1. Record Nr. UNISA996464489603316

Titolo	ICT systems security and privacy protection : 36th IFIP TC 11 International Conference, SEC 2021, Oslo, Norway, June 22-24, 2021 : proceedings / / Audun Josang, Lynn Futcher, Janne Hagen, editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-78120-8
Descrizione fisica	1 online resource (447 pages)
Collana	IFIP Advances in Information and Communication Technology ; ; v.625
Disciplina	005.8
Soggetti	Computer security Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- About IFIP Technical Committee 11 -- Organization -- Contents -- Digital Signatures -- XML Signature Wrapping Still Considered Harmful: A Case Study on the Personal Health Record in Germany -- 1 Introduction -- 2 Background: XML Signature Wrapping (XSW) -- 3 Personal Health Record (PHR) in Germany -- 4 XSW Vulnerable PHR in Germany -- 4.1 Specification Weaknesses -- 4.2 Attack Goals -- 4.3 Proof of Concept -- 5 Robust XML Signature Guidelines -- 5.1 XML Signature Generation Guideline -- 5.2 XML Signature Verification Guideline -- 6 Case-Based Evaluation -- 7 Discussion and Limitations -- 8 Conclusion and Outlook -- References -- Trust Me If You Can: Trusted Transformation Between (JSON) Schemas to Support Global Authentication of Education Credentials -- 1 Introduction -- 2 Background -- 3 Related Work -- 4 Architecture Overview -- 5 Issuer Authorization -- 6 Credential Transformation -- 7 Prototype -- 8 Discussion -- 9 Conclusion -- References -- SIUV: A Smart Car Identity Management and Usage Control System Based on Verifiable Credentials -- 1 Introduction -- 2 Background -- 2.1 Access and Usage Control -- 2.2 Abbreviated Language for Authorisation (ALFA) -- 2.3 Verifiable Credentials (VCs) -- 3 SIUV -- 3.1 Usage Control System Plus (UCS+) -- 3.2 SIUV Security Token Service (STS) -- 3.3 SIUV Architecture -- 3.4 Revocation of VCs -- 4 Experimental

Evaluation -- 4.1 Use Case -- 4.2 Test Cases -- 5 Conclusion and Future Work -- References -- Vulnerability Management -- A Performance Assessment of Free-to-Use Vulnerability Scanners - Revisited -- 1 Introduction -- 2 Related Work -- 3 Experimentation and Setup -- 3.1 Scanners Technical Features -- 3.2 Test-Bed Design and Setup -- 4 Results and Analysis -- 5 Conclusions -- References -- QuickBCC: Quick and Scalable Binary Vulnerable Code Clone Detection -- 1 Introduction.
2 Related Works -- 2.1 Source Code Clone Detection -- 2.2 Binary Code Clone Detection -- 3 Approach -- 3.1 Similarity and Equivalence Metric -- 3.2 Binary Preprocessor -- 3.3 Vulnerability Signature Generator -- 3.4 Code Clone Detector -- 4 Evaluation -- 4.1 Environmental Setup -- 4.2 Vulnerable Code Clone Detection -- 4.3 Comparison -- 5 Discussion and Future Work -- 5.1 Robustness to Multiple Compile Environments -- 5.2 Better Vulnerability Signature Generation -- 6 Conclusion -- References -- Automatic Inference of Taint Sources to Discover Vulnerabilities in SOHO Router Firmware -- 1 Introduction -- 2 Background and Motivation -- 2.1 Typical Architecture of SOHO Router -- 2.2 Key-Value Features -- 3 Detailed Design -- 3.1 Key-Value Taint Source Inferring -- 3.2 Static Taint Analysis -- 4 Evaluation -- 4.1 Implementation -- 4.2 Experiment Setup -- 4.3 Key-Value Taint Source Inferring -- 4.4 Effectiveness of Vulnerability Detection -- 4.5 Comparison -- 5 Discussion -- 6 Related Work -- 7 Conclusion -- References -- Covert Channels and Cryptography -- ESQABE: Predicting Encrypted Search Queries -- 1 Introduction -- 2 Related Work -- 3 ESQABE: Encrypted Search Query Analysis by Eavesdropping -- 3.1 Prerequisites -- 3.2 Step 1: Extracting Search Query Length-1em -- 3.3 Step 2: Identifying Opened Search Results -- 3.4 Step 3: Visiting Home Pages of Websites -- 3.5 Step 4: Wikipedia -- 3.6 Vulnerable Search Engines -- 4 Experimental Evaluation -- 4.1 Approach -- 4.2 Results -- 5 Defense Mechanisms -- 6 Conclusion -- References -- Reconnection-Based Covert Channels in Wireless Networks -- 1 Introduction -- 2 Fundamentals and Related Work -- 3 Concept and Implementation -- 4 Covert Channel Method 1 -- 4.1 Covert Sender -- 4.2 Covert Receiver -- 4.3 Evaluation -- 5 Covert Channel Method 2 -- 5.1 Covert Sender -- 5.2 Covert Receiver -- 5.3 Evaluation.
6 Passive Countermeasures: Covert Channel Detection -- 6.1 Detection of Covert Channel Method 1 -- 6.2 Detection of Covert Channel Method 2 -- 6.3 Evaluation of Detection Methods -- 7 Active Countermeasures: Covert Channel Limitation -- 8 Comparison with Other Covert Channels -- 8.1 Kraetzer et al.: WLAN Steganography -- 8.2 Zhao: Covert Channels in 802.11e Wireless Networks -- 9 Conclusion -- References -- Minecraft Altered Skin Channel (MASC) -- 1 Introduction -- 2 Background -- 3 Minecraft Skin Channel -- 4 Encoding and Decoding -- 4.1 Encoding -- 4.2 Decoding -- 5 Performance -- 6 Countermeasures -- 7 Conclusion and Future Works -- References -- Lattice-Based Weak Curve Fault Attack on ECDSA -- 1 Introduction -- 1.1 Existing Work on Fault Attacks -- 1.2 Our Approach -- 2 Preliminaries -- 2.1 ECDSA Digital Signature Algorithm -- 2.2 Smoothness of Weak Curve Order -- 2.3 Existing Fault Attacks on Weak Curves -- 2.4 Lattice Basis Reduction -- 3 Lattice-Based Weak Curve Attack -- 3.1 Fault Model -- 3.2 Proposed Fault Attack on Weak Curves -- 3.3 Proposed Lattice-Based ECDSA Key Recovery Algorithm -- 3.4 Attack on ECDSA with Scalar Masking -- 3.5 The Density of Smooth Numbers -- 4 Experimental Analysis -- 5 Conclusion -- References -- Application and System Security -- HyperSec: Visual Analytics for Blockchain Security Monitoring -- 1 Introduction -- 2 Related Work --

3 Blockchain Security Monitoring -- 3.1 Blockchain Security Monitoring Process -- 3.2 Users -- 3.3 Tasks -- 3.4 Data Elements -- 3.5 Design Requirements -- 4 HyperSec: Hyperledger Security Monitoring Using Visual Analytics -- 4.1 Architecture and Technology -- 4.2 Visual Representations and Interactions -- 5 Evaluation -- 6 Discussion -- 7 Conclusion -- References -- 100 Popular Open-Source Infosec Tools -- 1 Introduction -- 2 Methods -- 2.1 Collecting a Corpus of Tools.
2.2 Google Tool Name Search -- 2.3 Google Tool URL Search -- 2.4 Twitter Tool Name Search -- 2.5 SecTools.org Ranking -- 2.6 GitHub Stars -- 2.7 Tool Cross-references -- 2.8 Aggregate Popularity Metric -- 2.9 Dividing Tools into Categories -- 3 Results -- 3.1 Most Popular Tools -- 3.2 Reliability of the Results -- 3.3 Most Popular Tools per Category -- 3.4 Availability of the Result Data -- 4 Discussion -- 4.1 Future Work -- References -- RootAsRole: Towards a Secure Alternative to sudo/su Commands for Home Users and SME Administrators -- 1 Introduction -- 2 Linux Capabilities -- 3 Related Works -- 4 RootAsRole Module -- 5 Motivation Scenario -- 6 Discussion, Limitations and Conclusions -- References -- Privacy -- Accept All: The Landscape of Cookie Banners in Greece and the UK -- 1 Introduction -- 2 Related Work -- 3 Research Questions, Methodology, and Implementation -- 3.1 Building the Target List -- 3.2 Collecting Cookie Banners -- 3.3 Classifying and Normalising the Data -- 4 Data and Results -- 4.1 The Collected Dataset -- 4.2 Findings -- 5 Conclusion -- References -- The AppChk Crowd-Sourcing Platform: Which Third Parties are iOS Apps Talking To? -- 1 Introduction -- 2 Related Work -- 3 Our Approach -- 3.1 Design Goals -- 3.2 App Recordings -- 3.3 Continuous Monitoring -- 4 Evaluation -- 4.1 Use Case: Tracker Detection -- 4.2 Use Case: Comparing Apps and App Groups -- 4.3 Comparison: iOS13 vs. iOS14 -- 5 Discussion -- 6 Conclusion -- References -- Compiling Personal Data and Subject Categories from App Data Models -- 1 Introduction -- 2 Related Work -- 3 Schemalyser Approach -- 3.1 Seed Identification -- 3.2 Identifiability Markup -- 3.3 Role Determination -- 3.4 Decisive Role Selection -- 3.5 Condensed PD Listing -- 4 Evaluation -- 4.1 Interaction Cost and Complexity -- 4.2 Degree of Condensation -- 5 Integration into Development Workflows.
6 Conclusion -- References -- Privacy Concerns Go Hand in Hand with Lack of Knowledge: The Case of the German Corona-Warn-App -- 1 Introduction -- 2 Related Work -- 3 Methodology -- 3.1 Questionnaire -- 3.2 Data Collection and Demographics -- 4 Results -- 4.1 Analysis of Knowledge and Its Relation to Demographics -- 4.2 Privacy Concerns -- 4.3 Relationship of Knowledge and Concerns -- 5 Discussion -- 5.1 Knowledge -- 5.2 Concerns -- 5.3 Knowledge vs. Concerns vs. CWA -- 5.4 Limitations -- 6 Conclusion and Future Work -- A Survey Questionnaire -- References -- Perceived Privacy Problems Within Digital Contact Tracing: A Study Among Swedish Citizens -- 1 Introduction -- 2 Background -- 2.1 Surveillance -- 2.2 Identification -- 2.3 Aggregation -- 2.4 Secondary Use -- 2.5 Disclosure -- 2.6 Stigma -- 2.7 Perceived Privacy Problems and Digital Contact Tracing Apps -- 3 Methodology -- 4 Results -- 5 Discussion and Conclusion -- References -- Network Security -- Secure and Scalable IoT: An IoT Network Platform Based on Network Overlay and MAC Security -- 1 Introduction -- 2 Related Work -- 2.1 L2TP (Layer 2 Tunneling Protocol) -- 2.2 MACsec (802.1AE, MAC Security) -- 2.3 VXLAN (Virtual Extensible LAN) -- 3 Problem Analysis -- 3.1 Security Threats on the IoT Network -- 3.2 Limitations of IoT Application Protocol -- 3.3 Security Threat Modeling Using STRIDE -- 4 Secure and Scalable IoT (SSI) Model -- 4.1 Overview -- 4.2 L2TP and VXLAN Based Overlay

Network -- 4.3 End-to-End Encryption Using MACsec -- 4.4 Network Architecture -- 5 Evaluation -- 6 Conclusion -- References --
Enriching DNS Flows with Host-Based Events to Bypass Future Protocol Encryption -- 1 Introduction -- 2 Related Work -- 3 Event and Flow Capture Model -- 4 Event and Flow Matching Methods -- 4.1 Parameter-Based Matching Method -- 4.2 Time-Based Matching Method -- 4.3 Combined Matching Method.
5 DNS Communication Dataset.