribution problem and the challenge of persistent surveillance of user activity in

complex networks. *Journal of Computer Security*, 24(2):235–288, 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Traynor:2008:EOF

- [TEML08] Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Exploiting open functionality in SMS-capable cellular networks. *Journal of Computer Security*, 16(6):713–742, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Tripunitara:2007:TCE

- [TL07] Mahesh V. Tripunitara and Ninghui Li. A theory for comparing the expressive power of access control models. *Journal of Computer Security*, 15(2):231–272, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Toahchoodee:2011:FAS

- [TR11] Manachai Toahchoodee and Indrakshi Ray. On the formalization and analysis of a spatio-temporal role-based access control model. *Journal of Computer Security*, 19(3):399–452, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Trostle:1993:MFT

- [Tro93] Jonathan T. Trostle. Modelling a fuzzy time system. *Journal of Computer Security*, 2(4):291–309, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Thomas:1993:KAM

- [TS93] Roshan K. Thomas and Ravi S. Sandhu. A kernelized architecture for multilevel secure object-oriented databases supporting write-up. *Journal of Computer Security*, 2(2-3):231–275, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Thuraisingham:2003:GEP

- [TvdR03] Bhavani Thuraisingham and Reind van de Riet. Guest editors' preface. *Journal of Computer Security*, 11(3):289, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Teepe:2003:WAS

- [TvdRO03] Wouter Teepe, Reind van de Riet, and Martin Olivier. WorkFlow analyzed for security and privacy in using databases. *Journal of Computer Security*, 11(3):353–363, 2003. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Uzun:2014:SAT

- [UAV⁺14] Emre Uzun, Vijayalakshmi Atluri, Jaideep Vaidya, Shamik Sural, Anna Lisa Ferrara, Gennaro Parlato, and P. Madhusudan. Security analysis for temporal role based access control. *Journal of Computer Security*, 22(6):961–996, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Uribe:2007:AAF

- [UC07] Tomás E. Uribe and Steven Cheung. Automatic analysis of firewall and network intrusion detection system configurations. *Journal of Computer Security*, 15(6):691–715, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Vaidya:2009:ERM

- [VAGL09] Jaideep Vaidya, Vijayalakshmi Atluri, Qi Guo, and Haibing Lu. Edge-RMP: Minimizing administrative assignments for role-based access control. *Journal of Computer Security*, 17(2):211–235, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Vaidya:2005:SSI

- [VC05] Jaideep Vaidya and Chris Clifton. Secure set intersection cardinality with application to association rule mining. *Journal of Computer Security*, 13(4):593–622, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

vanderMeyden:2015:WII

- [vdM15] Ron van der Meyden. What, indeed, is intransitive noninterference? *Journal of Computer Security*, 23(2):197–228, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Vaidya:2011:I

- [VG11] Jaideep Vaidya and Ehud Gudes. Introduction. *Journal of Computer Security*, 19(3):485–486, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Volpano:1996:STS

- [VIS96] Dennis Volpano, Cynthia Irvine, and Geoffrey Smith. A sound type system for secure flow analysis. *Journal of Computer Security*, 4(2–3):167–187, 1996. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Visconti:2013:SIA

- [Vis13] Ivan Visconti. Special issue: Advances in security for communication networks. *Journal of Computer Security*, 21(5):599–600, ??? 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Vigna:1999:NNB

- [VK99] Giovanni Vigna and Richard A. Kemmerer. NetSTAT: A network-based intrusion detection system. *Journal of Computer Security*, 7(1):37–71, ??? 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

vanOorschot:2011:EPC

- [vOT11] P. C. van Oorschot and Julie Thorpe. Exploiting predictability in click-based graphical passwords. *Journal of Computer Security*, 19(4):669–702, ??? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Vavilis:2016:SBQ

- [VPZ16] Sokratis Vavilis, Milan Petković, and Nicola Zannone. A severity-based quantification of data leakages in database systems. *Journal of Computer Security*, 24(3):321–345, ??? 2016. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Volpano:1999:PNC

- [VS99] Dennis Volpano and Geoffrey Smith. Probabilistic noninterference in a concurrent language. *Journal of Computer Security*, 7(2–3):231–253, ??? 1999. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Vigna:2009:REA

- [VVB⁺09] Giovanni Vigna, Fredrik Valeur, Davide Balzarotti, William Robertson, Christopher Kruegel, and Engin Kirda. Reducing errors in the anomaly-based detection of web-based attacks through the combined analysis of web requests and SQL queries. *Journal of Computer Security*, 17(3):305–329, ??? 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wang:2006:GNR

- [Wan06] Guilin Wang. Generic non-repudiation protocols supporting transparent off-line TTP. *Journal of Computer Security*, 14(5):441–467,

???? 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Warinschi:2005:CAN

- [War05] Bogdan Warinschi. A computational analysis of the Needham–Schroeder–(Lowe) protocol. *Journal of Computer Security*, 13(3):565–591, ??? 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Winslett:1997:UDC

- [WCJS97] M. Winslett, N. Ching, V. Jones, and I. Slepchin. Using digital credentials on the World Wide Web. *Journal of Computer Security*, 5(3):255–267, ??? 1997. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wang:2008:CBH

- [WD08] Lifu Wang and Partha Dasgupta. Coprocessor-based hierarchical trust management for software integrity and digital identity protection. *Journal of Computer Security*, 16(3):311–339, ??? 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wespi:2000:FVV

- [WDDN00] Andreas Wespi, Hervé Debar, Marc Dacier, and Mehdi Nassehi. Fixed- vs. variable-length patterns for detecting suspicious process behavior. *Journal of Computer Security*, 8(2–3):159–181, ??? 2000. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wehner:2007:AWN

- [Weh07] Stephanie Wehner. Analyzing worms and network traffic using compression. *Journal of Computer Security*, 15(3):303–320, ??? 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Woo:1993:ADS

- [WL93] Thomas Y. C. Woo and Simon S. Lam. Authorization in distributed systems: A new approach. *Journal of Computer Security*, 2(2–3):107–136, ??? 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wang:2007:PBI

- [WLJW07] Lingyu Wang, Yingjiu Li, Sushil Jajodia, and Duminda Wijesekera. Parity-based inference control for multi-dimensional range

sum queries. *Journal of Computer Security*, 15(4):417–445, ??? 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wright:2001:DGM

- [WLM01] Rebecca N. Wright, Patrick D. Lincoln, and Jonathan K. Millen. Depender graphs: A method of fault-tolerant certificate distribution. *Journal of Computer Security*, 9(4):323–338, ??? 2001. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wright:2002:DGM

- [WLM02] Rebecca N. Wright, Patrick D. Lincoln, and Jonathan K. Millen. Depender graphs: A method of fault-tolerant certificate distribution. *Journal of Computer Security*, 10(3):297, ??? 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wüller:2017:DPP

- [WMF⁺17] Stefan Wüller, Daniel Mayer, Fabian Förg, Samuel Schüppen, Benjamin Assadsolimani, Ulrike Meyer, and Susanne Wetzel. Designing privacy-preserving interval operations based on homomorphic encryption and secret sharing techniques. *Journal of Computer Security*, 25(1):59–81, ??? 2017. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wray:1992:ACT

- [Wra92] John C. Wray. An analysis of covert timing channels. *Journal of Computer Security*, 1(3–4):219–232, ??? 1992. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Welch:2002:URM

- [WS02] Ian Welch and Robert J. Stroud. Using reflection as a mechanism for enforcing security policies on compiled code. *Journal of Computer Security*, 10(4):399–432, ??? 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wang:2004:CBI

- [WWJ04] Lingyu Wang, Duminda Wijesekera, and Sushil Jajodia. Cardinality-based inference control in data cubes. *Journal of Computer Security*, 12(5):655–692, ??? 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Wang:2008:IIA

- [WYSJ08] Lingyu Wang, Chao Yao, Anoop Singhal, and Sushil Jajodia. Implementing interactive analysis of attack graphs using relational databases. *Journal of Computer Security*, 16(4):419–437, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Xu:2009:ASL

- [XC09] Haizhi Xu and Steve J. Chapin. Address-space layout randomization using code islands. *Journal of Computer Security*, 17(3):331–362, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Xu:2007:SGC

- [Xu07] Shouhuai Xu. On the security of group communication schemes. *Journal of Computer Security*, 15(1):129–169, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Xia:2006:EWD

- [XVW⁺06] Jianhong Xia, Sarma Vangala, Jiang Wu, Lixin Gao, and Kevin Kwiat. Effective worm detection for various scan techniques. *Journal of Computer Security*, 14(4):359–387, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yahalom:1993:OAT

- [Yah93] Raphael Yahalom. Optimality of asynchronous two-party secure data-exchange protocols. *Journal of Computer Security*, 2(2–3):191–209, 1993. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yasinsac:2002:ESP

- [Yas02] Alec Yasinsac. An environment for security protocol intrusion detection. *Journal of Computer Security*, 10(1–2):177–188, 2002. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yee:2008:GEIa

- [YGH08] George O. M. Yee, Ali A. Ghorbani, and Patrick C. K. Hung. Guest Editors' introduction. *Journal of Computer Security*, 16(2):103–106, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yang:2015:PAA

- [YGSY15] Ping Yang, Mikhail I. Gofman, Scott D. Stoller, and Zijiang Yang. Policy analysis for administrative role based access control without separate administration. *Journal of Computer Security*, 23(1):1–29, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yu:2005:SUI

- [YLZ05] Meng Yu, Peng Liu, and Wanyu Zang. Specifying and using intrusion masking models to process distributed operations. *Journal of Computer Security*, 13(4):623–658, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yee:2008:GEIb

- [YRY08] George O. M. Yee, Chunming Rong, and Laurence T. Yang. Guest Editors' introduction. *Journal of Computer Security*, 16(3):261–264, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yarmand:2013:BBA

- [YSD13] Mohammad H. Yarmand, Kamran Sartipi, and Douglas G. Down. Behavior-based access control for distributed healthcare systems. *Journal of Computer Security*, 21(1):1–39, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yuen:2014:TCT

- [YSM14] Tsz Hon Yuen, Willy Susilo, and Yi Mu. Towards a cryptographic treatment of publish/subscribe systems. *Journal of Computer Security*, 22(1):33–67, 2014. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yasuoka:2011:BPQ

- [YT11] Hirotoshi Yasuoka and Tachio Terauchi. On bounding problems of quantitative information flow. *Journal of Computer Security*, 19(6):1029–1082, 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yao:2009:EPT

- [YWW⁺09] Chao Yao, Lingyu Wang, X. Sean Wang, Claudio Bettini, and Sushil Jajodia. Evaluating privacy threats in released database

views by symmetric indistinguishability. *Journal of Computer Security*, 17(1):5–42, 2009. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Yuan:2015:PPC

- [YY15] Jiawei Yuan and Shucheng Yu. PCPOR: Public and constant-cost proofs of retrievability in cloud1. *Journal of Computer Security*, 23(3):403–425, 2015. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zhou:2008:SPR

- [ZAF08] Jie Zhou and Jim Alves-Foss. Security policy refinement and enforcement for the design of multi-level secure systems. *Journal of Computer Security*, 16(2):107–131, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zanin:2007:RRD

- [ZDM07] Giorgio Zanin, Roberto Di Pietro, and Luigi V. Mancini. Robust RSA distributed signatures for large-scale long-lived ad hoc networks. *Journal of Computer Security*, 15(1):171–196, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zhou:2012:FAS

- [ZF12] Hongbin Zhou and Simon N. Foley. Fast automatic security protocol generation. *Journal of Computer Security*, 20(2–3):119–167, 2012. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zhang:2004:RAR

- [ZGD04] Jian Zhang, Jian Gong, and Yong Ding. Research on automated rollbackability of intrusion response. *Journal of Computer Security*, 12(5):737–751, 2004. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zhou:2013:SVC

- [ZGDS13] Fangfei Zhou, Manish Goel, Peter Desnoyers, and Ravi Sundaram. Scheduler vulnerabilities and coordinated attacks in cloud computing. *Journal of Computer Security*, 21(4):533–559, 2013. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zhou:2006:P

- [ZK06] Jianying Zhou and Meng-Chow Kang. Preface. *Journal of Computer Security*, 14(5):389–390, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zakinthinos:1995:CNI

- [ZL95] A. Zakinthinos and E. S. Lee. The composability of non-interference. *Journal of Computer Security*, 3(4):269–281, 1995. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zouridaki:2007:HQT

- [ZMHT07] Charikleia Zouridaki, Brian L. Mark, Marek Hejmo, and Roshan K. Thomas. Hermes: A quantitative trust establishment framework for reliable data packet delivery in MANETs. *Journal of Computer Security*, 15(1):3–38, 2007. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zhang:2008:SVA

- [ZRG08] Nan Zhang, Mark Ryan, and Dimitar P. Guelev. Synthesising verified access control systems through model checking. *Journal of Computer Security*, 16(1):1–61, 2008. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zhu:2006:GEG

- [ZSXJ06] Sencun Zhu, Sanjeev Setia, Shouhuai Xu, and Sushil Jajodia. GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks. *Journal of Computer Security*, 14(4):301–325, 2006. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).

Zuquete:2005:EHQ

- [Zúq05] André Zúquete. An efficient high quality random number generator for multi-programmed systems. *Journal of Computer Security*, 13(2):243–263, 2005. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic). URL <http://dl.acm.org/citation.cfm?id=1077819.1077821>.

Zhang:2011:UTA

- [ZZW⁺11] Chao Zhang, Wei Zou, Tielei Wang, Yu Chen, and Tao Wei. Using type analysis in compiler to mitigate integer-overflow-to-buffer-overflow threat. *Journal of Computer Security*, 19(6):1083–1107,

???? 2011. CODEN JCSIET. ISSN 0926-227X (print), 1875-8924 (electronic).