1. Record Nr. UNISA996466226903316

Titolo	Security Standardisation Research [[electronic resource]] : Second International Conference, SSR 2015, Tokyo, Japan, December 15-16, 2015, Proceedings / / edited by Liqun Chen, Shin'ichiro Matsuo
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-27152-0
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (X, 267 p. 41 illus. in color.)
Collana	Security and Cryptology ; ; 9497
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Computer communication systems Software engineering Data structures (Computer science) Computer science—Mathematics Systems and Data Security Cryptology Computer Communication Networks Software Engineering Data Structures Math Applications in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Preface -- Security Standardisation Research 2015 -- Contents -- Bitcoin and Payment -- Authenticated Key Exchange over Bitcoin -- 1 Introduction -- 2 Background -- 2.1 Bitcoin -- 2.2 Transaction Signature -- 3 Key Exchange Protocols -- 3.1 Setting the Stage -- 3.2 Authentication -- 3.3 Diffie-Hellman-over-Bitcoin Protocol -- 3.4 YAK-over-Bitcoin Protocol -- 4 Security Analysis -- 4.1 Security of Diffie-Hellman-over-Bitcoin -- 4.2 Security of YAK-over-Bitcoin -- 4.3 Security of ECDSA Signatures -- 5 Implementation -- 5.1 Time Analysis -- 5.2 Note About Domain Parameters -- 6 Conclusion -- References

-- Tap-Tap and Pay (TTP): Preventing the Mafia Attack in NFC Payment -- 1 Introduction -- 2 Our Solution: Tap-Tap and Pay (TTP) -- 2.1 Threat Model -- 2.2 Overview of the Solution -- 2.3 Sensor Data Preprocessing -- 2.4 Similarity Comparison -- 3 System Evaluation -- 3.1 Experiment Setup and Data Collection -- 3.2 Results -- 3.3 Online and Offline Modes -- 4 Usability Study -- 4.1 Experiment Setup and Data Collection -- 4.2 Findings -- 5 Comparison with Previous Works -- 6 Further Related Works -- 7 Conclusion -- References -- Protocol and API -- Robust Authenticated Key Exchange Using Passwords and Identity-Based Signatures -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 1.3 Organization -- 2 Preliminaries -- 3 Security Model -- 4 Our Identity-Based Signature Scheme -- 5 Our IBS-PAKE Protocols -- 5.1 Generic Construction -- 5.2 Instances -- 5.3 Security Proofs -- 6 Performance Analysis -- 6.1 Performance Comparison -- 6.2 Experimental Results -- 7 Conclusion -- A Bilinear Maps -- B Computational Assumptions -- C Simplified IBS-PAKE Protocols -- References -- Non-repudiation Services for the MMS Protocol of IEC 61850 -- 1 Introduction -- 2 The State of the Art -- 2.1 The standard IEC 61850 -- 2.2 The Standard IEC 62351.
2.3 The Weak Point of IEC 62351 -- 2.4 Additional Security Requirements -- 3 A Security Solution for the A-Profile -- 3.1 Difference Between NROT and NRDT -- 3.2 Generation of NROT and NRDT -- 3.3 The Verification of the APDUs -- 3.4 Checking the NRDT -- 3.5 NRD Tokens for the Server -- 3.6 The Application Security Sublayer -- 3.7 Providing the APDUs with Tokens -- 3.8 Access Control Lists -- 3.9 Logging of Events -- 4 An Implementation Using XML Signatures -- 4.1 How the Process Works -- 4.2 The Modified Communication -- 4.3 Example -- 4.4 Advantages of XML Signatures and Tokens -- 4.5 Possible Disadvantages of XML Signatures -- 5 Conclusion -- References -- Analysis of the PKCS#11 API Using the Maude-NPA Tool -- 1 Introduction -- 2 Maude-NPA -- 2.1 Preliminaries on Unification and Narrowing -- 2.2 Maude-NPA Syntax and Semantics -- 2.3 Never Patterns in Maude-NPA -- 3 PKCS#11 -- 4 Specification of PKCS#11 in Maude-NPA -- 4.1 Formal Model of PKCS#11 in Maude-NPA -- 4.2 Specification of PKCS#11 in Maude-NPA's Syntax -- 5 Experiments -- 6 Related Work -- 7 Conclusions -- References -- Analysis on Cryptographic Algorithm -- How to Manipulate Curve Standards: A White Paper for the Black Hat http: //bada55.cr.yp.to -- 1 Introduction -- 1.1 Elliptic-Curve Cryptography. -- 1.2 Organization. -- 1.3 Research Contributions of this Paper. -- 2 Public Security Analyses -- 2.1 Warning: Math Begins Here. -- 2.2 Review of Public ECDLP Security Criteria. -- 2.3 ECC Security vs. ECDLP Security. -- 2.4 The Probability of Passing Public Criteria. -- 2.5 The Probabilities for Various Feasible Attacks. -- 3 Manipulating Curves -- 3.1 Curves Without Public Justification. -- 3.2 The Attack. -- 3.3 Implementation. -- 4 Manipulating Seeds -- 4.1 Hash Verification Routine. -- 4.2 Acceptability Criteria. -- 4.3 The Attack. -- 4.4 Optimizing the Attack. -- 4.5 Implementation.
5 Manipulating Nothing-up-my-sleeve Numbers -- 5.1 The Brainpool Procedure. -- 5.2 The BADA55-VPR-224 Procedure. -- 5.3 How BADA55-VPR-224 Was Generated: Exploring the Space of Acceptable Procedures. -- 5.4 Manipulating Bit-Extraction Procedures. -- 5.5 Manipulating Choices of Hash Functions. -- 5.6 Manipulating Counter Sizes. -- 5.7 Manipulating Hash Input Sizes. -- 5.8 Manipulating the (a, b) Hash Pattern. -- 5.9 Manipulating Natural Constants. -- 5.10 Implementation. -- 6 Manipulating Minimality -- 6.1 NUMS Curves. -- 6.2 Choice of Security Level. -- 6.3 Choice of Prime. -- 6.4 Choice of Ordering of Field Elements. -- 6.5 Choice of Curve Shape and Cofactor

Requirement. -- 6.6 Choice of Twist Security. -- 6.7 Choice of Global vs. Local Curves. -- 6.8 More Choices. -- 6.9 Overall Count. -- 7 Manipulating Security Criteria -- Security of the SM2 Signature Scheme Against Generalized Key Substitution Attacks -- 1 Introduction -- 1.1 Our Contributions -- 2 Preliminaries -- 2.1 Collision-Resistant Hash Functions -- 2.2 Uniform (Smooth) Hash Functions -- 2.3 Almost-Invertibility of Conversion Functions -- 3 Definitions -- 4 Generalized WKS Attacks Against a General Framework of ISO/IEC CD 14888-3 -- 5 Security of the SM2 Signature Scheme -- 5.1 SM2 Digital Signature Scheme -- 5.2 EUF-CMA Security of SM2 -- 5.3 Security of SM2 Against Generalized SKS Attacks -- References -- Side Channel Cryptanalysis of Streebog -- 1 Introduction -- 2 Description of Streebog -- 3 The Message Recovery Attack -- 3.1 Implications of Our Attack -- 4 Countermeasures -- 5 Conclusions -- References -- Privacy -- Improving Air Interface User Privacy in Mobile Telephony -- 1 Introduction -- 2 Background -- 2.1 Mobile Telephony Systems -- 2.2 Proactive UICC -- 2.3 The AKA Protocol -- 3 User Privacy Threats -- 4 Threat Model -- 5 A Pseudonymity Approach -- 6 Predefined Multiple IMSIs.
6.1 USIM-Initiated IMSI Change -- 6.2 Network-Initiated IMSI Change -- 7 Modifiable Multiple IMSIs -- 8 Experimental Validation -- 9 Analysis -- 9.1 User Privacy -- 9.2 IMSI Synchronisation -- 10 Related Work -- 11 Conclusions -- References -- Generating Unlinkable IPv6 Addresses -- 1 Introduction -- 2 Background -- 2.1 Stateless Address Autoconfiguration (SLAAC) -- 2.2 Privacy Extensions to SLAAC -- 2.3 The Gont Approach -- 2.4 The Rafiee-Meinel Scheme -- 2.5 Other Schemes -- 2.6 A Summary -- 3 Practical Limitations to Privacy -- 3.1 Use of Randomness -- 3.2 Privacy Goals -- 3.3 RFC 4941 Method 1 -- 3.4 RFC 4941 Method 2 and the Rafiee-Meinel Scheme -- 3.5 The Gont Scheme -- 4 Practical Measures to Improve Randomness Generation -- 4.1 Generating Randomness -- 4.2 A Simple Improvement to RFC 4941 Method 1 -- 4.3 Making the Gont Scheme More Robust -- 5 Summary and Conclusions -- References -- Trust and Formal Analysis -- A Practical Trust Framework: Assurance Levels Repackaged Through Analysis of Business Scenarios and Related Risks -- 1 Introduction -- 2 Related Work on Trust Framework -- 3 Assessment Criteria of Assurance Levels -- 3.1 Credential Issuance and Identity Proofing Process Requirements -- 3.2 Authentication Process Requirements -- 3.3 Requirements for Certification -- 4 Analysis of Business Scenarios in Terms of Assurance Levels -- 4.1 Design Objectives of Field Survey -- 4.2 Classification of Business Scenarios -- 4.3 Self-Regulation and Objectivity -- 4.4 Effectiveness of High Level Authentication Processes -- 5 Level of Assurance 1+ -- 6 Concluding Remarks -- References -- First Results of a Formal Analysis of the Network Time Security Specification -- 1 Introduction -- 2 Security for Packet-Based Time Synchronization -- 2.1 Time Synchronization Methods -- 2.2 Criteria for Different Stages of Analysis.
2.3 Choice of Tool for the Analysis -- 3 Basic Assumptions and Protocol Notation -- 4 The Protocol Steps Under Analysis -- 4.1 The Network Time Security Project -- 4.2 Overview of the Protocol Sequence -- 5 Performing the Analysis -- 6 Results of the First Analysis -- 7 Conclusion -- A ProVerif Source Code -- A.1 Cryptographic Primitives -- A.2 Global Variables and Constants -- A.3 Events -- A.4 The Trusted Authority Process -- A.5 The Server Side Processes -- A.6 The Client Side Processes -- A.7 The Environment Process -- A.8 ProVerif Queries -- References -- Formal Support for Standardizing Protocols with State -- 1 Introduction -- 2 The Envelope Protocol -- 3 State-Respecting Bundles -- 3.1 Enriching Bundles with

State -- 3.2 Our Axioms of State -- 3.3 Enrich-by-need for Stateful Protocols -- 4 Analysis of the Envelope Protocol -- 4.1 The Importance of Observer Ordering -- 5 Related Work -- 6 Protocol Security Goals -- 7 Conclusion -- References -- Author Index.

Sommario/riassunto

This book constitutes the refereed proceedings of the Second International Conference on Security Standardisation Research, SSR 2015, held in Tokyo, Japan, in December 2015. The 13 papers presented in this volume were carefully reviewed and selected from 18 submissions. They are organized in topical sections named: bitcoin and payment; protocol and API; analysis on cryptographic algorithm; privacy; and trust and formal analysis. .