A Complete Bibliography of *Digital Threats: Research and Practice (DTRAP)*

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/`

28 May 2024
Version 1.05

Title word cross-reference

.eu [DSV+21]. **.NET** [RGK23].

1 [PLD+20]. **11510** [Koo20]. **19** [GPFV23, KGH+22, KMGR22, SCJ+22, SASTL22].

2020 [DvdH22]. **2023** [DS23].

ABI [AVS+22]. **Access** [HOGF23, LSK+22, OMHY20]. **Accuracy** [KGH+22]. **Accurate** [SMK20]. **Acoustic** [VPG+23]. **ACSAC'19** [PLD+20, PLD+21]. **ACSAC'20** [PLS22]. **Actionable** [ITZ23]. **Active** [DHT22, SBL22]. **Activism** [HLP22]. **Activities** [LLM20]. **adaptive** [XNC+23]. **Adopt** [KGH+22]. **Advanced** [AMS23, IKT+21, LLM20, MMY23]. **Adversarial** [AAF+22]. **Adversary** [SGH23]. **Adversary-Centric** [SGH23]. **Advertising** [CYGL20]. **Aegis** [SBU21]. **Affordable** [DD20]. **against** [AAF+22, DKP21, OMHY20, RBA+23]. **Agenda** [AFS+22]. **agnostic** [RRF+23]. **AI** [ANM23, DWN21]. **Aids** [KGH+22]. **Alerts** [HSZ+23]. **Algorithm** [BFF+23, CFZK23]. **AMiner** [LWS+23]. **Analysis** [CTA+23, HGKS23, HMD24, KCH+20, KMPS23, LWS+23, LCTC23, LHH22, LZ23, RRF+23, RUPT22, RKC+24, SNA+23, SGH23, TDZ+24, vHvdHdVvRD23]. **Analysts** [HAH+21]. **Analytics** [HTRO24]. **Analyze** [CMLV24, TCBK20]. **Analyzing** [DH22]. **Android** [GTL+20, GLTW23, KCH+20, KMPS23, PCG24].

ANDROIDGYNY [PCG24]. **Annotation** [KPBZ21]. **Anomalous** [SNA^{+}23]. **Anomaly** [EMS^{+}23, LWS^{+}23]. **Anomaly-based** [LWS^{+}23]. **Anonymization** [AYP^{+}21]. **Anti** [GAS24]. **Anti-Phishing** [GAS24]. **Antivirus** [GLS21]. **API** [UOI^{+}21]. **App** [SASTL22]. **Appliances** [WMY20]. **Applications** [GLTW23, OMHY20, SASTL22]. **Applied** [SRA24]. **Approach** [ANM23, MVM22, XNC^{+}23]. **Apps** [GTL^{+}20]. **APTHunter** [MMY23]. **Architecture** [LT23]. **ARIMA** [KB20]. **Artifact** [DH22]. **Artifacts** [DIPQ22]. **Artificial** [WASC22]. **Asm2Seq** [TDZ^{+}24]. **Assembly** [TDZ^{+}24]. **Assessing** [HAH^{+}21, LRMZA21]. **Assessment** [BIG^{+}23]. **Assets** [SLBC21]. **Assisted** [KIP21]. **Assurance** [KB20]. **ATFuzzer** [KCH^{+}20]. **ATT&CK** [DRS24]. **Attack** [ACS23, DD20, HMD24, LHH22, SKM^{+}20, Sun22]. **Attacks** [AVS^{+}22, AAF^{+}22, Bur20, CFQP23, CC23, DKP21, HND^{+}22, LCTC23, OMHY20, PMP20, RBA^{+}23]. **Audit** [GSS21, OWY^{+}23]. **Authentication** [BFF^{+}23, KIP21, LZ23, Sun22]. **Automated** [DRS24, HSZ^{+}23, KPBZ21, SMK20]. **Automatic** [KVB23, UOI^{+}21]. **Automation** [BSM^{+}22]. **Available** [BOI^{+}23]. **aware** [LSK^{+}22, MBP22, SBU21]. **Awareness** [APY21, DRS^{+}21, GDP20, KB20, SLBC21]. **AZSecure** [SLBC21].

Back [KVB23]. **Based** [ABA23, BKS23, DD20, MB23, RBA^{+}23, AYP^{+}21, BOI^{+}23, Bur20, CLH^{+}22, DKP21, GLTW23, HMD24, KIP21, LWS^{+}23, LZ23, RVD^{+}21]. **Battery** [SASTL22]. **Battery-consuming** [SASTL22]. **Behavior** [SNA^{+}23]. **Behaviors** [GLTW23]. **Behavioural** [IKT^{+}21]. **Benchmark** [KPBZ21]. **Benefits** [KGH^{+}22]. **Best** [BCC^{+}22]. **Better** [Sac20, SPM23, Van21]. **Beyond** [BOI^{+}23, VS20]. **BGP** [vHvdHdVvRD23]. **Biases** [DWN21]. **Binaries** [UOI^{+}21]. **Binary** [ADJ^{+}20, DIPQ22, FRF22]. **Biometrics** [IKT^{+}21, SKM^{+}20]. **Blockchain** [Ami21, MMT^{+}21]. **Blocklisting** [MS21]. **Botnet** [BMOV23]. **Bots** [IKT^{+}21]. **Breaking** [BIG^{+}23]. **Broken** [How23]. **BUDS** [SPM23]. **Building** [CLH^{+}22, UOI^{+}21]. **Buses** [RBA^{+}23].

Campaigns [CTA^{+}23]. **Campus** [HLP22]. **Capability** [AFS^{+}22]. **Captcha** [BIG^{+}23]. **Card** [GSS21]. **Card-style** [GSS21]. **Case** [HSZ^{+}23]. **Catch** [SPV23]. **CDN** [SMY23]. **CDN-to-Origin** [SMY23]. **CDNs** [SMY23]. **Centers** [RCGA22]. **Central** [BPP22]. **Centrality** [APY21]. **Centralized** [BCC^{+}22]. **Centric** [SGH23]. **Ceph** [BD23]. **Certain** [Bur20]. **Certificate** [UKM20]. **Certificates** [GPFV23]. **Chain** [CC23]. **Challenges** [RUPT22]. **Changepoint** [SNA^{+}23]. **Channel** [DD20, CFQP23, MCH23, OMHY20]. **Character** [MBP22]. **Characterization** [Bur20]. **Chat** [OASD^{+}22]. **Chosen** [Sun22]. **Circular** [JDCK22]. **Cities** [JDCK22]. **Claim** [KPBZ21]. **Classification** [HOGF23, PCG24]. **Classifying** [LBG23]. **Clinical** [OWY^{+}23]. **Clustering** [PCG24]. **Co** [LBG23]. **Co-resident** [LBG23]. **Code** [JYMJ22, MCH23, SRBS20, TDZ^{+}24]. **Codebases** [XZA^{+}23]. **Collaborative** [CKMB23]. **Collaboratively** [LRMZA21]. **Collection** [DHT22]. **Combining** [IKT^{+}21]. **Commercially** [BOI^{+}23]. **Commodity** [CPDH20]. **Communication** [CMLV24, RBA^{+}23]. **Comparative** [LCTC23]. **Competition** [GAS24]. **Components** [MCH23]. **Computer** [LBG23]. **Condensation** [AYP^{+}21]. **Condensation-based** [AYP^{+}21]. **Conference** [DvdH22]. **Confidentiality**

[MCH23]. **Conformity** [HGKS23]. **Connect** [Koo20]. **Connections** [SMY23]. **consensual** [FT23]. **Consistent** [KPBZ21]. **Conspicuous** [DIPQ22]. **consuming** [SASTL22]. **Contact** [BCC+22, SCJ+22, SASTL22]. **Contention** [LBG23]. **Context** [SBU21, ST20, VSV+21]. **Context-aware** [SBU21]. **Context-sensitive** [ST20]. **Contexts** [LSK+22]. **Contextualized** [ITZ23]. **Continuous** [Sac20]. **Control** [DKP21, GLS21, LSK+22]. **Control-based** [DKP21]. **Controllers** [AMS23]. **Converger** [SPM23]. **Cookies** [SRBS20]. **Coordinated** [WS23]. **Coping** [VSV+21]. **Correlation** [CTA+23, SKM+20]. **Countermeasures** [CYGL20, FRF22]. **Counters** [ACS23, CFQP23]. **COVID** [GPFV23, KGH+22, KMGR22, SCJ+22, SASTL22]. **COVID-19** [GPFV23, KGH+22, KMGR22, SCJ+22, SASTL22]. **CPS** [ANM23]. **Credible** [HZB21]. **Cryptographic** [XZA+23]. **CSIRTs** [KLA23]. **Cues** [VSV+21]. **Cut** [GLS21]. **Cut-and-Mouse** [GLS21]. **CVE** [Koo20]. **CVE-2019-11510** [Koo20]. **CVSS** [How23]. **Cyber** [APY21, BSM+22, DHT22, EMS+23, HTRO24, HMD24, KLA23, LSK+22, SBL22, SLBC21]. **Cyber-Physical** [HMD24, LSK+22]. **Cybersecurity** [ALM+23, AFS+22, GDP20, LRMZA21, Van21].

Dark [CKMB23, SLBC21, SMY23]. **Darkweb** [GPFV23]. **Data** [AYP+21, BSM+22, CKMB23, GSS21, GBB23, ITZ23, KLA23, LWS+23, MBP22, MB23, OWY+23, PMP20, SDA+22, XNC+23, dWBvdH22]. **Data-only** [PMP20]. **Database** [ST20]. **Datasets** [ABA23]. **DDoS** [Bur20]. **Debloating** [ADJ+20]. **Decentralized** [BCC+22]. **Deception** [HBRV+21]. **Decision** [HAH+21, KGH+22]. **Decrease** [GSS21]. **Deep** [BIG+23, RVD+21]. **Deepfake** [HND+22]. **Defences** [HBRV+21]. **Defenders** [SBL22]. **Delivery** [LRMZA21]. **Demonstrating** [Tsu24]. **Deployments** [Moz22]. **Desire** [BCC+22]. **Detailed** [BE23]. **Detect** [FRF22]. **Detecting** [MMY23]. **Detection** [ABA23, AMS23, ACS23, AAF+22, CFQP23, DKP21, EMS+23, HMD24, HSZ+23, HND+22, IKT+21, KPBZ21, LWS+23, MVM22, MS21, RVD+21, SNA+23, SMK20, ST20, VS20, WASC22, ZYW22, ZJPZ20, dWBvdH22]. **Detectors** [BOI+23]. **Developing** [KPBZ21]. **Device** [RRF+23]. **Device-agnostic** [RRF+23]. **Devices** [ANM23, SNA+23]. **Devising** [BE23]. **Different** [DH22]. **Differential** [AYP+21]. **Digital** [AG23, BPP22, GBB23, GH23, ITZ23, LM20, SMK20]. **Dimensions** [ZSS22]. **Direct** [DH22]. **Directional** [APY21]. **Dirichlet** [ZYW22]. **Disclosure** [WS23]. **Disclosures** [HS22]. **Discovery** [ITZ23]. **Discussion** [GBB23, LT23]. **Discussions** [KLA23]. **Dispensable** [GBB23]. **Dissected** [ZBF22]. **Dissemination** [KVB23]. **DNS** [Bur20, NPT21, WC22]. **DNS-based** [Bur20]. **DNS-over-TLS** [NPT21]. **Documenting** [GAS24]. **Documents** [CTA+23, SMK20, WS23]. **Does** [SASTL22]. **Doing** [BPP22]. **Domain** [DSV+21, HZB21, MS21]. **Driven** [JDCK22, ZJPZ20]. **During** [HLP22]. **Dynamic** [DIPQ22, FRF22, KCH+20, KMPS23, RGK23, dWBvdH22].

E-Voting [MMT+21]. **Early** [ACS23, LLM20, MMY23, ZJPZ20]. **Economics** [CC23]. **Ecosystem** [MS21]. **Editorial** [LM20, Met21]. **EEG** [SKM+20]. **Effective** [BE23, CMLV24]. **Efficient** [RKC+24]. **Election** [Met21]. **ELF** [TCBK20]. **Embedded** [AMS23]. **Embeddings** [RKC+24]. **Emerging** [AFS+22, KIP21]. **Emotets** [BMOV23].

Enabling [BSM^{+}22]. **Encrypted** [MBP22]. **Encryption** [MCH23]. **Energy** [LRMZA21]. **Engine** [UOI^{+}21]. **Engineering** [TDZ^{+}24, UOI^{+}21]. **Engines** [RGK23]. **Enhancements** [HTRO24]. **Enough** [KGH^{+}22]. **Ensemble** [ABA23]. **Enterprise** [SDA^{+}22, WMY20, RBA^{+}23]. **Enterprise-IoT** [RBA^{+}23]. **Environments** [AVS^{+}22, SGH23]. **EPSS** [JRE^{+}21]. **Europe** [BPP22]. **Evading** [GAS24]. **Evaluate** [KLA23]. **Evaluating** [DIPQ22]. **Evaluation** [BOI^{+}23]. **Evaluations** [DD20]. **Evasion** [FRF22, GAS24]. **Evidence** [CTA^{+}23, GH23]. **Evolving** [LCTC23]. **Examination** [BD23]. **Examining** [ABA23]. **Exchange** [BSM^{+}22]. **Execution** [AVS^{+}22]. **Exertion** [BIG^{+}23]. **Exfiltration** [MB23]. **Experience** [GAS24, XZA^{+}23]. **Experimenting** [RCGA22]. **Experts** [HZB21]. **Explainable** [TDZ^{+}24]. **Exploit** [JRE^{+}21]. **Exploitation** [GTL^{+}20]. **Exploiting** [GLS21]. **Exploring** [CMLV24]. **Exposing** [HND^{+}22]. **Exposure** [JDCK22, KVB23]. **Expressiveness** [GH23]. **ExSol** [LRMZA21]. **Extended** [UKM20]. **Extortions** [MB23].

Factchecking [KPBZ21]. **Factorization** [EMS^{+}23]. **Fake** [VSV^{+}21, ZLPA21, ZJPZ20]. **False** [Sac20]. **Family** [PCG24]. **Faulty** [AVS^{+}22]. **Feature** [ABA23]. **Features** [DIPQ22, TCBK20]. **Field** [BPP22, GAS24, Koo20, Moz22, SASTL22]. **Fight** [CFQP23]. **Files** [KVB23]. **Financial** [HZB21]. **Finding** [XZA^{+}23]. **Findings** [KLA23]. **Fine** [LSK^{+}22]. **Fine-grained** [LSK^{+}22]. **Fingerpointing** [Sac20]. **Fingerprinting** [SPV23]. **FIRST** [DvdH22, CV20]. **Flies** [JYMJ22]. **Focus** [KLA23]. **Forecasting** [LRW22]. **Forensic** [BD23, HOGF23]. **Forensics** [GBB23]. **Formal** [GH23]. **Forth** [KVB23]. **Forth-On** [KVB23]. **Foundations** [ZBF22]. **Framework** [BE23, CFZK23, KCH^{+}20, KMPS23, SBU21, SPV23, TCBK20]. **Frameworks** [FRF22]. **Function** [VPG^{+}23]. **Functional** [HOGF23, TDZ^{+}24]. **Fusion** [ITZ23, OWY^{+}23]. **Fuzzing** [CMLV24, RRF^{+}23].

Gait [KIP21]. **GALU** [CFZK23]. **Gaps** [AFS^{+}22, GDP20]. **General** [EMS^{+}23]. **General-purpose** [EMS^{+}23]. **Generation** [LHH22, MS21, TDZ^{+}24]. **Genetic** [CFZK23]. **Ghost** [GLS21]. **Goals** [VV22]. **Good** [KGH^{+}22]. **Goosewolf** [AMS23]. **Gotta** [SPV23]. **Government** [BIG^{+}23]. **grained** [LSK^{+}22]. **Graph** [JM24, LHH22]. **Graybox** [ST20]. **Greater** [WS23]. **Group** [KLA23, OASD^{+}22].

Hacker [SLBC21]. **Handling** [HLP22]. **Hardware** [ACS23, AG23, CFQP23]. **Hawkes** [ZYW22]. **HDP** [HMD24]. **HDP-HMM** [HMD24]. **Heterogeneous** [Moz22]. **HiPeR** [ACS23]. **Histories** [HS22]. **History** [SRBS20]. **HMM** [HMD24]. **Home** [SBU21]. **Honeypot** [SPV23]. **Horizon** [VS20]. **Host** [RVD^{+}21]. **Host-based** [RVD^{+}21]. **Hunting** [CLH^{+}22, HTRO24]. **Hybrid** [ABA23, LHH22]. **Hybrid-Ensemble** [ABA23]. **Hype** [BOI^{+}23].

Identification [LLM20, VPG^{+}23]. **Identifying** [HZB21]. **IMF** [DS23]. **Impact** [DH22, KGH^{+}22]. **Impacts** [ABA23]. **Implementation** [RRF^{+}23]. **Implications** [HOGF23]. **Improvement** [Sac20]. **Improving** [ANM23, DRS24]. **Inaugural** [LM20]. **Incident** [KLA23]. **independent** [SBU21]. **Indian** [BIG^{+}23]. **Industrial** [AFS^{+}22, XZA^{+}23]. **Inference** [SKM^{+}20, SDA^{+}22]. **Information** [HMS23, ITZ23, LBG23, SRA24, SGH23]. **Informative** [ABA23]. **Informing**

[SLBC21]. **Infrastructure** [vHvdHdVvRD23, BMOV23]. **Input** [SDA+22]. **Inputs** [GLS21]. **Inroduction** [ZLPA21]. **Insider** [Ano22, WASC22, ZYW22]. **Insiders** [ZBF22]. **Instrumentation** [DIPQ22, FRF22]. **Integrate** [Sac20]. **Integrated** [CC23]. **Intelligence** [BSM+22, CKMB23, DHT22, JDCK22, SLBC21, ZSS22]. **Intelligent** [SBL22]. **Interception** [ST20, WMY20]. **Interdisciplinary** [FT23]. **Interface** [KCH+20]. **Internet** [AFS+22, HLP22]. **Interpreting** [HS22]. **Introduction** [Ano22, ACHC+23, AG23, BKS23, CV20, DvdH22, DS23, DRS+21, HMS23, KMGR22, MNP+22, PLD+20, PLD+21, PLS22, RUPT22, SES22]. **Intrusion** [AMS23, AAF+22, CPDH20, DKP21, HSZ+23, LWS+23, RVD+21]. **Invasion** [HLP22]. **Investigating** [BSM+22]. **Investigation** [VSV+21]. **InviSeal** [KMPS23]. **Invoking** [WASC22]. **IoT** [ANM23, LZ23, MVM22, Moz22, RBA+23, SES22, TCBK20]. **IronNetInjector** [RGK23]. **Issue** [Ano22, ACHC+23, AG23, BKS23, CV20, DvdH22, DS23, HMS23, ITZ23, KMGR22, LM20, MNP+22, Met21, PLD+20, PLD+21, PLS22, RUPT22, SES22].

JIT [Moz22]. **Just** [HS22, SASTL22].

Keeping [BMOV23]. **Key** [DHT22, vHvdHdVvRD23]. **Know** [BE23]. **Knowledge** [BSM+22, HTRO24].

Label [WC22]. **Labeling** [DRS24]. **Language** [RGK23]. **Laplacian** [APY21]. **Large** [ADJ+20, Moz22, XZA+23]. **Large-Scale** [Moz22, ADJ+20, XZA+23]. **LAVA** [BFF+23]. **Layer** [MVM22]. **Leakage** [DD20]. **Leakage-Based** [DD20]. **Learned** [HSZ+23, LZ23]. **Learning** [ABA23, ALM+23, BIG+23, BOI+23, Bur20, CBB+24, CLH+22, GAS24, RVD+21, SRA24, SNA+23, SMK20, TCBK20, dWBvdH22]. **Learning-Based** [ABA23, BOI+23, CLH+22]. **Legal** [HOGF23]. **Less** [GSS21]. **Lessons** [HSZ+23, LZ23]. **Leveraging** [BCC+22]. **LGuard** [RBA+23]. **Libraries** [ADJ+20]. **Lifecycle** [SBL22, SES22]. **limiting** [GSS21]. **Locally** [JM24]. **Log** [BFF+23, LWS+23]. **Logic** [AMS23, CFZK23]. **Logs** [IKT+21]. **Longitudinal** [SCJ+22]. **Looking** [VS20]. **Lucky** [HS22].

MAC [MVM22]. **MAC-Layer** [MVM22]. **Machine** [ALM+23, BOI+23, CBB+24, CLH+22, GAS24, SRA24, SNA+23, TCBK20, dWBvdH22]. **Malicious** [CTA+23, DSV+21, SMK20]. **Malware** [BKS23, BOI+23, Bur20, DRS24, LLM20, PCG24, RUPT22, RKC+24, TCBK20, dWBvdH22]. **Mapping** [FT23]. **Marked** [ZYW22]. **Marketplaces** [CKMB23]. **Matching** [MBP22]. **Material** [DHT22]. **May** [SASTL22]. **Measure** [WASC22]. **Media** [DWN21]. **Meets** [MCH23]. **Memory** [BKS23, PMP20]. **Memory-Based** [BKS23]. **Memory-resident** [PMP20]. **Menace** [LCTC23]. **Methodology** [RCGA22]. **Methods** [RVD+21]. **Metric** [RKC+24]. **Metrics** [KB20]. **Mid** [LCTC23]. **Mid-pandemic** [LCTC23]. **Minimal** [BIG+23]. **Mitigating** [MB23, PMP20]. **Mitigation** [CFQP23, HTRO24, WASC22]. **Mobile** [dWBvdH22]. **Model** [BSM+22, SMK20, SKM+20, ZJPZ20]. **Modeling** [AAF+22, SDA+22]. **Modelling** [AEA+23]. **Models** [GAS24]. **Modular** [LWS+23]. **Monitoring** [BPP22, Sac20]. **Mouse** [GLS21, IKT+21]. **Moving** [MVM22]. **Multi** [BMOV23, ITZ23]. **Multi-infrastructure** [BMOV23]. **Multimodal** [HMD24]. **Multiple** [MB23].

Multistage [SPV23].

Name [DSV+21]. **National** [KLA23]. **Native** [GLTW23]. **Native-based** [GLTW23]. **Nature** [ABA23, DRS+21]. **negative** [EMS+23]. **Netherlands** [Koo20]. **Network** [AYP+21, AAF+22, HBRV+21, HLP22, XNC+23]. **Networks** [CC23, JM24, WASC22]. **Neural** [JM24, WASC22]. **News** [DWN21, VSV+21, ZLPA21, ZJPZ20]. **Noisy** [SPM23]. **Non** [EMS+23, FT23]. **Non-consensual** [FT23]. **Non-negative** [EMS+23]. **Note** [BPP22, GAS24, Koo20, Moz22]. **Notes** [SASTL22]. **Novel** [Moz22]. **Number** [Tsu24].

OATs'inside [GLTW23]. **Obfuscated** [GLTW23]. **Object** [GLTW23]. **Off** [WC22]. **Off-Label** [WC22]. **Office** [CTA+23]. **One** [SASTL22]. **Online** [CYGL20]. **only** [PMP20]. **onto** [DH22]. **Opcode** [TCBK20]. **Operating** [CPDH20]. **Operation** [RCGA22]. **Operational** [DSV+21, SGH23]. **Opinion** [SCJ+22]. **Opportunities** [GDP20]. **Organizational** [SDA+22]. **Origin** [KVB23, SMY23]. **Originating** [Tsu24]. **Other** [BKS23]. **Outsourced** [MBP22]. **Overview** [AFS+22].

pandemic [LCTC23]. **Part** [PLD+20]. **Passive** [DHT22]. **Past** [SRBS20]. **Pattern** [MBP22]. **PDoT** [NPT21]. **People** [UKM20]. **Perceptions** [OASD+22, UKM20]. **Perfect** [DWN21]. **Performance** [ACS23, CFQP23]. **Persistent** [LLM20, MMY23]. **Personality** [YCG+23]. **Perspective** [HLP22, VV22]. **Perspectives** [FT23, ZLPA21]. **Phishing** [ABA23, GAS24]. **Physical** [HMD24, LSK+22]. **Physically** [VPG+23]. **Pipeline** [LWS+23]. **Pitaya** [DD20]. **Platform** [HSZ+23, SBU21]. **Platform-independent** [SBU21]. **Point** [AVS+22]. **Poisoning** [AVS+22]. **Policy** [WS23]. **Polymorphism** [MCH23]. **Pornography** [FT23]. **Portal** [SLBC21]. **Positives** [Sac20]. **Possible** [HS22]. **Power** [DD20]. **Practical** [DD20, LHH22]. **Practice** [Ami21, LM20, LRW22, ZSS22]. **Pre** [LCTC23]. **Pre-pandemic** [LCTC23]. **Predator** [AEA+23]. **Prediction** [JRE+21]. **Premadoma** [DSV+21]. **Prevalence** [HGKS23]. **Prevent** [DSV+21]. **Prevention** [MVM22]. **Prey** [AEA+23]. **Privacy** [AYP+21, KGH+22, KMGR22, MBP22, OASD+22, SPM23, SCJ+22]. **Privacy-aware** [MBP22]. **Private** [JM24, NPT21]. **Proactive** [VS20]. **Problems** [CBB+24, SMY23]. **Process** [SBL22]. **Processes** [ZYW22]. **Processing** [SRBS20]. **Programmable** [AMS23]. **Programs** [LBG23]. **Project** [BPP22]. **Proposing** [BSM+22]. **Proprietary** [RBA+23]. **Protected** [DKP21]. **Protecting** [LRMZA21, PMP20]. **Protection** [MCH23]. **Protocol** [RRF+23, Sun22]. **Protocols** [CMLV24, LZ23]. **Psychological** [DWN21]. **Public** [SCJ+22, vHvdHdVvRD23]. **PUF** [LZ23]. **PUF-based** [LZ23]. **Pulse** [Koo20]. **purpose** [EMS+23].

Quality [KB20, ZSS22]. **Quantifying** [KGH+22]. **Quantitative** [FT23].

Random [Sun22]. **Randomized** [JYMJ22, MVM22]. **Ransomware** [ACS23, ACHC+23, AEA+23, BE23, CC23, LCTC23, MB23, YCG+23]. **Real** [BIG+23, HZB21]. **Real-time** [BIG+23]. **Real-world** [HZB21]. **Realistic** [AAF+22, GBB23]. **Redacted** [SDA+22]. **Registrations** [DSV+21]. **Relevanceof** [GH23]. **Reports** [DRS24]. **Repositories** [DH22]. **Representation** [BSM+22]. **Request** [SRBS20]. **Research**

[AFS+22, FT23, LM20, SASTL22, ZLPA21, ZSS22, ZBF22]. **resident** [LBG23, PMP20]. **Resource** [LBG23, OMHY20, vHvdHdVvRD23]. **Response** [BE23, KLA23]. **Results** [WASC22]. **Retrieving** [GLTW23]. **Revealed** [LBG23]. **Reverse** [TDZ+24, UOI+21]. **Reviewing** [PCG24]. **Revisited** [HGKS23]. **Rights** [BPP22]. **Risk** [AEA+23, BIG+23, GSS21, LT23, LSK+22]. **Risk-aware** [LSK+22]. **Risk-limiting** [GSS21]. **Risks** [LRMZA21]. **Robotic** [DKP21]. **Robust** [HND+22]. **Role** [ALM+23]. **rpkiller** [vHvdHdVvRD23]. **Runtime** [RGK23]. **Russian** [HLP22].

SABU [HSZ+23]. **SAE** [Sun22]. **SAIBERSOC** [RCGA22]. **Sample** [GSS21]. **SCA** [DD20]. **SCA-Pitaya** [DD20]. **Scale** [Moz22, ADJ+20, XZA+23]. **Schema** [KPBZ21]. **Scoring** [JRE+21]. **Scratch** [CLH+22]. **Script** [UOI+21]. **Scrybe** [OWY+23]. **Secure** [Koo20, MMT+21, OWY+23, XNC+23]. **Securely** [JYMJ22]. **Securing** [OMHY20, RBA+23]. **Security** [ANM23, AG23, CBB+24, GAS24, KMGR22, KB20, Met21, Moz22, OASD+22, RRF+23, RCGA22, Sac20, SRA24, SMY23, SBU21, SGH23, WMY20, SES22]. **security.txt** [HGKS23]. **Seem** [SASTL22]. **Selection** [ABA23]. **Self** [XNC+23]. **Self-adaptive** [XNC+23]. **Sending** [Tsu24]. **Sensitive** [PMP20, ST20]. **Sensor** [ITZ23, KIP21, VPG+23]. **Sensor-based** [KIP21]. **Serial** [RBA+23]. **Serial-Based** [RBA+23]. **Series** [HMD24]. **Server** [SRBS20]. **Server-side** [SRBS20]. **Setup** [DD20]. **Share** [XNC+23]. **Shared** [ADJ+20]. **Sharing** [BSM+22, HMS23, HSZ+23, JYMJ22, VSV+21]. **Shuffling** [SPM23]. **Side** [CFQP23, DD20, MCH23, OMHY20, SMY23, SRBS20]. **Side-Channel** [DD20, CFQP23, MCH23, OMHY20]. **Simulating** [SDA+22]. **Simulation** [MB23]. **Simulations** [HTRO24]. **Single** [ABA23]. **Situational** [APY21, DRS+21, GDP20, KB20, SLBC21]. **Sizes** [GSS21]. **Skillful** [HS22]. **Smart** [JDCK22, SBU21]. **Smartphone** [SNA+23, dWBvdH22]. **Smartphones** [KCH+20]. **SMPP** [Tsu24]. **SMS** [Tsu24]. **Sniffing** [SRBS20]. **SOC** [HAH+21]. **Social** [DWN21]. **Software** [GLS21, MCH23]. **Solution** [DSV+21]. **Sorry** [WMY20]. **Southeast** [BPP22]. **Special** [Ano22, ACHC+23, AG23, BKS23, CV20, DvdH22, DS23, HMS23, ITZ23, KMGR22, MNP+22, Met21, PLD+20, PLD+21, PLS22, RUPT22, SES22]. **Spoofability** [Tsu24]. **Spoofing** [KIP21, MVM22]. **SSH** [DHT22]. **SSL** [Koo20]. **SSL-VPN** [Koo20]. **Stages** [MMY23]. **State** [WMY20]. **Stealthy** [DKP21, KMPS23]. **Sticky** [HMD24]. **Storage** [HOGF23]. **Stored** [ST20]. **Storm** [DWN21]. **Strategies** [BE23, CMLV24, LHH22]. **Stream** [CBB+24]. **Structurally** [JM24]. **Study** [SCJ+22]. **Style** [GSS21]. **Summary** [TDZ+24]. **Supplemented** [KB20]. **Supply** [CC23]. **Support** [HAH+21, NPT21]. **Survey** [CYGL20]. **Survivability** [CPDH20]. **SwissCovid** [VV22]. **Synthesized** [GLS21]. **Synthetic** [GBB23]. **System** [AMS23, BIG+23, CLH+22, JRE+21]. **Systematisation** [ZBF22]. **Systemic** [AEA+23]. **Systems** [AAF+22, BCC+22, CPDH20, DIPQ22, HMD24, HND+22, KMPS23, LRMZA21, MVM22, RBA+23, SBU21]. **Systemwide** [CFQP23].

Tactics [DRS24]. **TAGS** [KIP21]. **Target** [MVM22]. **Technical** [CYGL20, FT23]. **Technique** [ABA23]. **Techniques** [Bur20, DKP21, FRF22, PCG24, SNA+23].

Technology [SGH23]. **TEE** [NPT21]. **Tensor** [EMS+23]. **Testing** [SGH23]. **Theory** [LRW22, ZJPZ20]. **Theory-driven** [ZJPZ20]. **Things** [AFS+22]. **Thinking** [SKM+20]. **Thoughts** [VS20]. **Threat** [BSM+22, CLH+22, CKMB23, DRS24, DHT22, HTRO24, ITZ23, KIP21, LLM20, MB23, SLBC21, VSV+21, WASC22, ZYW22, ZSS22, vHvdHdVvRD23]. **Threat-Based** [MB23]. **Threats** [Ano22, AG23, BKS23, CYGL20, LM20, MMY23, VS20]. **Thwart** [GTL+20]. **Thy** [BE23]. **Time** [HMD24, BIG+23]. **Timing** [SRBS20]. **TLD** [DSV+21]. **TLS** [NPT21, UKM20, WMY20]. **Tool** [HAH+21, RCGA22]. **Tools** [KLA23]. **Trace** [XNC+23]. **Tracers** [UOI+21]. **Traces** [AYP+21]. **Tracing** [BCC+22, SCJ+22, SASTL22]. **Tracking** [BMOV23]. **Traffic** [ST20]. **Trail** [OWY+23]. **Transitive** [DH22]. **Treadmill** [KIP21]. **Treatment** [GH23]. **Trends** [RUPT22, ZLPA21]. **Triage** [LLM20]. **Trial** [OWY+23]. **Trust** [LT23, UKM20]. **Trusted** [AVS+22]. **Types** [YCG+23].

Ubiquitous [How23]. **Ukraine** [HLP22]. **Unclonable** [VPG+23]. **Unconventional** [BKS23]. **Understanding** [Bur20, KLA23, Van21, WS23]. **Unit** [AVS+22]. **Unless** [SASTL22]. **Unlocking** [CFZK23]. **Unpredictability** [HBRV+21]. **Unsupervised** [Bur20, EMS+23]. **Unveiled** [SKM+20]. **Use** [WC22]. **Useless** [SASTL22]. **User** [OASD+22]. **Using** [CFQP23, HBRV+21, ITZ23, LBG23, RKC+24, TCBK20, ZYW22, dWBvdH22, ACS23, SNA+23, Tsu24].

Vaccination [GPFV23]. **Value** [Sun22]. **Varied** [ABA23]. **Vehicles** [DKP21]. **Verification** [BFF+23]. **Version** [UKM20]. **Veto** [OMHY20]. **Vetting** [GTL+20]. **via** [EMS+23, RRF+23, RBA+23, VPG+23]. **Victimisation** [YCG+23]. **Virus** [VSV+21]. **Visual** [CTA+23]. **Vol** [PLD+21]. **Voting** [MMT+21]. **VPN** [Koo20]. **Vulnerabilities** [Ami21, DH22, GTL+20, HND+22, MNP+22, XZA+23]. **Vulnerability** [HTRO24, HS22, JDCK22, LRW22, TDZ+24, WS23]. **Vulvet** [GTL+20].

Weaponizing [RGK23]. **Wearable** [KIP21]. **Web** [CKMB23, IKT+21, SLBC21]. **Website** [ABA23]. **Websites** [BIG+23]. **Will** [UKM20]. **Willingness** [KGH+22]. **Windows** [KVB23]. **within** [SGH23]. **Work** [GSS21]. **Working** [UKM20]. **world** [HZB21]. **WPA3** [Sun22].

XSS [ST20].

Zero [LT23]. **Zigbee** [RRF+23]. **Zika** [VSV+21].

References

Apruzzese:2022:MRA

[AAF+22] Giovanni Apruzzese, Mauro Andreolini, Luca Ferretti, Mirco Marchetti, and Michele Colajanni. Modeling realistic adversarial attacks against network intrusion detection systems. *Digital Threats: Research and Practice (DTRAP)*, 3(3):31:1–31:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3469659`.

Adane:2023:SHE

[ABA23] Kibreab Adane, Berhanu Beyene, and Mohammed

Abebe. Single and hybrid-ensemble learning-based phishing Website detection: Examining impacts of varied nature datasets and informative feature selection technique. *Digital Threats: Research and Practice (DTRAP)*, 4(3):46:1–46:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3611392`.

Arief:2023:ISI

[ACHC+23] Budi Arief, Lena Connolly, Julio Hernandez-Castro, Allan Liska, and Peter Y. A. Ryan. Introduction to the special issue on ransomware. *Digital Threats: Research and Practice (DTRAP)*, 4(4):51:1–51:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3629999`.

Anand:2023:HED

[ACS23] P. Mohan Anand, P. V. Sai Charan, and Sandeep K. Shukla. HiPeR — early detection of a ransomware attack using hardware performance counters. *Digital Threats: Research and Practice (DTRAP)*, 4(3):43:1–43:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3608484`.

Agadakos:2020:LSD

[ADJ+20] Ioannis Agadakos, Nicholas Demarinis, Di Jin, Kent Williams-King, Jearson Alfajardo, Benjamin Shteinfeld, David Williams-King, Vasileios P. Kemerlis, and Georgios Portokalidis. Large-scale debloating of binary shared libraries. *Digital Threats: Research and Practice (DTRAP)*, 1(4):19:1–19:28, December 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3414997`.

Axon:2023:RPM

[AEA+23] Louise Axon, Arnau Erola, Ioannis Agrafiotis, Ganbayar Uuganbayar, Michael Goldsmith, and Sadie Creese. Ransomware as a predator: Modelling the systemic risk to prey. *Digital Threats: Research and Practice (DTRAP)*, 4(4):55:1–55:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https:`

//dl.acm.org/doi/10.1145/3579648.

Axon:2022:ECC

[AFS+22] Louise Axon, Katherine Fletcher, Arianna Schuler Scott, Marcel Stolz, Robert Hannigan, Ali El Kaafarani, Michael Goldsmith, and Sadie Creese. Emerging cybersecurity capability gaps in the industrial Internet of Things: Overview and research agenda. *Digital Threats: Research and Practice (DTRAP)*, 3(4):34:1–34:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3503920`.

Aysu:2023:ISI

[AG23] Aydin Aysu and Scott R. Graham. Introduction to the special issue on the digital threats of hardware security. *Digital Threats: Research and Practice (DTRAP)*, 4(2):16:1–16:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3585011`.

Apruzzese:2023:RML

[ALM+23] Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Brdalo Rapa, Athanasios Vasileios Grammatopoulos, and Fabio Di Franco. The role of machine learning in cybersecurity. *Digital Threats: Research and Practice (DTRAP)*, 4(1):8:1–8:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3545574`.

Amiet:2021:BVP

[Ami21] Nils Amiet. Blockchain vulnerabilities in practice. *Digital Threats: Research and Practice (DTRAP)*, 2(2):8:1–8:7, March 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3407230`.

Allison:2023:GEI

[AMS23] David Allison, Kieran McLaughlin, and Paul Smith. Goosewolf: an embedded intrusion detection system for advanced programmable logic controllers. *Digital Threats: Research and Practice (DTRAP)*, 4(4):59:1–59:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3617692`.

Albasir:2023:TIS

[ANM23] Abdurhman Albasir, Kshirasagar Naik, and Ricardo Manzano. Toward improving the security of IoT and CPS devices: an AI approach. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):22:1–22:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3497862`.

Anonymous:2022:ISI

[Ano22] Anonymous. Introduction to the special issue on insider threats. *Digital Threats: Research and Practice (DTRAP)*, 3(1): 1:1–1:3, March 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3477501`.

Aksoy:2021:DLC

[APY21] Sinan G. Aksoy, Emilie Purvine, and Stephen J. Young. Directional Laplacian centrality for cyber situational awareness. *Digital Threats: Research and Practice (DTRAP)*, 2(4):28:1–28:28, December 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3450286`.

Alder:2022:FPU

[AVS+22] Fritz Alder, Jo Van Bulck, Jesse Spielman, David Oswald, and Frank Piessens. Faulty point unit: ABI poisoning attacks on trusted execution environments. *Digital Threats: Research and Practice (DTRAP)*, 3(2): 13:1–13:26, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3491264`.

Aleroud:2021:ANT

[AYP+21] Ahmed Aleroud, Fan Yang, Sai Chaithanya Pallaprolu, Zhiyuan Chen, and George Karabatis. Anonymization of network traces data through condensation-based differential privacy. *Digital Threats: Research and Practice (DTRAP)*, 2(4):30:1–30:23, December 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3425401`.

Boutet:2022:DLB

[BCC+22] Antoine Boutet, Claude Castelluccia, Mathieu Cunche, Cédric Lauradou, Vincent

Roca, Adrien Baud, and Pierre-Guillaume Raverdy. Desire: Leveraging the best of centralized and decentralized contact tracing systems. *Digital Threats: Research and Practice (DTRAP)*, 3 (3):28:1–28:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3480467`.

Bausch:2023:FEC

[BD23] Florian Bausch and Andreas Dewald. Forensic examination of Ceph. *Digital Threats: Research and Practice (DTRAP)*, 4(3):37:1–37:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3609862`.

Bajpai:2023:KTR

[BE23] Pranshu Bajpai and Richard Enbody. Know thy ransomware response: a detailed framework for devising effective ransomware response strategies. *Digital Threats: Research and Practice (DTRAP)*, 4(4):57:1–57:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3606022`.

Bajramovic:2023:LLA

[BFF+23] Edita Bajramovic, Christofer Fein, Marius Frinken, Paul Rösler, and Felix Freiling. LAVA: Log authentication and verification algorithm. *Digital Threats: Research and Practice (DTRAP)*, 4(3):35:1–35:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3609233`.

Bhowmick:2023:BCS

[BIG+23] Rajat Subhra Bhowmick, Rahul Indra, Isha Ganguli, Jayanta Paul, and Jaya Sil. Breaking Captcha system with minimal exertion through deep learning: Real-time risk assessment on Indian government Websites. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):28:1–28:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3584974`.

Botacin:2023:ISI

[BKS23] Marcus Botacin, Uriel Kosayev, and Ruimin Sun. Introduction to the special issue on memory-based malware and other unconventional threats. *Digital Threats: Research and Practice (DTRAP)*, 4(3):39:1–39:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3627521`.

Boyarchuk:2023:KET

[BMOV23] Oleg Boyarchuk, Sebastiano Mariani, Stefano Ortolani, and Giovanni Vigna. Keeping up with the emotets: Tracking a multi-infrastructure botnet. *Digital Threats: Research and Practice (DTRAP)*, 4(3):41:1–41:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3594554`.

Bridges:2023:BHE

[BOI+23] Robert A. Bridges, Sean Oesch, Michael D. Iannacone, Kelly M. T. Huffer, Brian Jewell, Jeff A. Nichols, Brian Weber, Miki E. Verma, Daniel Scofield, Craig Miles, Thomas Plummer, Mark Daniell, Anne M. Tall, Justin M. Beaver, and Jared M. Smith. Beyond the hype: an evaluation of commercially available machine learning-based malware detectors. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):27:1–27:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3567432`.

Bajic:2022:FND

[BPP22] Mila Bajić, Andrej Petrovski, and Bojan Perkov. Field note on doing digital rights: Central and Southeast Europe Monitoring Project. *Digital Threats: Research and Practice (DTRAP)*, 3(3):23:1–23:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3513024`.

Bromander:2022:ISC

[BSM+22] Siri Bromander, Morton Swimmer, Lilly Pijnenburg Muller, Audun Jøsang, Martin Eian, Geir Skjøtskift, and Fredrik Borg. Investigating sharing of cyber threat intelligence and proposing a new data model for enabling automation in knowledge representation and exchange. *Digital Threats: Research and Practice (DTRAP)*, 3(1): 6:1–6:22, March 2022. CODEN ???? ISSN 2692-

1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3458027.

Burton:2020:ULT

[Bur20] Renée Burton. Unsupervised learning techniques for malware characterization: Understanding certain DNS-based DDoS attacks. *Digital Threats: Research and Practice (DTRAP)*, 1(3):14:1–14:26, September 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3377869.

Ceschin:2024:MLS

[CBB+24] Fabrício Ceschin, Marcus Botacin, Albert Bifet, Bernhard Pfahringer, Luiz S. Oliveira, Heitor Murilo Gomes, and André Grégio. Machine learning (in) security: a stream of problems. *Digital Threats: Research and Practice (DTRAP)*, 5(1):9:1–9:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3617897.

Cartwright:2023:ERA

[CC23] Anna Cartwright and Edward Cartwright. The economics of ransomware attacks on integrated supply chain networks. *Digital Threats: Research and Practice (DTRAP)*, 4(4):56:1–56:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3579647.

Carna:2023:FHH

[CFQP23] Stefano Carnà, Serena Ferracci, Francesco Quaglia, and Alessandro Pellegrini. Fight hardware with hardware: Systemwide detection and mitigation of side-channel attacks using performance counters. *Digital Threats: Research and Practice (DTRAP)*, 4(1):5:1–5:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3519601.

Chen:2023:GGA

[CFZK23] Huili Chen, Cheng Fu, Jishen Zhao, and Farinaz Koushanfar. GALU: a genetic algorithm framework for logic unlocking. *Digital Threats: Research and Practice (DTRAP)*, 4(2):21:1–21:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3491256.

Connolly:2023:DWM

[CKMB23] Kate Connolly, Anna Klempay, Mary McCann, and Paul Brenner. Dark Web marketplaces: Data for collaborative threat intelligence. *Digital Threats: Research and Practice (DTRAP)*, 4 (4):49:1–49:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3615666`.

Chen:2022:BML

[CLH+22] Chung-Kuan Chen, Si-Chen Lin, Szu-Chun Huang, Yung-Tien Chu, Chin-Laung Lei, and Chun-Ying Huang. Building machine learning-based threat hunting system from scratch. *Digital Threats: Research and Practice (DTRAP)*, 3(3):20:1–20:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3491260`.

Chen:2024:EEF

[CMLV24] Yurong Chen, Yongsheng Mei, Tian Lan, and Guru Venkataramani. Exploring effective fuzzing strategies to analyze communication protocols. *Digital Threats: Research and Practice (DTRAP)*, 5(1): 11:1–11:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3526088`.

Chevalier:2020:ISC

[CPDH20] Ronny Chevalier, David Plaquin, Chris Dalton, and Guillaume Hiet. Intrusion survivability for commodity operating systems. *Digital Threats: Research and Practice (DTRAP)*, 1(4):21:1–21:30, December 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3419471`.

Casino:2023:ACV

[CTA+23] Fran Casino, Nikolaos Totosis, Theodoros Apostolopoulos, Nikolaos Lykousas, and Constantinos Patsakis. Analysis and correlation of visual evidence in campaigns of malicious Office documents. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):26:1–26:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3513025`.

Cormack:2020:IFS

[CV20] Andrew Cormack and Jeroen Van der Ham. Introduction to the FIRST special issue. *Digital Threats: Research and Practice (DTRAP)*, 1(1): 2:1–2:3, March 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3380746.

Cai:2020:TOA

[CYGL20] Yegui Cai, George O. M. Yee, Yuan Xiang Gu, and Chung-Horng Lung. Threats to online advertising and countermeasures: a technical survey. *Digital Threats: Research and Practice (DTRAP)*, 1 (2):11:1–11:27, July 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3374136.

Durvaux:2020:SPP

[DD20] François Durvaux and Marc Durvaux. SCA-Pitaya: a practical and affordable side-channel attack setup for power leakage-based evaluations. *Digital Threats: Research and Practice (DTRAP)*, 1 (1):3:1–3:16, March 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3371393.

Dusing:2022:ADT

[DH22] Johannes Düsing and Ben Hermann. Analyzing the direct and transitive impact of vulnerabilities onto different artifact repositories. *Digital Threats: Research and Practice (DTRAP)*, 3(4):38:1–38:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3472811.

Dulaunoy:2022:APC

[DHT22] Alexandre Dulaunoy, Jean-Louis Huynen, and Aurelien Thirion. Active and passive collection of SSH key material for cyber threat intelligence. *Digital Threats: Research and Practice (DTRAP)*, 3(3):19:1–19:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3491262.

DElia:2022:EDB

[DIPQ22] Daniele Cono D'Elia, Lorenzo Invidia, Federico Palmaro, and Leonardo Querzoni. Evaluating dynamic binary instrumentation systems for conspicuous features and artifacts. *Digital Threats: Research and Practice (DTRAP)*, 3 (2):10:1–10:13, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3478520`.

Dash:2021:SAA

[DKP21] Pritam Dash, Mehdi Karimibiuki, and Karthik Pattabiraman. Stealthy attacks against robotic vehicles protected by control-based intrusion detection techniques. *Digital Threats: Research and Practice (DTRAP)*, 2(1): 7:1–7:25, March 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3419474`.

Dykstra:2021:INS

[DRS+21] Josiah Dykstra, Neil Rowe, Timothy Shimeall, Angela Horneman, and Marisa Midler. Introduction: On the nature of situational awareness. *Digital Threats: Research and Practice (DTRAP)*, 2(4): 25:1–25:3, December 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3462334`.

Domschot:2024:IAL

[DRS24] Eva Domschot, Ramyaa Ramyaa, and Michael R. Smith. Improving automated labeling for ATT&CK tactics in malware threat reports. *Digital Threats: Research and Practice (DTRAP)*, 5(1):2:1–2:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3594553`.

Dewald:2023:IIS

[DS23] Andreas Dewald and Thomas Schreck. Introduction to the IMF 2023 special issue. *Digital Threats: Research and Practice (DTRAP)*, 4(3):31:1–31:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3626105`.

Desmet:2021:POS

[DSV+21] Lieven Desmet, Jan Spooren, Thomas Vissers, Peter Janssen, and Wouter Joosen. Premadoma: an operational solution to prevent malicious domain name registrations in the `.eu` TLD. *Digital Threats: Research and Practice (DTRAP)*, 2(1): 2:1–2:24, March 2021. CO-

DEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3419476.

Desidera:2022:ISI

[DvdH22] Lucimara Desiderá and Jeroen van der Ham. Introduction to the special issue on the 2020 FIRST Conference. *Digital Threats: Research and Practice (DTRAP)*, 3(3):18:1–18:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3549069.

deWit:2022:DDM

[dWBvdH22] J. S. Panman de Wit, D. Bucur, and J. van der Ham. Dynamic detection of mobile malware using smartphone data and machine learning. *Digital Threats: Research and Practice (DTRAP)*, 3(2): 9:1–9:24, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3484246.

Datta:2021:PSS

[DWN21] Pratim Datta, Mark Whitmore, and Joseph K. Nwankpa. A perfect storm: Social media news, psychological biases, and AI. *Digital Threats: Research and Practice (DTRAP)*, 2(2): 15:1–15:21, June 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3428157.

Eren:2023:GPU

[EMS+23] Maksim E. Eren, Juston S. Moore, Erik Skau, Elisabeth Moore, Manish Bhattarai, Gopinath Chennupati, and Boian S. Alexandrov. General-purpose unsupervised cyber anomaly detection via non-negative tensor factorization. *Digital Threats: Research and Practice (DTRAP)*, 4(1): 6:1–6:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3519602.

Filho:2022:ECT

[FRF22] Ailton Santos Filho, Ricardo J. Rodríguez, and Eduardo L. Feitosa. Evasion and countermeasures techniques to detect dynamic binary instrumentation frameworks. *Digital Threats: Research and Practice (DTRAP)*, 3(2): 11:1–11:28, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https:

//dl.acm.org/doi/10.1145/3480463.

Falduti:2023:MIR

[FT23] Mattia Falduti and Sergio Tessaris. Mapping the interdisciplinary research on non-consensual pornography: Technical and quantitative perspectives. *Digital Threats: Research and Practice (DTRAP)*, 4(3):44:1–44:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3608483.

Gao:2024:EAP

[GAS24] Yang Gao, Benjamin M. Ampel, and Sagar Samtani. Evading anti-phishing models: a field note documenting an experience in the machine learning security evasion competition 2022. *Digital Threats: Research and Practice (DTRAP)*, 5(1):7:1–7:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3603507.

Gobel:2023:DDF

[GBB23] Thomas Göbel, Harald Baier, and Frank Breitinger. Data for digital forensics: Why a discussion on "How Realistic is Synthetic Data" is dispensable. *Digital Threats: Research and Practice (DTRAP)*, 4(3):38:1–38:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3609863.

Gutzwiller:2020:GOS

[GDP20] Robert Gutzwiller, Josiah Dykstra, and Bryan Payne. Gaps and opportunities in situational awareness for cybersecurity. *Digital Threats: Research and Practice (DTRAP)*, 1(3):18:1–18:6, September 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3384471.

Gruber:2023:FTE

[GH23] Jan Gruber and Merlin Humml. A formal treatment of expressiveness and relevanceof digital evidence. *Digital Threats: Research and Practice (DTRAP)*, 4(3):33:1–33:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3608485.

Genc:2021:CMG

[GLS21] Ziya Alper Genç, Gabriele Lenzini, and Daniele Sgandurra. Cut-and-mouse and ghost control: Exploiting antivirus software with synthesized inputs. *Digital Threats: Research and Practice (DTRAP)*, 2(1): 4:1–4:23, March 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3431286`.

Graux:2023:ORO

[GLTW23] Pierre Graux, Jean-François Lalande, Valérie Viet Triem Tong, and Pierre Wilke. OATs'inside: Retrieving object behaviors from native-based obfuscated Android applications. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):30:1–30:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3584975`.

Georgoulias:2023:CVC

[GPFV23] Dimitrios Georgoulias, Jens Myrup Pedersen, Morten Falch, and Emmanouil Vasilomanolakis. COVID-19 vaccination certificates in the Darkweb. *Digital Threats: Research and Practice (DTRAP)*, 4(1):7:1–7:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3530877`.

Glazer:2021:MSL

[GSS21] Amanda K. Glazer, Jacob V. Spertus, and Philip B. Stark. More style, less work: Card-style data decrease risk-limiting audit sample sizes. *Digital Threats: Research and Practice (DTRAP)*, 2(4):32:1–32:15, December 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3457907`.

Gajrani:2020:VVV

[GTL+20] Jyoti Gajrani, Meenakshi Tripathi, Vijay Laxmi, Gaurav Somani, Akka Zemmari, and Manoj Singh Gaur. Vulvet: Vetting of vulnerabilities in Android apps to thwart exploitation. *Digital Threats: Research and Practice (DTRAP)*, 1(2): 10:1–10:25, July 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3376121`.

Happa:2021:ADS

[HAH+21] Jassim Happa, Ioannis Agrafiotis, Martin Helmhout, Thomas Bashford-Rogers, Michael Goldsmith, and Sadie Creese. Assessing a decision support tool for SOC analysts. *Digital Threats: Research and Practice (DTRAP)*, 2(3):22:1–22:35, September 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3430753`.

Happa:2021:DND

[HBRV+21] Jassim Happa, Thomas Bashford-Rogers, Alastair Janse Van Rensburg, Michael Goldsmith, and Sadie Creese. Deception in network defences using unpredictability. *Digital Threats: Research and Practice (DTRAP)*, 2(4):29:1–29:26, December 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3450973`.

Hilbig:2023:STR

[HGKS23] Tobias Hilbig, Thomas Geras, Erwin Kupris, and Thomas Schreck. `security.txt` revisited: Analysis of prevalence and conformity in 2022. *Digital Threats: Research and Practice (DTRAP)*, 4(3):36:1–36:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3609234`.

Husak:2022:HIA

[HLP22] Martin Husák, Martin Lastovicka, and Tomás Plesník. Handling Internet activism during the Russian invasion of Ukraine: a campus network perspective. *Digital Threats: Research and Practice (DTRAP)*, 3(3):17:1–17:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3534566`.

Hong:2024:TAD

[HMD24] Andrew E. Hong, Peter P. Malinovsky, and Suresh K. Damodaran. Towards attack detection in multimodal cyber-physical systems with sticky HDP-HMM based time series analysis. *Digital Threats: Research and Practice (DTRAP)*, 5(1):5:1–5:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3604434`.

Hueca:2023:ISI

[HMS23] Angel Hueca, Sharon Mudd, and Timothy Shimeall. Introduction to the special issue on information sharing. *Digital Threats: Research and Practice (DTRAP)*, 4(4):47:1–47:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3635391`.

Hussain:2022:EVD

[HND+22] Shehzeen Hussain, Paarth Neekhara, Brian Dolhansky, Joanna Bitton, Cristian Canton Ferrer, Julian McAuley, and Farinaz Koushanfar. Exposing vulnerabilities of deepfake detection systems with robust attacks. *Digital Threats: Research and Practice (DTRAP)*, 3(3):30:1–30:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3464307`.

Hammer:2023:FCF

[HOGF23] Andreas Hammer, Mathis Ohlig, Julian Geus, and Felix Freiling. A functional classification of forensic access to storage and its legal implications. *Digital Threats: Research and Practice (DTRAP)*, 4(3):32:1–32:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3609231`.

Howland:2023:CUB

[How23] Henry Howland. CVSS: Ubiquitous and broken. *Digital Threats: Research and Practice (DTRAP)*, 4 (1):1:1–1:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3491263`.

Householder:2022:WSJ

[HS22] Allen D. Householder and Jonathan Spring. Are we skillful or just lucky? Interpreting the possible histories of vulnerability disclosures. *Digital Threats: Research and Practice (DTRAP)*, 3(4):39:1–39:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3477431`.

Husak:2023:LLA

[HSZ+23] Martin Husák, Pavol Sokol, Martin Zádník, Václav Bartos, and Martin Horák. Lessons learned from automated sharing of intrusion detection alerts: The case of the SABU platform. *Digital Threats: Research and Practice (DTRAP)*, 4(4):48:1–48:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3611391`.

Hemberg:2024:ETV

[HTRO24] Erik Hemberg, Matthew J. Turner, Nick Rutar, and Una-May O'reilly. Enhancements to threat, vulnerability, and mitigation knowledge for cyber analytics, hunting, and simulations. *Digital Threats: Research and Practice (DTRAP)*, 5(1): 8:1–8:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3615668`.

Huang:2021:IRW

[HZB21] Teng-Chieh Huang, Razieh Nokhbeh Zaeem, and K. Suzanne Barber. Identifying real-world credible experts in the financial domain. *Digital Threats: Research and Practice (DTRAP)*, 2(2): 17:1–17:14, June 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3446783`.

Iliou:2021:DAW

[IKT+21] Christos Iliou, Theodoros Kostoulas, Theodora Tsikrika, Vasilis Katos, Stefanos Vrochidis, and Ioannis Kompatsiaris. Detection of advanced Web bots by combining Web logs with mouse behavioural biometrics. *Digital Threats: Research and Practice (DTRAP)*, 2(3):24:1–24:26, September 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3447815`.

Iyengar:2023:SIA

[ITZ23] S. S. Iyengar, Bhavani Thuraisingham, and Marek Zmuda. Special issue on actionable information for digital threat discovery using contextualized data or multi sensor data fusion. *Digital Threats: Research and Practice (DTRAP)*, 4(2): 23:1–23:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3585079`.

Jarvis:2022:VED

[JDCK22] Paul-David Jarvis, Amalia

Damianou, Cosmin Ciobanu, and Vasilis Katos. Vulnerability exposure driven intelligence in smart, circular cities. *Digital Threats: Research and Practice (DTRAP)*, 3 (4):40:1–40:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3487059`.

Joshi:2024:LSP

[JM24] Rucha Bhalchandra Joshi and Subhankar Mishra. Locally and structurally private graph neural networks. *Digital Threats: Research and Practice (DTRAP)*, 5(1):10:1–10:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3624485`.

Jacobs:2021:EPS

[JRE+21] Jay Jacobs, Sasha Romanosky, Benjamin Edwards, Idris Adjerid, and Michael Roytman. Exploit Prediction Scoring System (EPSS). *Digital Threats: Research and Practice (DTRAP)*, 2 (3):20:1–20:17, July 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3436242`.

Jelesnianski:2022:SSR

[JYMJ22] Christopher Jelesnianski, Jinwoo Yom, Changwoo Min, and Yeongjin Jang. Securely sharing randomized code that flies. *Digital Threats: Research and Practice (DTRAP)*, 3(3):32:1–32:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3474558`.

Kohlrausch:2020:ASS

[KB20] Jan Kohlrausch and Eugene A. Brin. ARIMA supplemented security metrics for quality assurance and situational awareness. *Digital Threats: Research and Practice (DTRAP)*, 1 (1):6:1–6:21, March 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3376926`.

Karim:2020:ADA

[KCH+20] Imtiaz Karim, Fabrizio Cicala, Syed Rafiul Hussain, Omar Chowdhury, and Elisa Bertino. ATFuzzer: Dynamic analysis framework of AT interface for Android smartphones. *Digital Threats: Research and Practice (DTRAP)*, 1(4):23:1–23:29, December 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3416125.

Kaptchuk:2022:HGG

[KGH+22] Gabriel Kaptchuk, Daniel G. Goldstein, Eszter Hargittai, Jake M. Hofman, and Elissa M. Redmiles. How good is good enough? Quantifying the impact of benefits, accuracy, and privacy on willingness to adopt COVID-19 decision aids. *Digital Threats: Research and Practice (DTRAP)*, 3(3):27:1–27:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3488307.

Kumar:2021:TAG

[KIP21] Rajesh Kumar, Can Isik, and Vir V. Phoha. Treadmill Assisted Gait Spoofing (TAGS): an emerging threat to wearable sensor-based gait authentication. *Digital Threats: Research and Practice (DTRAP)*, 2(3):23:1–23:17, September 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3442151.

Kassim:2023:UHN

[KLA23] Sharifah Roziah Binti Mohd Kassim, Shujun Li, and Budi Arief. Understanding how national CSIRTs evaluate cyber incident response tools and data: Findings from focus group discussions. *Digital Threats: Research and Practice (DTRAP)*, 4(3):45:1–45:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3609230.

Kaptchuk:2022:ISI

[KMGR22] Gabriel Kaptchuk, Fabio Massacci, Sara Nieves Matheu Garcia, and Elissa M. Redmiles. Introduction to the special issue on security and privacy for COVID-19. *Digital Threats: Research and Practice (DTRAP)*, 3(3):24:1–24:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3549070.

Kumar:2023:ISD

[KMPS23] Saurabh Kumar, Debadatta Mishra, Biswabandan Panda, and Sandeep Kumar Shukla. InviSeal: a stealthy dynamic analysis framework for Android systems. *Digital Threats: Research and Practice (DTRAP)*, 4(1): 13:1–13:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3567599`.

Koot:2020:FNC

[Koo20] Matthijs Koot. Field note on CVE-2019-11510: Pulse connect secure SSL-VPN in The Netherlands. *Digital Threats: Research and Practice (DTRAP)*, 1 (2):13:1–13:7, July 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3382765`.

Konstantinovskiy:2021:TAF

[KPBZ21] Lev Konstantinovskiy, Oliver Price, Mevan Babakar, and Arkaitz Zubiaga. Toward automated factchecking: Developing an annotation schema and benchmark for consistent automated claim detection. *Digital Threats: Research and Practice (DTRAP)*, 2 (2):14:1–14:16, June 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3412869`.

Klier:2023:BFA

[KVB23] Samantha Klier, Jan Varenkamp, and Harald Baier. Back and forth-on automatic exposure of origin and dissemination of files on Windows. *Digital Threats: Research and Practice (DTRAP)*, 4(3):34:1–34:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3609232`.

Langehaug:2023:CCR

[LBG23] Tor Langehaug, Brett Borghetti, and Scott Graham. Classifying co-resident computer programs using information revealed by resource contention. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):17:1–17:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3464306`.

Lang:2023:EMR

[LCTC23] Michael Lang, Lena Connolly, Paul Taylor, and Phillip J. Corner. The evolving menace of ransomware: a comparative analysis of pre-pandemic and mid-pandemic attacks. *Digital Threats:*

Research and Practice (DTRAP), 4(4):52:1–52:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3558006.

Li:2022:SPH

[LHH22] Ming Li, Peter Hawrylak, and John Hale. Strategies for practical hybrid attack graph generation and analysis. *Digital Threats: Research and Practice (DTRAP)*, 3(4):41:1–41:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3491257.

Laurenza:2020:MTE

[LLM20] Giuseppe Laurenza, Riccardo Lazzeretti, and Luca Mazzotti. Malware triage for early identification of advanced persistent threat activities. *Digital Threats: Research and Practice (DTRAP)*, 1(3):16:1–16:17, September 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3386581.

Lakhotia:2020:DTR

[LM20] Arun Lakhotia and Leigh Metcalf. Digital threats: Research and practice inaugural issue editorial. *Digital Threats: Research and Practice (DTRAP)*, 1(1):1:1–1:3, March 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3380320.

Lamp:2021:ECA

[LRMZA21] Josephine Lamp, Carlos E. Rubio-Medrano, Ziming Zhao, and Gail-Joon Ahn. ExSol: Collaboratively assessing cybersecurity risks for protecting energy delivery systems. *Digital Threats: Research and Practice (DTRAP)*, 2(3):21:1–21:23, July 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3428156.

Leverett:2022:VFT

[LRW22] Éireann Leverett, Matilda Rhode, and Adam Wedgbury. Vulnerability forecasting: Theory and practice. *Digital Threats: Research and Practice (DTRAP)*, 3(4):42:1–42:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3492328.

Liu:2022:RAF

[LSK+22] Jinxin Liu, Murat Simsek, Burak Kantarci, Melike Erol-kantarci, Andrew Malton, and Andrew Walenstein. Risk-aware fine-grained access control in cyber-physical contexts. *Digital Threats: Research and Practice (DTRAP)*, 3(4):43:1–43:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3480468`.

Levine:2023:ZTA

[LT23] Alan Levine and Brett Alan Tucker. Zero trust architecture: Risk discussion. *Digital Threats: Research and Practice (DTRAP)*, 4(1):15:1–15:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3573892`.

Landauer:2023:AML

[LWS+23] Max Landauer, Markus Wurzenberger, Florian Skopik, Wolfgang Hotwagner, and Georg Höld. AMiner: a modular log data analysis pipeline for anomaly-based intrusion detection. *Digital Threats: Research and Practice (DTRAP)*, 4(1):12:1–12:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3567675`.

Lounis:2023:LLA

[LZ23] Karim Lounis and Mohammad Zulkernine. Lessons learned: Analysis of PUF-based authentication protocols for IoT. *Digital Threats: Research and Practice (DTRAP)*, 4(2):19:1–19:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3487060`.

Mundt:2023:TBS

[MB23] Michael Mundt and Harald Baier. Threat-based simulation of data exfiltration toward mitigating multiple ransomware extortions. *Digital Threats: Research and Practice (DTRAP)*, 4(4):54:1–54:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3568993`.

Mainardi:2022:PAC

[MBP22] Nicholas Mainardi, Alessandro Barenghi, and Gerardo Pelosi. Privacy-aware character pattern matching over outsourced encrypted data. *Digital Threats: Research and Practice (DTRAP)*, 3(1): 7:1–7:38, March 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3462333`.

Morel:2023:CPM

[MCH23] Lionel Morel, Damien Couroussé, and Thomas Hiscock. Code polymorphism meets code encryption: Confidentiality and side-channel protection of software components. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):18:1–18:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3487058`.

Metcalf:2021:ESI

[Met21] Leigh Metcalf. Editorial on the special issue on election security. *Digital Threats: Research and Practice (DTRAP)*, 2(4): 31:1, December 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3471534`.

Mccorry:2021:SVB

[MMT+21] Patrick Mccorry, Maryam Mehrnezhad, Ehsan Toreini, Siamak F. Shahandashti, and Feng Hao. On secure e-voting over blockchain. *Digital Threats: Research and Practice (DTRAP)*, 2(4):33:1–33:13, December 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3461461`.

Mahmoud:2023:ADA

[MMY23] Moustafa Mahmoud, Mohammad Mannan, and Amr Youssef. APTHunter: Detecting advanced persistent threats in early stages. *Digital Threats: Research and Practice (DTRAP)*, 4(1):11:1–11:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3559768`.

Massacci:2022:ISI

[MNP+22] Fabio Massacci, Nick Nikiforakis, Ivan Pashchenko, Antonino Sabetta, and Victoria Wang. Introduction to the special issue on vulnerabilities. *Digital Threats: Research and Practice (DTRAP)*, 3(4):37:1–37:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https:`

//dl.acm.org/doi/10.1145/3580605.

Mozurkewich:2022:FNI

[Moz22] Karl Mozurkewich. Field note on IoT security: Novel JIT security for large-scale heterogeneous IoT deployments. *Digital Threats: Research and Practice (DTRAP)*, 3(4):36:1–36:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3503919.

Metcalf:2021:EDB

[MS21] Leigh Metcalf and Jonathan M. Spring. The ecosystem of detection and blocklisting of domain generation. *Digital Threats: Research and Practice (DTRAP)*, 2(3):19:1–19:22, September 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3423951.

Madani:2022:RMT

[MVM22] Pooria Madani, Natalija Vlajic, and Ivo Maljevic. Randomized moving target approach for MAC-Layer spoofing detection and prevention in IoT systems. *Digital Threats: Research and Practice (DTRAP)*, 3(4):35:1–35:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3477403.

Nakatsuka:2021:PPD

[NPT21] Yoshimichi Nakatsuka, Andrew Paverd, and Gene Tsudik. PDoT: Private DNS-over-TLS with TEE support. *Digital Threats: Research and Practice (DTRAP)*, 2(1):3:1–3:22, March 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3431171.

Oesch:2022:UPS

[OASD+22] Sean Oesch, Ruba Abu-Salma, Oumar Diallo, Juliane Krämer, James Simmons, Justin Wu, and Scott Ruoti. User perceptions of security and privacy for group chat. *Digital Threats: Research and Practice (DTRAP)*, 3(2):15:1–15:29, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3491265.

Osman:2020:SAA

[OMHY20] Tousif Osman, Mohammad Mannan, Urs Hengartner, and Amr Youssef.

Securing applications against side-channel attacks through resource access veto. *Digital Threats: Research and Practice (DTRAP)*, 1(4):22:1–22:29, December 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3416124`.

Oakley:2023:SSA

[OWY+23] Jonathan Oakley, Carl Worley, Lu Yu, Richard R. Brooks, Ilker Özçelik, Anthony Skjellum, and Jihad S. Obeid. Scrybe: a secure audit trail for clinical trial data fusion. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):24:1–24:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3491258`.

Pimenta:2024:ARC

[PCG24] Thalita Scharr Rodrigues Pimenta, Fabricio Ceschin, and Andre Gregio. ANDROIDGYNY: Reviewing clustering techniques for Android malware family classification. *Digital Threats: Research and Practice (DTRAP)*, 5(1): 3:1–3:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3587471`.

Perdisci:2020:IAS

[PLD+20] Roberto Perdisci, Martina Lindorfer, Adam Doupé, Andrea Lanzi, Alexandros Kapravelos, and Gianluca Stringhini. Introduction to the ACSAC'19 special issue — Part 1. *Digital Threats: Research and Practice (DTRAP)*, 1(4):19e:1–19e:3, December 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3437251`.

Perdisci:2021:IAS

[PLD+21] Roberto Perdisci, Martina Lindorfer, Adam Doupé, Andrea Lanzi, Alexandros Kapravelos, and Gianluca Stringhini. Introduction to the ACSAC'19 special issue — vol. 2. *Digital Threats: Research and Practice (DTRAP)*, 2(1): 1:1–1:2, March 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3437253`.

Perdisci:2022:IAS

[PLS22] Roberto Perdisci, Martina Lindorfer, and Gianluca Stringhini. Introduction to the AC-

SAC'20 special issue. *Digital Threats: Research and Practice (DTRAP)*, 3(2): 12:1–12:2, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3534708`.

Palit:2020:MDO

[PMP20] Tapti Palit, Fabian Monrose, and Michalis Polychronakis. Mitigating data-only attacks by protecting memory-resident sensitive data. *Digital Threats: Research and Practice (DTRAP)*, 1(4):20:1–20:26, December 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3419475`.

Rondon:2023:LSE

[RBA+23] Luis Puche Rondon, Leonardo Babun, Ahmet Aris, Kemal Akkaya, and A. Selcuk Uluagac. LGuard: Securing Enterprise-IoT systems against serial-based attacks via proprietary communication buses. *Digital Threats: Research and Practice (DTRAP)*, 4(1):10:1–10:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3555721`.

Rosso:2022:SMT

[RCGA22] Martin Rosso, Michele Campobasso, Ganduulga Gankhuyag, and Luca Allodi. SAIBERSOC: a methodology and tool for experimenting with security operation centers. *Digital Threats: Research and Practice (DTRAP)*, 3 (2):14:1–14:29, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3491266`.

Rose:2023:IWN

[RGK23] Anthony Rose, Scott Graham, and Jacob Krasnov. IronNetInjector: Weaponizing .NET dynamic language runtime engines. *Digital Threats: Research and Practice (DTRAP)*, 4(3):40:1–40:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3603506`.

Rudd:2024:EMA

[RKC+24] Ethan M. Rudd, David Krisiloff, Scott Coull, Daniel Olszewski, Edward Raff, and James Holt. Efficient malware analysis using metric embeddings. *Digital Threats: Research* *and Practice (DTRAP)*, 5 (1):4:1–4:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3615669`.

Ren:2023:SAZ

[RRF+23] Mengfei Ren, Xiaolei Ren, Huadong Feng, Jiang Ming, and Yu Lei. Security analysis of Zigbee protocol implementation via device-agnostic fuzzing. *Digital Threats: Research and Practice (DTRAP)*, 4 (1):9:1–9:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3551894`.

Rodriguez:2022:ISI

[RUPT22] Ricardo J. Rodríguez, Xabier Ugarte-Pedrero, and Juan Tapiador. Introduction to the special issue on challenges and trends in malware analysis. *Digital Threats: Research and Practice (DTRAP)*, 3(2): 8:1–8:2, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3536319`.

Ring:2021:MHB

[RVD+21] John H. Ring, Colin M. Van Oort, Samson Durst, Vanessa White, Joseph P. Near, and Christian Skalka. Methods for host-based intrusion detection with deep learning. *Digital Threats: Research and Practice (DTRAP)*, 2(4):26:1–26:29, December 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3461462`.

Sacher:2020:FFP

[Sac20] Desiree Sacher. Fingerpointing false positives: How to better integrate continuous improvement into security monitoring. *Digital Threats: Research and Practice (DTRAP)*, 1 (1):7:1–7:7, March 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3370084`.

Stojkovski:2022:UOD

[SASTL22] Borce Stojkovski, Ruba Abu-Salma, Karen Triquet, and Gabriele Lenzini. "Unless One Does the Research, It May Seem as Just a Useless Battery-consuming App" — field notes on COVID-19 contact tracing applications. *Digital Threats: Research and Practice (DTRAP)*, 3(3):26:1–26:??, September 2022. CODEN

???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3480466.

Sacher-Boldewin:2022:IPL

[SBL22] Desiree Sacher-Boldewin and Eireann Leverett. The intelligent process lifecycle of active cyber defenders. *Digital Threats: Research and Practice (DTRAP)*, 3(3):22:1–22:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3499427.

Sikder:2021:ACA

[SBU21] Amit Kumar Sikder, Leonardo Babun, and A. Selcuk Uluagac. Aegis+: a context-aware platform-independent security framework for smart home systems. *Digital Threats: Research and Practice (DTRAP)*, 2(1):6:1–6:33, March 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3428026.

Simko:2022:CCT

[SCJ+22] Lucy Simko, Jack Chang, Maggie Jiang, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. COVID-19 contact tracing and privacy: a longitudinal study of public opinion. *Digital Threats: Research and Practice (DTRAP)*, 3(3):25:1–25:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3480464.

Sticha:2022:SOD

[SDA+22] Paul J. Sticha, Tirso E. Diaz, Elise T. Axelrad, Sean D. Vermillion, and Dennis M. Buede. Simulating organizational data from redacted input for inference enterprise modeling. *Digital Threats: Research and Practice (DTRAP)*, 3(1):4:1–4:30, March 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3457910.

Shomo:2022:ISI

[SES22] Paul Shomo, Sebastian Echeverria, and Jesse Sowell. Introduction to the special issue on the lifecycle of IoT (in)security. *Digital Threats: Research and Practice (DTRAP)*, 3(4):33:1–33:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https:

//dl.acm.org/doi/10.1145/3569901.

Staves:2023:AAC

[SGH23] Alexander Staves, Antonios Gouglidis, and David Hutchison. An analysis of adversary-centric security testing within information and operational technology environments. *Digital Threats: Research and Practice (DTRAP)*, 4(1): 14:1–14:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3569958.

Shukla:2020:TUI

[SKM+20] Diksha Shukla, Partha Pratim KUNDU, Ravichandra Malapati, Sujit Poudel, Zhanpeng Jin, and Vir V. Phoha. Thinking unveiled: an inference and correlation model to attack EEG biometrics. *Digital Threats: Research and Practice (DTRAP)*, 1(2): 9:1–9:29, July 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3374137.

Samtani:2021:ICT

[SLBC21] Sagar Samtani, Weifeng Li, Victor Benjamin, and Hsinchun Chen. Informing cyber threat intelligence through dark Web situational awareness: The AZSecure hacker assets portal. *Digital Threats: Research and Practice (DTRAP)*, 2(4):27:1–27:10, December 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3450972.

Scofield:2020:AML

[SMK20] Daniel Scofield, Craig Miles, and Stephen Kuhn. Automated model learning for accurate detection of malicious digital documents. *Digital Threats: Research and Practice (DTRAP)*, 1(3):15:1–15:21, September 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3379505.

Shobiri:2023:CDS

[SMY23] Behnam Shobiri, Mohammad Mannan, and Amr Youssef. CDNs' dark side: Security problems in CDN-to-origin connections. *Digital Threats: Research and Practice (DTRAP)*, 4(1):3:1–3:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https:

//dl.acm.org/doi/10.1145/3499428.

Sanchez:2023:DAB

[SNA+23] Ricardo Alejandro Manzano Sanchez, Kshirasagar Naik, Abdurhman Albasir, Marzia Zaman, and Nishith Goel. Detection of anomalous behavior of smartphone devices using changepoint analysis and machine learning techniques. *Digital Threats: Research and Practice (DTRAP)*, 4(1): 2:1–2:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3492327.

Sengupta:2023:BBP

[SPM23] Poushali Sengupta, Sudipta Paul, and Subhankar Mishra. BUDS+: Better privacy with converger and noisy shuffling. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):25:1–25:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3491259.

Srinivasa:2023:GCE

[SPV23] Shreyas Srinivasa, Jens Myrup Pedersen, and Emmanouil Vasilomanolakis. Gotta catch 'em all: a multistage framework for honeypot fingerprinting. *Digital Threats: Research and Practice (DTRAP)*, 4(3):42:1–42:??, September 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3584976.

Samtani:2024:AML

[SRA24] Sagar Samtani, Edward Raff, and Hyrum Anderson. Applied machine learning for information security. *Digital Threats: Research and Practice (DTRAP)*, 5(1): 1:1–1:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3652029.

Sanchez-Rola:2020:CPT

[SRBS20] Iskander Sanchez-Rola, Davide Balzarotti, and Igor Santos. Cookies from the past: Timing server-side request processing code for history sniffing. *Digital Threats: Research and Practice (DTRAP)*, 1(4):24:1–24:24, December 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3419473.

//dl.acm.org/doi/abs/10.1145/3378448.

Steinhauser:2020:DTI

[ST20] Antonín Steinhauser and Petr Tuma. Database traffic interception for gray-box detection of stored and context-sensitive XSS. *Digital Threats: Research and Practice (DTRAP)*, 1(3):17:1–17:23, September 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3399668.

Sun:2022:CRV

[Sun22] Sheng Sun. A chosen random value attack on WPA3 SAE authentication protocol. *Digital Threats: Research and Practice (DTRAP)*, 3(2):16:1–16:8, June 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3468526.

Tien:2020:MLF

[TCBK20] Chin-Wei Tien, Shang-Wen Chen, Tao Ban, and Sy-Yen Kuo. Machine learning framework to analyze IoT malware using ELF and opcode features. *Digital Threats: Research and Practice (DTRAP)*, 1(1):5:1–5:19, March 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https:

Taviss:2024:AEA

[TDZ+24] Scarlett Taviss, Steven H. H. Ding, Mohammad Zulkernine, Philippe Charland, and Sudipta Acharya. Asm2Seq: Explainable assembly code functional summary generation for reverse engineering and vulnerability analysis. *Digital Threats: Research and Practice (DTRAP)*, 5(1):6:1–6:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3592623.

Tsunoda:2024:DSO

[Tsu24] Akaki Tsunoda. Demonstrating spoofability of an originating number when sending an SMS using SMPP. *Digital Threats: Research and Practice (DTRAP)*, 5(1):12:1–12:??, March 2024. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3615667.

Ukrop:2020:WYT

[UKM20] Martin Ukrop, Lydia Kraus, and Vashek Matyas. Will you trust this TLS certificate?: Perceptions of people working in IT (extended version). *Digital Threats: Research and Practice (DTRAP)*, 1(4):25:1–25:29, December 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3419472`.

Usui:2021:ARE

[UOI+21] Toshinori Usui, Yuto Otsuki, Tomonori Ikuse, Yuhei Kawakoya, Makoto Iwamura, Jun Miyoshi, and Kanta Matsuura. Automatic reverse engineering of script engine binaries for building script API tracers. *Digital Threats: Research and Practice (DTRAP)*, 2(1): 5:1–5:31, March 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3416126`.

VanDerHam:2021:TBU

[Van21] Jeroen Van Der Ham. Toward a better understanding of "cybersecurity". *Digital Threats: Research and Practice (DTRAP)*, 2(3):18:1–18:3, September 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3442445`.

vanHove:2023:RTA

[vHvdHdVvRD23] Koen van Hove, Jeroen van der Ham-de Vos, and Roland van Rijswijk-Deij. rpkiller: Threat analysis of the BGP resource public key infrastructure. *Digital Threats: Research and Practice (DTRAP)*, 4(4):58:1–58:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3617182`.

Vaidya:2023:SIA

[VPG+23] Girish Vaidya, T. V. Prabhakar, Nithish Gnani, Ryan Shah, and Shishir Nagaraja. Sensor identification via acoustic physically unclonable function. *Digital Threats: Research and Practice (DTRAP)*, 4 (2):20:1–20:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3488306`.

VanderToorn:2020:LBH

[VS20] Olivier Van der Toorn and Anna Sperotto. Looking beyond the horizon: Thoughts on proactive detection of threats. *Digital Threats: Research and Practice (DTRAP)*, 1(1): 4:1–4:13, March 2020. CODEN ???? ISSN 2692-

1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3373639.

Valecha:2021:FNS

[VSV+21] Rohit Valecha, Srikrishna Krishnarao Srinivasan, Tejaswi Volety, K. Hazel Kwon, Manish Agrawal, and H. Raghav Rao. Fake news sharing: an investigation of threat and coping cues in the context of the Zika virus. *Digital Threats: Research and Practice (DTRAP)*, 2 (2):16:1–16:16, June 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3410025.

Vaudenay:2022:SPG

[VV22] Serge Vaudenay and Martin Vuagnoux. SwissCovid in the perspective of its goals. *Digital Threats: Research and Practice (DTRAP)*, 3(3):29:1–29:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3480465.

Williams:2022:RIA

[WASC22] Adam D. Williams, Shannon N. Abbott, Nathan Shoman, and William S. Charlton. Results from invoking artificial neural networks to measure insider threat detection & mitigation. *Digital Threats: Research and Practice (DTRAP)*, 3(1): 3:1–3:20, March 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3457909.

Wala:2022:LUD

[WC22] Fatema Bannat Wala and Chase Cotton. “Off-Label” use of DNS. *Digital Threats: Research and Practice (DTRAP)*, 3(3):21:1–21:??, September 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/10.1145/3491261.

Waked:2020:SST

[WMY20] Louis Waked, Mohammad Mannan, and Amr Youssef. The sorry state of TLS security in enterprise interception appliances. *Digital Threats: Research and Practice (DTRAP)*, 1(2):8:1–8:26, July 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL https://dl.acm.org/doi/abs/10.1145/3372802.

Walshe:2023:TGU

[WS23] Thomas Walshe and Andrew Simpson. Towards a greater understanding of coordinated vulnerability disclosure policy documents. *Digital Threats: Research and Practice (DTRAP)*, 4(2): 29:1–29:??, June 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3586180`.

Xenakis:2023:SAS

[XNC+23] Antonios Xenakis, Sabrina Mamtaz Nourin, Zhiyuan Chen, George Karabatis, Ahmed Aleroud, and Jhancy Amarsingh. A self-adaptive and secure approach to share network trace data. *Digital Threats: Research and Practice (DTRAP)*, 4(4):50:1–50:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3617181`.

Xiao:2023:IEF

[XZA+23] Ya Xiao, Yang Zhao, Nicholas Allen, Nathan Keynes, Danfeng (Daphne) Yao, and Cristina Cifuentes. Industrial experience of finding cryptographic vulnerabilities in large-scale codebases. *Digital Threats: Research and Practice (DTRAP)*, 4(1): 4:1–4:??, March 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3507682`.

Yilmaz:2023:PTR

[YCG+23] Yagiz Yilmaz, Orcun Cetin, Claudia Grigore, Budi Arief, and Julio Hernandez-Castro. Personality types and ransomware victimisation. *Digital Threats: Research and Practice (DTRAP)*, 4(4):53:1–53:??, December 2023. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3568994`.

Zimmer:2022:IDN

[ZBF22] Ephraim Zimmer, Christian Burkert, and Hannes Federrath. Insiders dissected: New foundations and a systematisation of the research on insiders. *Digital Threats: Research and Practice (DTRAP)*, 3 (1):2:1–2:35, March 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3473674`.

Zhou:2020:FNE

[ZJPZ20] Xinyi Zhou, Atishay Jain, Vir V. Phoha, and Reza Zafarani. Fake news early detection: a theory-driven model. *Digital Threats: Research and Practice (DTRAP)*, 1(2): 12:1–12:25, July 2020. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/abs/10.1145/3377478`.

Zafarani:2021:IRT

[ZLPA21] Reza Zafarani, Huan Liu, Vir V. Phoha, and Javad Azimi. Inroduction on recent trends and perspectives in fake news research. *Digital Threats: Research and Practice (DTRAP)*, 2 (2):13:1–13:3, March 2021. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3448634`.

Zibak:2022:TIQ

[ZSS22] Adam Zibak, Clemens Sauerwein, and Andrew C. Simpson. Threat intelligence quality dimensions for research and practice. *Digital Threats: Research and Practice (DTRAP)*, 3(4):44:1–44:??, December 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3484202`.

Zheng:2022:UDM

[ZYW22] Panpan Zheng, Shuhan Yuan, and Xintao Wu. Using Dirichlet marked Hawkes processes for insider threat detection. *Digital Threats: Research and Practice (DTRAP)*, 3 (1):5:1–5:19, March 2022. CODEN ???? ISSN 2692-1626 (print), 2576-5337 (electronic). URL `https://dl.acm.org/doi/10.1145/3457908`.