1. Record Nr. UNISA996464530903316

Titolo	Socio-technical aspects in security and trust : 10th international workshop, STAST 2020, virtual event, September 14, 2020, revised selected papers / / Thomas Gross, Luca Vigano, editors
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-79318-4
Descrizione fisica	1 online resource (211 pages)
Collana	Lecture Notes in Computer Science ; ; 12812
Disciplina	005.8
Soggetti	Computer networks - Security measures - Social aspects
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Message from the Workshop Organizers -- Organization -- Contents -- Personality and Behavior -- How Can Personality Influence Perception on Security of Context-Aware Applications? -- 1 Introduction -- 2 Study Design -- 2.1 Motivating Scenario Example -- 2.2 Goal and Research Questions -- 2.3 Participant Selection -- 2.4 Hypothesis, Variables and Metrics -- 2.5 Web-Based Survey Implementation -- 2.6 Survey Validation and Conduction -- 3 Results -- 3.1 RQ1: How Do Service Consumers Perceive the Importance of Security of a Context-Aware Software Intensive System? -- 3.2 RQ2: Do the Personality Influence on the Importance Perceived of Security of Context-Aware Software Applications? -- 4 Threats to Validity -- 5 Related Work -- 6 Conclusions and Further Work -- References -- Refining the Blunt Instruments of Cybersecurity: A Framework to Coordinate Prevention and Preservation of Behaviours -- 1 Introduction -- 2 Managing Security for an Ecosystem of Behaviours -- 2.1 Discouraging Malicious Security-Related Behaviours -- 2.2 Encouraging Positive Security-Related Behaviours -- 2.3 Risk Management for Systems of Behaviours -- 2.4 Existing Examples -- 2.5 Related Work -- 2.6 Synthesis of Sociotechnical Risk-Related Research -- 3 Framework for Precision in Sociotechnical Controls -- 3.1 Prevention and Preservation of Behaviours -- 3.2 Intersection of Behaviours to Prevent or Preserve --

3.3 Identifying Lack of Precision in Risk Controls -- 3.4 Managing for the Precision of Risk Controls -- 4 Use Case-Online Abuse Controls for Social Media -- 4.1 Factors in Positive and Negative Behaviours -- 4.2 Risk Controls -- 4.3 Refining Risk Controls -- 5 Discussion -- 6 Conclusion -- References -- Behavior in Face of Adversaries -- Natural Strategic Abilities in Voting Protocols -- 1 Introduction -- 2 Methodology.
2.1 Modeling the Voting Process -- 2.2 Natural Strategic Ability -- 2.3 Natural Strategies and Their Complexity -- 3 Specification and Verification of Voting Properties Based on Natural Strategies -- 3.1 How to Specify Voter-Verifiability -- 3.2 Towards Dispute Resolution -- 3.3 Strategic-Epistemic Specifications -- 3.4 Receipt-Freeness -- 3.5 Using Verification Tools to Facilitate Analysis -- 4 Use Case Scenario: vVote -- 5 Models -- 5.1 Voter Model -- 5.2 Refinements of the Voter Model -- 5.3 Voting Infrastructure -- 5.4 Coercer Model -- 6 Strategies and Their Complexity -- 6.1 Strategies for the Voter -- 6.2 Counting Other Kinds of Resources -- 6.3 Natural Strategies for Coalitions -- 7 Automated Verification of Strategies -- 8 Conclusions -- References -- A Study of Targeted Telephone Scams Involving Live Attackers -- 1 Introduction -- 1.1 Social Engineering Study -- 1.2 Social Engineering Dataset -- 2 Telephone vs. Email Scams -- 3 Experimental Procedure -- 3.1 Ethical and Legal Concerns -- 4 Attack Scripts -- 4.1 Structure of a Script -- 4.2 Controlled and Uncontrolled Variables -- 5 Study Results -- 5.1 Demographics of the Participants -- 5.2 Success Rates -- 5.3 Hypotheses Tests -- 6 Discussion and Limitations -- 7 Telephone Scam Dataset -- 7.1 Transcript Examples -- 8 Related Work -- 8.1 Social Engineering Studies -- 8.2 Social Engineering Attack Datasets -- 9 Conclusion -- References -- Smart Environments -- User Privacy Concerns and Preferences in Smart Buildings -- 1 Introduction -- 2 Methodology -- 2.1 Survey Design -- 2.2 Questionnaire Structure -- 2.3 Case Study -- 2.4 Questionnaire Distribution -- 2.5 Analysis Methods -- 2.6 Ethics -- 3 Evaluation -- 3.1 Results -- 3.2 Thematic Analysis -- 4 Discussion -- 4.1 Further Analysis -- 4.2 Recommendations -- 4.3 Limitations -- 5 Conclusion -- A Questionnaire -- A.1 Background Information.
A.2 Views on Privacy -- A.3 Awareness of USB Data Collection and Access -- A.4 USB Privacy Concerns -- A.5 Information Page -- A.6 USB Privacy Concerns (Revisited) -- A.7 Consent -- References -- Work in Progress: Towards Usable Updates for Smart Home Devices -- 1 Introduction -- 2 Related Work -- 2.1 User Update Behaviors -- 2.2 IoT Updates -- 3 Methodology -- 3.1 Participant Recruitment and Demographics -- 3.2 Data Collection and Analysis -- 4 Preliminary Results -- 4.1 Update Modes and Notifications -- 4.2 Update Purpose and Urgency -- 4.3 Uncertainty About Update Status -- 4.4 Updates to Apps vs. Updates to Devices -- 4.5 Update Concerns -- 4.6 Relationship to Security -- 5 Discussion -- 5.1 Comparison to Traditional Updates -- 5.2 Informing Usable Updates -- 6 Limitations and Planned Future Work -- References -- Decentralized Systems and Digital Ledgers -- WARChain: Blockchain-Based Validation of Web Archives -- 1 Introduction -- 2 Related Works -- 3 Solution -- 4 Implementation -- 4.1 The EduPoS Blockchain -- 4.2 Validators -- 4.3 Crawler Simulator -- 5 Experiments -- 5.1 Experiment #1: Proof of Concept -- 5.2 Experiment #2: Validation -- 5.3 Experiment #3: Duplicate Detection -- 6 Conclusion and Future Work -- References -- Cyber 9/11 Will Not Take Place: A User Perspective of Bitcoin and Cryptocurrencies from Underground and Dark Net Forums -- 1 Introduction -- 2 Background -- 2.1 User Studies -- 2.2 Dark Net Studies -- 3 Research Questions -- 4 Research Method -- 4.1 Data

Collection Method -- 4.2 Sample Selection -- 4.3 Data Analysis -- 5 Ethics -- 6 Results and Analysis -- 6.1 It's About Finality, Not Anonymity -- 6.2 Anonymity Isn't Everything -- 6.3 The Payment Mechanism -- 6.4 Dark Nets Are Hard -- 7 Discussion -- 7.1 Implications for Policy -- 7.2 Limitations -- 8 Conclusion and Future Work -- References.
Self-Governing Public Decentralised Systems -- 1 Introduction -- 2 State of the Art -- 2.1 Proof-of-Work -- 2.2 Proof-of-Stake -- 2.3 Delegated Proof-of-Stake -- 2.4 Proof-of-Personhood -- 2.5 Proof-of-Authority -- 2.6 Voting `On-Ledger' -- 3 Problem Motivation -- 4 Solution -- 4.1 `One Person/One Vote' in Delegated Proof-of-Stake -- 4.2 Establishing Personhood -- 5 Conclusion and Future Work -- References -- Reflections on Socio-Technical Aspects of Security -- Statistical Reliability of 10 Years of Cyber Security User Studies -- 1 Introduction -- 2 Background -- 2.1 Statistical Inferences and Null Hypothesis Significance Testing -- 2.2 Effect Sizes and Confidence Intervals -- 2.3 Statistical Power -- 2.4 Research Biases -- 3 Related Works -- 3.1 Appraisal of the Field -- 3.2 Guidelines -- 4 Aims -- 5 Method -- 5.1 Sample -- 5.2 Procedure -- 6 Results -- 6.1 Sample -- 6.2 Effect Size Estimates and Their Confidence -- 6.3 Upper Bounds of Statistical Power -- 6.4 Power of Actual Tests -- 6.5 Publication Bias -- 6.6 The Winner's Curse -- 7 Discussion -- 7.1 Limitations -- 8 Concluding Recommendations -- A Sample Characteristics -- References -- Privacy, Security and Trust in the Internet of Neurons -- 1 Introduction: From the Human Computer to... the Human Computer -- 2 The IoN: From brainwaves to packets, and Vice versa -- 3 Privacy, Security and Trust -- 3.1 System Model -- 3.2 Threat Model -- 3.3 Security Properties -- 4 Conclusions -- References -- Author Index.