Tätigkeitsbericht 2014/2015

Horst Görtz Institut
für IT-Sicherheit

Sehr geehrte Damen und Herren,
liebe Freunde des Horst Görtz Instituts,

das HGI steht für Exzellenz in Forschung, Lehre und Nachwuchsförderung. In dieser Ausgabe möchten wir Ihnen – zusätzlich zu den Einblicken in unsere Forschungsvorhaben, die Sie in der Sonderausgabe 2016 von RUBIN nachlesen können – einige Statistiken zu unserer Forschung und Ausbildung in der IT-Sicherheit aus den Jahren 2014 und 2015 angeben.

In diesen beiden überaus eindrucksvollen Jahren haben insgesamt 210 Absolventinnen und Absolventen erfolgreich ein Studium der IT-Sicherheit an der Ruhr-Universität Bochum beendet, davon 123 Bachelor- und 87 Masterabschlüsse. Hinzu kommen 15 Promotionen aus den verschiedensten Bereichen der IT-Sicherheit.

Wir blicken auf insgesamt 210 wissenschaftliche Veröffentlichungen auf renommierten internationalen Konferenzen und in Zeitschriften zurück, die ebenso wie die 11 Preise, mit denen unsere Wissenschaftlerinnen und Wissenschaftler im Berichtszeitraum ausgezeichnet wurden, den Erfolg und die internationale Sichtbarkeit des Instituts veranschaulichen.

Nicht zuletzt blicken wir auf unsere vier jüngsten Firmenausgründungen, die das im Studium erworbene theoretische Wissen erfolgreich in eigene Geschäftsideen umgewandelt haben und florierende junge Start-ups erschaffen haben.

Wir wünschen Ihnen und Euch viel Spaß beim Lesen.

Ihr

Prof. Christof Paar

Geschäftsführender Direktor des
Horst Görtz Instituts

Bachelor IT-Sicherheit

Malware in the Wild: Android Malware in 3rd Party Markets

Implementation of a Channel-based Key Establishment Protocol on a Resource-constrained Platform

Secure Execution of Cryptographic Algorithms on Embedded Devices using Smartcards

Location Based Security using Software-Defined Radio on Smartphones

Implementing a Virtual Machine-based fingerprinting Scheme

Detection and Analysis of Malicious DNS Resolvers

A Cooperative Approach to Affordable Data Retention

TLS secure bindings and their application in Single Sign-On schemes

Possibilities and Limitations of Timing Side-Channel Attacks in the Cloud

Entwurf und Evaluation eines Hardwarebeschleunigers für Elliptische-Kurven-Kryptographie

On Certificate Validation in SSL Implementations

Security Analysis of a Bluetooth-based Door Lock

Design and Implementation of a Flexible Configuration-File-Based PKI Code Generator

Security Analysis of Diagnostic and Communication Interfaces in Automobiles

An Evaluation Framework for Channel-based Key Establishment Systems

BYOB: Keystroke Localization using Smartphone Microphones

Static Analysis and Extraction of ROP Gadgets

Analysis of PHP Bytecode Protection Mechanisms

2nd order Cyclostationarity of Side-Channel Leaks: Impact on Future Attacks?

Systematic Analysis and Classification of XSLT Attacks

Security Analysis of the Square Mobile Payment Application

Efficient Implementation of NTRUEncrypt on ARM Platforms using NEON ISE

Implementation of a Test Suite for Laser Fault Injection

Efficiency Analysis of Block Ciphers on Sensor Nodes

Entwurf und Evaluation eines Hardwarebeschleunigers für Elliptische-Kurven-Kryptographie

Berechtigungskonzepte zur Datenschutzselbstkontrolle: Desktop und Smartphone Betriebssysteme im Vergleich

Praktische Sicherheitsevaluierung des Funkstandards ZigBee

External Management of Android User Secrets on a Bluetooth Interfaced Secure Element

Analysis of Stratum - a Bitcoin Mining Pool Protocol

Sourcecodebasierte Analyse des Instant Messengers TextSecure

On the Feasibility of Timing Attacks on WPA2 Implementations

Biometrics and Privacy - An Evaluation of Biometric Template Protection

Enhancing Security for IEEE 802.11 Wireless Networks with a Key-Evolving Approach using Channel Variations

User authentication from acceleration sensor data

How Safe is Your Safe? - A Security Analysis of an Electronic Safe Lock

Characterization of Laser-Induced Faults on an 8-Bit Microcontroller

Development of a Smartphone-Based Module for the Security Analysis of Remote Keyless Entry Systems

Dynamic Key Agreement for VOIP Encryption on Reconfigurable Devices

Erweiterung eines virtuellen Network-on-Chip-basierten Multiprozessorsystems hinsichtlich gemeinsam genutzten Speichers

Praktische Sicherheitsanalyse des Mozilla Single Sign-On Protokolls BrowserID

Webbasiertes Management geschlossener Benutzergruppen für mobile Sprachkommunikationssysteme auf Basis von Hardware Security Modulen

On-line Entropy Estimation for Physical Layer Security

Implementing a Network-based Intrusion Detection System for CAN-based Automotive Networks

Trustworthy Transmission of Vehicle Status Data to a Smart Device

Mobile Device Fingerprinting Utilizing Hardware-Tolerances of Accelerometers

Efficient Machine Learning-Attacks on Physically Unclonable Functions

Understanding Free Proxies and their Business Model

Side-Channel Analysis of Automotive Access Control Systems

A Comparison of PRIDE to Other Block Ciphers on Microcontrollers

Erkennungsraten bei der Sprachsteuerung komplexer Softwaresysteme

Entwicklung einer graphischen Benutzeroberfläche (GUI) zur 3D-Visualisierung und Steuerung eines CFD-Vernetzers mittels QT und objektorientierter C++ Programmierung sowie Dual-Quaternion basierter OpenGL-Darstellung

JTAG Port Probing and Discovery

Implementation and Evaluation of Differential Power Attacks against a Mask-Protected AES Implementation

Authentication of a Hardware Security Module against a User

Reengineering of a Password Guessing Framework

Algebraischer Angriff auf SEA

On the Portability of Instruction Recovery using the EM Side Channel

Implementation and Evaluation of a Recycling-based Channel Estimation Scheme for Physical Layer Security

Don't Trust Open Hotspots: Wi-Fi Hacker Detection and Privacy Protection via Smartphone

Detecting Rule Evasion Attacks on SDN Controllers

Ok Google, Call Hacker. Using Acoustic Obfuscation to Execute Google Voice Commands

A Security Analysis of Private Cloud Interfaces in openQRM

Blended Attacks Abusing The Web

Efficient DPA on Xilinx Bitstream Encryption Feature

Architektur- und Sicherheitsanalyse von Tresorit und Tresorit DRM

Version Detection by Fingerprinting Piwik Installations

Automated Power Equalization as Side-Channel Countermeasure for Reconfigurable Devices

Benutzerfreundlichkeit als Sicherheitsproblem - Schwachstellenanalyse von WLAN-Konfigurationen mobiler Endgeräte

Laser-Assisted Reverse Engineering of Cryprographic Schemes

Log Me In with Facebook: Security Analysis of Facebook Connect

Sicherheitsanalyse von OpenID Connect Implementierungen

Design and Simulation of Parallel Image Processing Systems in a Virtual Prototyping Tool

Implementation of an ARM Hooking Engine to Fuzz FirefoxOS IPC

Evaluation of Natural Language Processing as a Method for Stylometry Obfuscation

Development of a Web Crawler to Harvest Personal Information for Password Guessing

Sound of Silence: Wi-Fi Eavesdropping and Traffic Analysis on Android

Sicherheitsauswirkung durch Googles Sprachsteuerung

Analyse von Microsofts Right Management Services in Windows Server 2012R2

Sicherheitsanalyse der Private Cloud Plattform Apache CloudStack

Automated Security Concept Generation and Evaluation for Design Space Exploration of Embedded Systems

Secure and Efficient Implementation of Fuzzy Extractors

Phishing-Erkennung mittels visuellem Ähnlichkeitsvergleich

ECU-Fuzzing in Automotive Networks

Analysis of Modes of Operation in the Context of Backwards Compatibility

Implementing a Framework for Comparing Password Guessing Tools

Concept and Implementation of Measures to increase IT-Security in an industrial Verificationmanagement-Workflow

Untersuchung von Playload Analyse Lösungen zur Erkennung von gezielten Angriffen im Netzwerkverkehr

Digitale Signaturen im Standard Model

Penetration Testing Guide for Hybrid Android Applications

Efficient Software Conversion between Arithmetic and Boolean Masking Schemes

Strong-RSA-basierte Signaturen ohne teure Primzahlgenerierung

Analyse einer embedded Linux-Plattform unter Verwendung einer µSD-Smartcard hinsichtlich der Eignung als mobile Ende-zu-Ende-Sprachverschlüsselungslösung

Interfering with Smartcard Communication Protocols

Hardening OpenID Connect Authentication Flow via the TLS Secure Binding Holder-of-Key

On Compromising Metadata for Cross-Site Scripting in PGP Keys

Practical Man-In-The-Middle Attacks on Passive Car Entry Systems

Data-Aware In-Memory Fuzzing

Implementation of a Framework for Automatic Reverse-Engineering of Xilinx FPGA Designs

Implementation of a Novel Channel-based Key Extraction and Authentication Scheme on a smartphone

Implementierung eines Plugins zur Automatisierung von Smartphone Apps und Anbindung an eine automotive Testautomatisierungsumgebung

Sicherheitsanalyse des Single Sign-On Dienstes Microsoft-Konto

Implementierung von Cramer-Shoup Verschlüsselung in CrypTool 2

Incorporating DTLS into the penetration testing framework TLS-Attacker

Full-capable Physical Layer Security Demonstration System

Housebreaking 2.0 - Security Analysis of a modern Home Automation System

Security Analysis of the Vawtrak Botnet

Microsoft Azure - Design und Architektur

Analysis of Encrypted Databases with CryptDB

Sicherheitsanalyse von Facebook-Login auf Android Systemen

Analysis of Applied Cryptography in Android Applications

Analyse von Verschleierungsalgorithmen für Android-Apps

Automatic Recognition, Processing and Attacking of Single Sign-On Protocols with Burp Suite

Automatische Analyse von HTTP Headern zur Absicherung von Webanwendungen

Development of a Secure SDN Application Environment

Validation of Eduroam Authentication Configuration using an Intel Galileo Board

Efficient Incremental Implementation of Side-Channel Evaluation and Attack Methods for Multi-Core Platforms

Management von verschiedenen User- und Rechte-Gruppen in gekoppelter Software mit Hilfe von Identity und Access Management

Using Localized Electro-Magnetic Emanations for Instruction Recovery on Atmel ATXMega Microcontrollers

Optimizing Time-Based Blind SQL Injections

Meaningful Computational Problems in Cryptocurrencies

Master IT-Sicherheit | Informationstechnik

Type Recovery on VEX Intermediate Representation

Fingerprinting Mobile iOS Devices for Fraud Detection

GPU-Assisted Password Hashing: The Example of scrypt

Reverese Engineering and Protocol Analysis: On the Security of a Wireless Locking System

Analysis and Design of a Secure Automotive In-Vehicle Communication and Electronics Architecture

Integration von Application Phase basierten Angriffen in das T.I.M.E. Framework am Beispiel des TLS Renegotiation Angriffs

Evaluation of SMC Techniques to Address Typical Security Issues in Enterprises

Security Analysis of the OpenID Connect Standard and its real-life Implementations

Design and Development of a modular Penetration Testing Tool for the Analysis of Automotive Buses

Retrofitting SGX with a Hypervisor

Nearest Neighbor: Faster Decoding of Random Linear Codes

Construction of a Demonstrator for Man-in-the-Middle attacks on GSM

Analyzing Location Privacy in GSM Mobile Telephony using Software Radios

Malware Classification Based on Simulated Network Traffic

Extremely Short Group Signatures (XSGS) for Privacy Conserving E-Mobility Applications

SOAKMS - A Service-Oriented Architecture Key-Management System

User identification based on application information combined with system and sensor information on Android devices

Exploiting Physical Characteristics for Novel Wireless Security Mechanisms

Design and Implementation of a Secure and Non-Interactive Update Framework for Embedded Devices

Nearest Neighbor: Faster Decoding of Random Linear Codes

Cryptographic Analysis of IPsec IKE

Security Analysis of the OpenID Connect Standard and its real-life Implementation

Combining Laser Fault Injection and Side-Channel Analysis

Malware Clustering Based on Static and Dynamic Analysis

Retrospective Malware Detection via Behavior Graph-Based Analysis

On Learning Generated Authentication Secrets: The Example of Knock Patterns

A Centralized Key Management Solution for S/MIME

Side-Channel Resistant Realization of PRINCE under Asynchronous Logic Design

Integration of a Mix Network within Tor

Hiding under the Open Sky(pe) - A steganographic Scheme for Skype's audio codec SILK

Preventing Side-Channel Analysis by Dynamic Partial Reconfiguration of Reconfigurable Hardware

Forensic Analysis of the B-Tree File-system (BTRFS)

Side-Channel Resistant Implementation of Lattice-Based Cryptography on Embedded Devices

Multimodal Biometric Authentication

Securing Mobile Banking Applications Against Mobile Threats

Automatisierte kontextsensitive Analyse von iOS Apps

Development of a Basic Embedded Operating System for Mixed Criticality Applications on a Heterogeneous Computing Platform

Differential Cryptanalysis Attack on Zorro Cipher using RIVYERA

Static data flow analysis and constraint solving to craft inputs for binary programs

Master IT-Sicherheit | Netze und Systeme

Cryptographic Hardware Trojans in FPGA Bitstreams

Signaturverfahren mit scharfen Sicherheitsbeweisen

Differential Trail Weights in AES-like Ciphers Using New Permutation Layers

Anbindung eines Trusted Platform Module an die Festplattenverschlüsselung TrustedDisk

Blackbox Penetration Testing of LCOS

A Study on the Security of User Authentication Methods for Smartphones: Android Unlock Patterns

Utilizing Homomorphic Cryptography to Improve Privacy in Driving Pattern-Based Insurance Plans

Effiziente kurze digitale Signaturen basierend auf der diskreten Logarithmus-Annahme und der RSA-Annahme

Kryptographische Analyse von IPsec

Preventing Backdoors by Ensuring the Modular Integrity of Processes in POSIX OS

Implementierung von ISD-Angriffen auf kodierungsbasierte Kryptographie

Entwicklung eines Konzeptes für die Sicherheitsanalyse datenbankbasierter Java-Webanwendungen

Graphical Fallback Authentication

Fingerprinting Android Devices via Browsers

Evaluating the Feasibility of Side-Channel Attacks on Fingerprint Readers

Security Analysis of Real-World Random Number Generators

Vendor Independent Android Containerization

Verifiable Random Functions

A Study on the Security of User Authentication Methods for Smartphones

Stealth Hardware Trojan Generation and Implantation

Rebound Attack on JH Hash Function

SSO Security in the Wild - An Automated Security Evaluation of OpenID Websites

Low-Latency Memory Encryption on Programmable SoCs

Developing a Backup Monitoring Plug-in for the ICINGA Monitoring Tool

Schaffung einer Zertifizierungsgrundlage für ein HSM-B

Analyse und Vergleich von Standards für Penetrationstests

Web Applications and Technologies

Private Information Retrieval & Trapdoor Function

Security Analysis of MSP430 Firmware Images on the Basis of VEX Intermediate Representation

Preventing Information Leaks via Compile-time Instrumentation (PILCI)

Binary Patch Fuzzing

Security Implications of DTD Attacks Against a Wide Range of XML Parsers

Stealth Hardware Trojan Generation and Implantation

MySSL, a client side TLS test framework

XnR for Windows: Implementation and Evaluation

Entwurf und Evaluierung eines LLVM Compiler Back-Ends für ein FPGA-basiertes Multiprozessor System-on-Chip

Timing-based Side-Channel Attacks over Networks

Introducing Physical Layer Security for 8-bit Commercial Off-the-Shelf Wireless Transceiver Platforms

Cross Platform Code Gadget Discovery for Code Reuse Attacks

Implementierung und Analyse eines Algorithmus zum Finden von Vektor-Paaren mit kürzestem Abstand

Automated Detection of Evasive Malware on Android

HW/SW Co-Design of Attribute-Based Encryption on Reconfigurable Hardware

Development of a Framework for Applied LTE Security Analysis

Side-Channel Evaluation of a Complex System-on-Chip in Automotive Applications

Efficient Implementation of a Generic Coprocessor for Elliptic Curve Cryptography on Reconfigurable Hardware

Dynamic Analysis of ARM Applications Using Hardware Virtualization Extensions

Broadcast Encryption

Promotionen

Christopher Meyer

20 Jahre Forschung an SSL/TLS - Eine Analyse der Basistechnologie für Internetsicherheit

Betreuer: Prof. Jörg Schwenk
Januar 2014

Sebastian Uellenbeck

Der Weg zur sicheren und nutzbaren Nutzerauthentifizierung auf mobilen Geräten

Betreuer: Prof. Thorsten Holz
Mai 2014

Johannes Hoffmann

From Mobile to Security – Towards Secure Smartphones

Betreuer: Prof. Thorsten Holz
August 2014

Michael Kallweit

Margin Parameters for Linear Classification and Their Connectionsto Selected Complexity Measures

Betreuer: Prof. Hans Simon
August 2014

Gottfried Herold

Applications of Classical Algebraic Geometry to Cryptography

Betreuer: Prof. Alexander May
Dezember 2014

Tilman Frosch

On Mitigation of Client-Side Attacks and Protection of Private Data

Betreuer: Prof. Thorsten Holz
Januar 2015

Malte Darnstadt

An Investigation on the Power of Unlabeled Data

Betreuer: Prof. Hans Ulrich Simon
Februar 2015

Elif Bilge Kavun

Resource-efficient Cryptography for Ubiquitous Computing: Lightweight Cryptographic Primitives from a Hardware & Software Perspective

Betreuer: Prof. Christof Paar
Februar 2015

Saqib A. Kakvi

On the Improvement of Security Proofs: Bridging the Gap between Theory and Practice

Betreuer: Prof. Eike Kiltz
Februar 2015

Christoph Bader

On the Possibility and Impossibility of Tight Reductions in Cryptography

Betreuer: Prof. Jörg Schwenk
Juni 2015

Marc Kührer

Large-Scale Analysis of Network-based Threats and Potential Countermeasures

Betreuer: Prof. Thorsten Holz
Juli 2015

Thomas Pöppelmann

Efficient Implementation of Ideal Lattice-Based Cryptography

Betreuer: Prof. Tim Güneysu
Juli 2015

Ralf Zimmermann

Cryptanalysis Using Reconfigurable Hardware Clusters for High-Performance Computing

Betreuer: Prof. Christof Paar
Juli 2015

Ahmed Hussen Abdelaziz

Noise-robust HMM-based Pattern Recognition using Multimodal Features and Observation Uncertainties

Betreuerin: Prof. Dorothea Kolossa
August 2015

Felix Schuster

Securing Application Software in Modern Adversarial Settings

Betreuer: Prof. Thorsten Holz
September 2015

Start-ups

RIPS (2016)

www.ripstech.com

Cyber Defence (2015)

PHYSEC (2015)

www.physec.de

Forthmind (2015)

Auszeichnungen und Preise

Amir Moradi, Sylvain Guilley, Annelie Heuser

Best Student Paper Award - International Conference on Applied Cryptography and Network Security

Juni 2014

David Oswald

Eickhoff Promotionspreis

Juli 2014

Thorsten Holz, Johannes Dahse

Internet Defense Preis

August 2014

Johannes Dahse, Nikolai Krein, Thorsten Holz

CCS Best Paper Award

November 2014

Florian Bergsma, Benjamin Dowling, Florian Kohlar, Jörg Schwenk, Douglas Stebila

CCS Best Paper Award

November 2014

Hendrik Meutzner, Viet Hung Nguyen, Thorsten Holz, Dorothea Kolossa

ACSAC Outstanding Paper Award

Dezember 2014

Tilman Frosch, Sven Schäge, Martin Goll, Thorsten Holz

CPDP Junior Scholar award

Januar 2015

Amir Moradi, Gesine Hinterwälder

Best Paper Award – 6th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2015

April 2015

SkIDentity

European Identity & Cloud Award 2015

Mai 2015

Christian Zenger, Dr. Benedikt Driessen, Heiko Koepke und Jan-Felix Posielek

EXIST Grant

Juni 2015

Tilman Frosch

Wissenschaftspreis der Gesellschaft für Datenschutz und Datensicherheit (GDD)

Dezember 2015

Irfan Altiok, Sebastian Uellenbeck, Thorsten Holz

GraphNeighbors: Hampering Shoulder-Surfing Attacks on Smartphones

Sicherheit 2014: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Wien, März 2014

Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow and Ahmad-Reza Sadeghi

On the (In)Security of Mobile Two-Factor Authentication

18th International Conference on Financial Cryptography and Data Security, FC 2014, Barbados

Alex Escala, Javier Herranz, Benoît Libert, Carla Ràfols

Identity-Based Lossy Trapdoor Functions: New Definitions, Hierarchical Extensions, and Implications

Public Key Cryptography 2014: 239-256

Hugo Gascon, Sebastian Uellenbeck, Christopher Wolf, Konrad Rieck

Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior

Sicherheit 2014: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Wien, März 2014

Shankar Karuppayah, Christian Rossow, Mathias Fischer, Max Mühlhäuser

On Advanced Monitoring in Resilient and Unstructured P2P Botnets

2014 IEEE International Conference on Communications, ICC 2014, Sydney, Australien

Eike Kiltz, Daniel Masny, Krzysztof Pietrzak

Simple Chosen-Ciphertext Security from Low-Noise LPN

Public Key Cryptography 2014: 1-18

Marius Konitzer and Hans Ulrich Simon

DFA with Bounded Activity Level

Proceedings der 8th International Conference on Language and Automata Theory and Applications (LATA 2014)

Kim Pecina, Esfandiar Mohammadi and Christina Pöpper

Zero-Communication Seed Establishment for Anti-Jamming Techniques

Proceedings des NDSS , Workshop on Security of Emerging Networking Technologies (SENT), 2014

Christian Rossow

Amplification Hell: Revisiting Network Protocols for DDoS Abuse

Annual Network & Distributed System Security Symposium (NDSS), San Diego, Februar 2014

Johannes Dahse, Thorsten Holz

Simulation of Built-in PHP features for Precise Static Code Analysis

Annual Network & Distributed System Security Symposium (NDSS), San Diego, Februar 2014

Hendrik Meutzner, Viet-Hung Nguyen, Thorsten Holz, Dorothea Kolossa

Using Automatic Speech Recognition for Attacking Acoustic CAPTCHAs: The Trade-off between Usability and Security

ACSAC, New Orleans, USA, Dezember 2014

Malte Darnstädt, Hendrik Meutzner, Dorothea Kolossa

Reducing the Cost of Breaking Audio CAPTCHAs by Active and Semi-Supervised Learning

ICMLA, Detroit, USA, Dezember 2014

Alexander May, Ilya Ozerov

A Generic Algorithm for Small Weight Discrete Logarithms in Composite Groups

Selected Areas in Cryptography, Springer LNCS, 2014

Francesco Aldà, Hans Ulrich Simon

Randomized Response Schemes, Privacy and Usefulness

Proceedings des 7th ACM Workshop on Artificial Intelligence and Security

Malte Darnstaedt, Thorsten Kiss, Sandra Zilles and Hans Ulrich Simon

Order Compression Schemes

Theoretical Computer Science (TCS)

Thorsten Doliwa, Gaojian Fan, Sandra Zilles and Hans-Ulrich Simon

Recursive Teaching Dimension, VC-Dimension and Sample Compression

Journal of Machine Learning Research (JMLR)

Malte Darnstaedt, Balazs Szoerenyi and Hans Ulrich Simon:

Supervised Learning and Co-Training

Theoretical Computer Science (TCS)

Andrey Bogdanov, Elif Bilge Kavun, Elmar Tischhauser, Tolga Yalçin

Large-Scale High-Resolution Computational Validation of Novel Complexity Models in Linear Cryptanalysis

Journal of Computational and Applied Mathematics, Ausgabe 259, Teil B, 592-598. Elsevier, 2014

Martin R. Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, Tolga Yalçin

Block Ciphers – Focus On The Linear Layer (feat. PRIDE)

34th International Cryptology Conference 2014 (CRYPTO'14), Ausgabe 8616 Lecture Notes in Computer Science, 57-76. Springer, 2014

Martin R. Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, Tolga Yalçin

Block Ciphers – Focus On The Linear Layer (feat. PRIDE): Full Version

In IACR Cryptology ePrint Archive 2014:453, 2014

Naveed Ahmed, Christina Pöpper, Srdjan Capkun

Enabling Short Fragments for Uncoordinated Spread Spectrum Communication

Proceedings of the European Symposium on Research in Computer Security (ESORICS), September 2014

Christian T. Zenger, Markus Chur, Jan-Felix Posielek, Gerhard Wunder, Christof Paar

A Novel Key Generating Architecture for Wireless Low-Resource Devices

3rd International Workshop on Secure Internet of Things (SIoT), 2014

René Guillaume, Christian T. Zenger, Andreas Mueller, Christof Paar, Andreas Czylwik

Fair Comparison and Evaluation of Quantization Schemes for PHY-based Key Generation

18th International OFDM Workshop (InOWo), 2014

Christian T. Zenger, Abhijit Ambekar, Fredrik Winzer, Thomas Pöppelmann, Hans D. Schotten, Christof Paar

Preventing Scaling of Successful Attacks: A Cross-Layer Security Architecture for Resource-Constrained Platforms

1st International Conference on Cryptography and Information Security (BalkanCryptSec), 2014

Jannik Pewny, Felix Schuster, Lukas Bernhard, Christian Rossow, Thorsten Holz

Leveraging Semantic Signatures for Bug Search in Binary Programs

Annual Computer Security Applications Conference (ACSAC), New Orleans, USA, Dezember 2014

Robert Gawlik, Thorsten Holz

Towards Automated Integrity Protection of C++ Virtual Function Tables in Binary Programs

Annual Computer Security Applications Conference (ACSAC), New Orleans, USA, Dezember 2014

Michael Backes, Thorsten Holz, Benjamin Kollenda, Philipp Koppe, Stefan Nürnberger, Jannik Pewny

You Can Run but You Can't Read: Preventing Disclosure Exploits in Executable Code

21st ACM Conference on Computer and Communications Security (CCS), Scottsdale, Arizona, USA, November 2014

Apostolis Zarras, Alexandros Kapravelos, Gianluca Stringhini, Thorsten Holz, Christopher Kruegel, Giovanni Vigna

The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements

2014 Internet Measurement Conference (IMC), Vancouver, Canada, November 2014

Apostolis Zarras

The Art of False Alarms in the Game of Deception: Leveraging Fake Honeypots for Enhanced Security

48th IEEE International Carnahan Conference on Security Technology (ICCST), Rome, Italy, Oktober 2014

Johannes Dahse, Nikolai Krein, Thorsten Holz

Code Reuse Attacks in PHP: Automated POP Chain Generation

21st ACM Conference on Computer and Communications Security (CCS), Scottsdale, Arizona, USA, November 2014

Marc Kührer, Johannes Hoffmann, Thorsten Holz

CloudSylla: Detecting Suspicious System Calls in the Cloud

16th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS), Paderborn, Germany, September 2014

Felix Schuster, Thomas Tendyck, Jannik Pewny, Andreas Maaß, Martin Steegmanns, Moritz Contag, Thorsten Holz

Evaluating the Effectiveness of Current Anti-ROP Defenses

Research in Attacks, Intrusions and Defenses (RAID) Symposium, Gothenburg, Sweden, September 2014

Marc Kührer, Christian Rossow, Thorsten Holz

Paint it Black: Evaluating the Effectiveness of Malware Blacklists

Research in Attacks, Intrusions and Defenses (RAID) Symposium, Gothenburg, Sweden, September 2014

Jannik Pewny, Felix Schuster, Lukas Bernhard, Christian Rossow, Thorsten Holz

Leveraging Semantic Signatures for Bug Search in Binary Programs

Annual Computer Security Applications Conference (ACSAC), New Orleans, USA, Dezember 2014

Robert Gawlik, Thorsten Holz

Towards Automated Integrity Protection of C++ Virtual Function Tables in Binary Programs

Annual Computer Security Applications Conference (ACSAC), New Orleans, USA, Dezember 2014

Hendrik Meutzner, Viet Hung Nguyen, Thorsten Holz, Dorothea Kolossa

Using Automatic Speech Recognition for Attacking Acoustic CAPTCHAs: The Trade-off between Usability and Security

Annual Computer Security Applications Conference (ACSAC), New Orleans, USA, Dezember 2014

Apostolis Zarras, Alexandros Kapravelos, Gianluca Stringhini, Thorsten Holz, Christopher Kruegel, Giovanni Vigna

The Dark Alleys of Madison Avenue: Understanding Malicious Advertisements

2014 Internet Measurement Conference (IMC), Vancouver, Canada, November 2014

Johannes Dahse, Nikolai Krein, Thorsten Holz

Code Reuse Attacks in PHP: Automated POP Chain Generation

21st ACM Conference on Computer and Communications Security (CCS), Scottsdale, Arizona, USA, November 2014

Michael Backes, Thorsten Holz, Benjamin Kollenda, Philipp Koppe, Stefan Nürnberger, Jannik Pewny

You Can Run but You Can't Read: Preventing Disclosure Exploits in Executable Code

21st ACM Conference on Computer and Communications Security (CCS), Scottsdale, Arizona, USA, November 2014

Apostolis Zarras

The Art of False Alarms in the Game of Deception: Leveraging Fake Honeypots for Enhanced Security

48th IEEE International Carnahan Conference on Security Technology (ICCST), Rom, Italien, Oktober 2014

Marc Kührer, Johannes Hoffmann, Thorsten Holz

CloudSylla: Detecting Suspicious System Calls in the Cloud

16th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS), Paderborn, Germany, September 2014

Felix Schuster, Thomas Tendyck, Jannik Pewny, Andreas Maaß, Martin Steegmanns, Moritz Contag, Thorsten Holz

Evaluating the Effectiveness of Current Anti-ROP Defenses

Research in Attacks, Intrusions and Defenses (RAID) Symposium, Göteborg, Schweden, September 2014

Marc Kührer, Christian Rossow, Thorsten Holz

Paint it Black: Evaluating the Effectiveness of Malware Blacklists

Research in Attacks, Intrusions and Defenses (RAID) Symposium, Göteborg, Schweden, September 2014

Sebastian Uellenbeck, Thomas Hupperich, Christopher Wolf, Thorsten Holz

Tactile One-Time Pad. Smartphone Authentification. Resilient Against Shoulder Surfing

TR-HGI-2014-003, Ruhr-Universität Bochum, Horst Görtz Institut für IT-Sicherheit (HGI), September 2014

Johannes Dahse, Thorsten Holz

Static Detection of Second-Order Vulnerabilities in Web Applications

23rd USENIX Security Symposium, San Diego, CA, USA, August 2014

Sebastian Vogl, Robert Gawlik, Behrad Garmany, Thomas Kittel, Jonas Pfoh, Claudia Eckert, Thorsten Holz

Dynamic Hooks: Hiding Control Flow Changes within Non-Control Data

23rd USENIX Security Symposium, San Diego, CA, USA, August 2014

Marc Kührer, Thomas Hupperich, Christian Rossow, Thorsten Holz

Exit from Hell? Reducing the Impact of Amplification DDoS Attacks

23rd USENIX Security Symposium, San Diego, CA, USA, August 2014

Marc Kührer, Thomas Hupperich, Christian Rossow, Thorsten Holz

Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks

8th USENIX Workshop on Offensive Technologies (WOOT), San Diego, CA, USA, August 2014

Apostolis Zarras, Antonis Papadogiannakis, Robert Gawlik, Thorsten Holz

Automated Generation of Models for Fast and Precise Detection of HTTP-Based Malware

12th Annual Conference on Privacy, Security and Trust (PST), Toronto, Kanada, Juli 2014

Marc Kührer, Christian Rossow, Thorsten Holz

Technical Report: Paint it Black: Evaluating the Effectiveness of Malware Blacklists

TR-HGI-2014-002, Ruhr-Universität Bochum, Horst Görtz Institut für IT-Sicherheit (HGI), Juni 2014

Felix Schuster, Thomas Tendyck, Jannik Pewny, Andreas Maaß, Martin Steegmanns, Moritz Contag, Thorsten Holz

Technical Report: Evaluating the Effectiveness of Current Anti-ROP Defenses

TR-HGI-2014-001, Ruhr-Universität Bochum, Horst Görtz Institut für IT-Sicherheit (HGI), Mai 2014

Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, Jörg Schwenk

Scriptless attacks: Stealing more pie without touching the sill

Journal of Computer Security, Ausgabe 22, Nummer 4 / 2014, Web Application Security – Web @ 25

Karl-Heinz Krempels, Christoph Terwelp, Stefan Wüller, Tilman Frosch, Sevket Gökay

Communication Reduced Interaction Protocol between Customer, Charging Station, and Charging Station Management System

3rd International Conference on Smart Grids and Green IT Systems (SMARTGREENS 2014), Barcelona, Spanien, April 2014

Christopher Meyer, Juraj Somorovsky, Eugen Weiss, Jörg Schwenk, Sebastian Schinzel, Erik Tews

Revisiting SSL/TLS Implementations: New Bleichenbacher Side Channels and Attacks

USENIX Security 2014, San Diego, USA

Olivier Blazy, Eike Kiltz, Jiaxin Pan

(Hierarchical) Identity-Based Encryption from Affine Message Authentication

CRYPTO 2014: 408-425

Alexandre Pinto, Bertram Poettering, Jacob C. N. Schuldt

Multi-recipient encryption, revisited

ASIACCS 2014

Giorgia Azzurra Marson, Bertram Poettering

Even More Practical Secure Logging: Tree-Based Seekable Sequential Key Generators

ESORICS 2014

Bertram Poettering, Douglas Stebila

Double-Authentication-Preventing Signatures

ESORICS 2014

Gottfried Herold, Julia Hesse, Dennis Hofheinz, Carla Ràfols, Andy Rupp

Polynomial Spaces: A New Framework for Composite-to-Prime-Order Transformations

In: Proceedings of CRYPTO (1) 2014. Lecture Notes in Computer Science 8616. Springer, 2014, 261-279

Felix Heuer, Tibor Jager, Eike Kiltz,, Sven Schäge

On the Selective Opening Security of Practical Public-Key Encryption Schemes

PKC 2015, Maryland, USA, Mai 2015

Thorsten Kranz, Markus Dürmuth

On Password Guessing with GPUs and FPGAs

PASSWORDS 2014, Trondheim, Norway

Christoph Bader

Efficient Signatures with Tight Real World Security in the Random Oracle Model

CANS 2014, Heraklion, Griechenland

Christoph Bader, Dennis Hofheinz, Tibor Jager, Eike Kiltz, Yong Li

Tightly Secure Authenticated Key Exchange

TCC 2015, Warschau, Polen

Florian Bergsma, Tibor Jager, Jörg Schwenk

One-Round Key Exchange with Strong Security: An Efficient and Generic Construction in the Standard Model

PKC 2015

Tibor Jager

Verifiable Random Functions from Weaker Assumptions

TCC 2015

Carla Ràfols Salvador

Stretching Groth-Sahai: NIZK Proofs of Partial Satisfiability

TCC 2015

Felix Schuster, Manuel Costa, Cédric Fournet, Christos Gkantsidis, Marcus Peinado, Gloria Mainar-Ruiz, Mark Russinovich

VC3: Trustworthy Data Analytics in the Cloud

MSR-TR-2014-39, Microsoft Research, Dezember 2014

Robert Gawlik, Thorsten Holz

Technical Report: Towards Automated Integrity Protection of C++ Virtual Function Tables in Binary Programs

TR-HGI-2014-004, Ruhr-Universität Bochum, Horst Görtz Institut für IT-Sicherheit (HGI), Dezember 2014

Nils Fleischhacker, Tibor Jager, and Dominique Schröder

On Tight Security Proofs for Schnorr Signatures

Asiacrypt 2014

Claude Castelluccia, Mar¬kus Dürmuth and Fatma Imamoglu

Learning from Neuroscience to Improve Internet Security

ERCIM News 2014(99), 2014

Ashar Javed, David Bletgen, Florian Kohlar, Markus Dürmuth, Jörg Schwenk

Secure Fallback Authentication and the Trusted Friend Attack

Proceedings International Conference on Distributed Computing Systems Workshops (ICDCS Workshops), 2014

Daniel V. Bailey, Markus Dürmuth, Christof Paar

Statistics on Password Re-use and Adaptive Strength for Financial Accounts

Proceedings 9th International Conference on Security and Cryptography (SCN), 2014

Daniel V. Bailey, Markus Dürmuth, Christof Paar

Typing passwords with voice recognition --or-- How to authenticate to Google Glass

Adventures in Authentication: WAY Workshop, 2014

Eike Kiltz, Hoeteck Wee

Quasi-Adaptive NIZK for Linear Subspaces Revisited

IACR Eurocrypt 2015

Alexander May, Ilya Ozerov

On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes

IACR Eurocrypt 2015

Gregor Leander, Brice Minaud, Sondre Ronjom

A Generic Approach toInvariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro On Tight Security Proofs for Schnorr Signatures

IACR Eurocrypt 2015

Josep Balasch, Sebastian Faust, Benedikt Gierlichs

Towards Non-Linear Higher-Order Masking - Inner Product revisited

IACR Eurocrypt 2015

Alexandre Duc, Sebastian Faust, François-Xavier Standaert

Masking Security Proofs Concrete (Or How to Evaluate the Security of any Leaking Device)

IACR Eurocrypt 2015

Stefan Dziembowski, Sebastian Faust, Maciej Skórski

Noisy Leakage Revisited

IACR Eurocrypt 2015

Olivier Blazy, Saqib A. Kakvi, Eike Kiltz, Jiaxin Pan

Tightly-Secure Signatures from Chameleon Hash Functions

IACR PKC 2015

David Cash, Rafael Dowsley, Eike Kiltz

Digital Signatures from Strong RSA without Prime Generation

IACR PKC 2015

Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, Daniele Venturi

A Tamper and Leakage Resilient von Neumann Architecture

IACR PKC 2015

Ingo von Maurich, Tobias Oder, Tim Güneysu

Implementing QC-MDPC McEliece Encryption

ACM Transactions on Embedded Computing

Tim Güneysu, Vadim Lyubashevsky, Thomas Pöppelmann

Lattice-Based Signatures: Optimization and Implementation on Reconfigurable Hardware

IEEE Transactions on Computers.

Ingo von Maurich, Tim Güneysu

Towards Side-Channel Resistant Implementations of QC-MDPC McEliece Encryption on Con-

strained Devices

Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Kanada, Oktober 2014

Maik Ender, Gerd Düppmann, Alexander Wild, Thomas Pöppelmann, Tim Güneysu

A Hardware-Assisted Proof-of-Concept for Secure VoIP Clients on Untrusted Operating Systems

2014 International Conference on Reconfigurable Computing and FPGAs (ReCon-Fig 2014), Cancun, Mexiko, Dezember 2014

Dennis Hofheinz, Tibor Jager

Tightly Secure Signatures and Public-Key Encryption

Designs, Codes and Cryptography, 2015.

Florian Böhl, Dennis Hofheinz, Tibor Jager, Jessica Koch, Christoph Striecks

Confined Guessing: New Signatures From Standard Assumptions

Journal of Cryptology, 2015

Cong Chen, Thomas Eisenbarth, Ingo von Maurich, Rainer Steinwandt

Differential Power Analysis of a McEliece CryptoSystem

13th International Conference on Applied Cryptography and Network Security (ACNS), New York, USA, Juni 2015

Alexander May, Ilya Ozerov

On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes

In Advances in Cryptology (Eurocrypt 2015)

Johannes Dahse, Thorsten Holz

Experience Report: An Empirical Study of PHP Security Mechanism Usage

International Symposium on Software Testing and Analysis (ISSTA)

Felix Schuster, Thomas Tendyck, Christopher Liebchen, Lucas Davi, Ahmad-Reza Sadeghi, Thorsten Holz

Counterfeit Object-oriented Programming: On the Difficulty of Preventing Code Reuse Attacks in C++ Applications

36th IEEE Symposium on Security and Privacy (Oakland), San Jose, Mai 2015

Jannik Pewny, Behrad Garmany, Robert Gawlik, Christian Rossow, Thorsten Holz

Cross-Architecture Bug Search in Binary Executables

36th IEEE Symposium on Security and Privacy (Oakland), San Jose, Mai 2015

Felix Schuster, Manuel Costa, Cédric Fournet, Christos Gkantsidis, Marcus Peinado, Gloria Mainar-Ruiz, Mark Russinovich

VC3: Trustworthy Data Analytics in the Cloud using SGX

36th IEEE Symposium on Security and Privacy (Oakland), San Jose, Mai 2015

Pawel Swierczynski, Marc Fyrbiak, Philipp Koppe, Christof Paar

FPGA Trojans through Detecting and Weakening of Cryptographic Primitives

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Ausgabe PP 99, Februar 2015

Sebastian Uellenbeck, Thomas Hupperich, Christopher Wolf, Thorsten Holz

Tactile One-Time Pad: Leakage-Resilient Authentication for Smartphones

Financial Cryptography and Data Security

Pascal Sasdrich, Amir Moradi, Oliver Mischke, Tim Güneysu

Achieving Side-Channel Protection with Dynamic Logic Reconfiguration on Modern FPGAs

IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2015, McLean, VA, USA, Mai 2015

Alexander Wild, Amir Moradi, Tim Güneysu

Side-Channel Protection by Randomizing Look-Up Tables on Reconfigurable Hard-Ware Pitfalls of Memory Primitives

6th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2015, Berlin, April 2015

Pascal Sasdrich, Oliver Mischke, Amir Moradi, Tim Güneysu

Side-Channel Protection by Randomizing Look-Up Tables on Reconfigurable Hardware - Pitfalls of Memory Primitives

6th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2015, Berlin, April 2015

James Howe, Thomas Pöppelmann, Maire O'Neill, Elizabeth O'Sullivan, Tim Güneysu

Practical Lattice-based Digital Signature Schemes

ACM Transaction on Embedded Computing, 2015

Georg T. Becker, Alexander Wild, Tim Güneysu

Security Analysis of Index-based Syndrome Coding for Puf-based Key Generation

IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2015, McLean, VA, USA, Mai 2015

Dennis Kupser, Christian Mainka, Jörg Schwenk, Juraj Somorovsky

How to Break XML Encryption - Automatically

WOOT 2015 (Workshop on Offensive Technologies)

Tobias Schneider, Amir Moradi, Tim Güneysu

Arithmetic Addition over Boolean Masking - Towards First- and Second-Order Resistance in Hardware

ACNS 2015

Tobias Schneider, Amir Moradi

Leakage Assessment Methodology - a clear roadmap for side-channel evaluations
CHES 2015

Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, Krzysztof Pietrzak

Proofs of Space

CRYPTO 2015

Tilman Frosch, Sven Schäge, Martin Goll, Thorsten Holz

On Locational Privacy in the Absence of Anonymous Payments

in: Gutwirth, S., Leenes R., P. De Hert and Y. Poullet, Data protection on the Move. Dordrecht: Springer, 2015

Sebastian Brenza, Andre Pawlowski, Christina Pöpper

A Practical Investigation of Identity Theft Vulnerabilities in Eduroam

In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec), 2015

Frederic Schulz, Dennis Felsch, Jörg Schwenk

Sicherheitsanalyse der Private Cloud Interfaces von openQRM

DACH Security 2015

Marcus Niemietz, Jörg Schwenk

Owning Your Home Network: Router Security Revisited

Web 2.0 Security & Privacy 2015

Christian Brandl, Hans U. Simon

Complexity Analysis: Finite Transformation Monoids

International Conference on Developments in Language Theory (DLT 2015)

Hans U. Simon

An Almost Optimal PAC Algorithm

Conference on Learning Theory (COLT 2015)

Malte Darnstädt, Christoph Ries, Hans U. Simon

Hierarchical Design of Fast Minimum Disagreement Algorithms

International Conference on Algorithmic Learning Theory (ALT 2015)

Ziyuan Gao, Hans U. Simon, Sandra Zilles

On the Teaching Complexity of Linear Sets

International Conference on Algorithmic Learning Theory (ALT 2015)

Tibor Jager, Jörg Schwenk, Juraj Somorovsky

Small Subgroup Attacks on TLS-ECDH

ESORICS 15

Christian Zenger, Jan Zimmer, Mario Pietersz, Jan-Felix Posielek, Christof Paar

Exploiting the Physical Environment for Securing the Internet of Things

New Security Paradigms Workshop, NSPW 2015, Twente, The Niederlande, September 2015

Rene Guillaume, Fredrik Winzer, Christian Zenger, Christof Paar, Andreas Czylwik

Bringing PHY-based Key Generation into the Field: An Evaluation for Practical Scenarios

82nd Vehicular Technology Conference, VTC 2015, Boston, USA, September 2015

Christian Zenger, Jan Zimmer, Jan-Felix Posielek, Christof Paar

Online Entropy Estimation for Secure Information Reconciliation

Workshop on Wireless Communication Security at the Physical Layer, WiComSecPhy 2015, Coimbra, Portugal, Juli 2015

Christian Zenger, Jan Zimmer, Christof Paar

Security Analysis of Quantization Schemes for Channel-based Key Extraction

Workshop on Wireless Communication Security at the Physical Layer, WiComSecPhy 2015, Coimbra, Portugal, Juli 2015

David Cash, Eike Kiltz, Stefano Tessaro

Two-Round Man-in-the-Middle Security from LPN

13th IACR Theory of Cryptography Conference - TCC 2016-A

Andrej Bogdanov, Siyao Guo, Daniel Masny, Silas Richelson, Alon Rosen

On the Hardness of Learning with Rounding over Small Modulus

13th IACR Theory of Cryptography Conference - TCC 2016-A

Georg Fuchsbauer, Felix Heuer, Eike Kiltz, Krzysztof Pietrzak

Standard Security Does Imply Security Against Selective Opening for Markov Distributions

13th IACR Theory of Cryptography Conference - TCC 2016-A

Dennis Hofheinz, Tibor Jager

Verifiable Random Functions from Standard Assumptions

13th IACR Theory of Cryptography Conference - TCC 2016-A

Stefan Dziembowski , Sebastian Faust, Maciej Skorski

Optimal Amplification of Noisy Leakages

13th IACR Theory of Cryptography Conference - TCC 2016-A

Felix Heuer, Tibor Jager, Eike Kiltz, Sven Schäge

On the Selective Opening Security of Practical Public-Key Encryption Schemes

Public Key Cryptography – PKC 2015

Olivier Blazy, Saqib A. Kakvi, Eike Kiltz, Jiaxin Pan

Tightly-Secure Signatures from Chameleon Hash Functions

Public Key Cryptography – PKC 2015

David Cash, Rafael Dowsley, Eike Kiltz

Digital Signatures from Strong RSA without Prime Generation

Public Key Cryptography – PKC 2015

Mihir Bellare, Dennis Hofheinz, Eike Kiltz

Subtleties in the Definition of IND-CCA: When and How Should Challenge Decryption Be Disallowed?

Journal of Cryptology

Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, Jorge Villar

An Algebraic Framework for Diffie-Hellman Assumptions

Journal of Cryptology

Tibor Jager, Jörg Schwenk, Juraj Somorovsky

Practical Invalid Curve Attacks on TLS-ECDH

20th European Symposium on Research in Computer Security - ESORICS 2015

Mario Heiderich, Marcus Niemietz, Jörg Schwenk

Waiting for CSP — Securing Legacy Web Applications with JSAgents

20th European Symposium on Research in Computer Security – ESORICS 2015

Tibor Jager, Jörg Schwenk, Juraj Somorovsky

On the Security of TLS 1.3 and QUIC Against Weaknesses in PKCS#1 v1.5 Encryption

22nd ACM Conference on Computer and Communications Security - ACM CCS 2015

Eike Kiltz, Jiaxin Pan, Hoeteck Wee

Structure-Preserving Signatures from Standard Assumptions, Revisited

Proceedings of IACR CRYPTO 2015, (2) 275--295 LNCS 9216 (2015)

Christian Altmeier, Christian Mainka, Juraj Somorovsky, Jörg Schwenk

AdIDoS -- Adaptive and Intelligent Fully-Automatic Detection of Deni-

al-of-Service Weaknesses in Web Services

International Workshop on Quantitative Aspects of Security Assurance - QASA 2015

Marcus Niemietz, Juraj Somorovsky, Christian Mainka, Jörg Schwenk

Not so Smart: On Smart TV Apps

International Workshop on Secure Internet of Things - SIoT 2015

Andreas Schilling, Brigitte Werners

Optimal selection of IT security safeguards from an existing knowledge base

European Journal of Operational Research, Vol. 248, No. 1 (2016), S. 318-327. DOI: 10.1016/j.ejor.2015.06.048

Andreas Schilling, Brigitte Werners

Optimal Information Security Expenditures Considering Budget Constraints

PACIS 2015 Proceedings, Paper 251, 1-14

Andreas Schilling, Brigitte Werners

Optimizing Information Systems Security Design Based on Existing Security Knowledge

Persson, A. and Stirna, J. (eds.): Advanced Information Systems Engineering Workshops, CAiSE 2015, Stockholm, Schweden, Proceedings Lecture Notes in Business Information Processing, Ausgabe 215, 447-458

Dennis Felsch, Mario Heiderich, Frederic Schulz, Jörg Schwenk

How Private is Your Private Cloud?: Security Analysis of Cloud Control Interfaces

ACM CCSW 2015 in conjunction with the ACM Conference on Computer and Communications Security - CCS

Stephen Crane, Stijn Volckaert, Felix Schuster, Christopher Liebchen, Per Larsen, Lucas Davi, Ahmad-Reza Sadeghi, Thorsten Holz, Bjorn De Sutter, Michael Franz

It's a TRAP: Table Randomization and Protection against Function Reuse Attacks

22nd ACM Conference on Computer and Communications Security - CCS 2015

Thomas Hupperich, Davide Maiorca, Marc Kührer, Thorsten Holz, Giorgio Giacinto

On the Robustness of Mobile Device Fingerprinting

31th Annual Computer Security Applications Conference - ACSAC 2015

Christian Röpke, Thorsten Holz

SDN Rootkits: Subverting Network Operating Systems of Software-Defined Networks

International Symposium on Research in Attacks, Intrusions and Defenses - RAID 2015

Marc Kührer, Thomas Hupperich, Jonas Bushart, Christian Rossow, Thorsten Holz

Going Wild: Large-Scale Classification of Open DNS Resolvers

15th ACM Internet Measurement Conference - IMC 2015

Bernd Jäger, Christian Röpke, Iris Adam, Thorsten Holz

Multi-Layer Access Control for SDN-based Telco Clouds

Nordic Conference on Secure IT System - NordSec2015

Tilman Frosch, Sven Schäge, Martin Goll, Thorsten Holz

On Locational Privacy in the Absence of Anonymous Payments

Gutwirth, S., Leenes R., P. De Hert and Y. Poullet, Data protection on the Move. Current Developments in ICT and Privacy/Data Protection. Springer, Dordrecht

Eike Kiltz, Hoeteck Wee

Quasi-Adaptive NIZK for Linear Subspaces Revisited

34th Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 2015

Alonso González, Alejandro Hevia, Carla Ràfols

QA-NIZK Arguments in Asymmetric Groups: New Tools and New Constructions

21st Annual International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2015

Felix Günther, Bertram Poettering

Linkable Message Tagging: Solving the Key Distribution Problem of Signature Schemes

20th Australasian Conference on Information Security and Privacy - ACISP 2015

Bertram Poettering, Dale Sibborn

Cold Boot Attacks in the Discrete Logarithm Setting

RSA Conference Cryptographers' Track - CT-RSA 2015

Jean Paul Degabriele, Pooya Farshim, Bertram Poettering

A More Cautious Approach to Security Against Mass Surveillance

22nd Workshop on Functional Software Encryption - FSE 2015

Francesco Aldà, Riccardo Aragona, Lorenzo Nicolodi, Massimiliano Sala

Implementation and Improvement of the Partial Sum Attack on 6-Round AES

In Physical and Data-Link Security Techniques for Future Communication Systems, Ausgabe 358 of Lecture Notes in Electrical Engineering, 181-195, Springer, 2015

Dario Weißer, Johannes Dahse, Thorsten Holz

Security Analysis of PHP Bytecode Protection Mechanisms

Research in Attacks, Intrusions and Defenses (RAID) Symposium, Kyoto, Japan, November 2015

Andreas Schilling

Robust optimization of IT security safeguards using standard security data

Accepted for publication in: Operations Research Proceedings 2015

Maximilian Golla, Markus Dürmuth

Analyzing 4 Million Real-World Personal Knowledge Questions

The International Conference on Passwords (Passwords^15), Cambridge, UK, Dezember 2015

Christian Kison, Jürgen Frinken, Christof Paar

Finding the AES Bits in the Haystack: Reverse Enginering and SCA Using Voltage Contrast

Workshop on Cryptographic Hardware and Embedded Systems, CHES 2015, Saint-Malo, Frankreich, September 2015

Falk Schellenberg, Markus Finkeldey, Bastian Richter, Maximilian Schäpers, Nils C. Gerhardt, Martin R. Hofmann , Christof Paar

On the Complexity Reduction of Laser Fault Injection Campaigns using OBIC Measurements

Fault Diagnosis and Tolerance in Cryptography - FDTC 2015, Saint Malo, Frankreich, September 2015

Christian Zenger, Jan Zimmer, Christof Paar

Security Analysis of Quantization Schemes for Channel-based Key Extraction

EAI Endorsed Transactions on Security and Safety, Ausgabe 15, Nr.. 6

Shweta Malik, Georg T. Becker, Christof Paar, Wayne P. Burleson

Development of a Layout-Level Hardware Obfuscation Tool

IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2015 (Invited Paper), Montpellier, Frankreich, Juli 2015

Gesine Hinterwälder, Felix Riek, Christof Paar

Efficient E-cash with Attributes on MULTOS Smartcards

11th Workshop on RFID Security - RFIDsec 2015

Andreas Gornik, Amir Moradi, Jürgen Oehm, Christof Paar

A Hardware-based Countermeasure to Reduce Side-Channel Leakage - Design, Implementation, and Evaluation

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Daehyun Strobel, Florian Bache, David Oswald, Falk Schellenberg, Christof Paar

SCANDALee: A Side-ChANnel-based DisAssembLer using Local Electromagnetic Emanations

Design, Automation & Test in Europe Conference & Exhibition, DATE 2015, Grenoble, Frankreich, März 2015

Michael Düll, Björn Haase, Gesine Hinterwälder, Michael Hutter, Christof Paar, Ana Helena Sánchez, Peter Schwabe

High-speed Curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers

Designs, Codes and Cryptography comprising the "Special Issue on Cryptography, Codes, Designs and Finite Fields: In Memory of Scott A. Vanstone", Springer

Andy Rupp, Foteini Baldimtsi, Gesine Hinterwälder, Christof Paar

Cryptographic Theory Meets Practice: Efficient and Privacy-Preserving Payments for Public Transport

ACM Transactions on Information and System Security (TISSEC), Band 17 Ausgabe 3, März 2015, Artikel Nr. 10

Pawel Swierczynski, Marc Fyrbiak, Christof Paar, Christophe Huriaux, Russell Tessier

Protecting against Cryptographic Trojans in FPGAs

In the Proceedings of the IEEE Symposium on Field-Programmable Custom Computing Machines, Vancouver, British Columbia, Mai 2015

Pawel Swierczynski, Amir Moradi, David Oswald, Christof Paar

Physical Security Evaluation of the Bitstream Encryption Mechanism of Altera Stratix II and Stratix III FPGAs

ACM Transactions on Reconfigurable Technology and Systems (TRETS), Band 7 Ausgabe 4, Dezember 2014

Ariano-Tim Donda, Peter Samarin, Jacek Samotyja, Kerstin Lemke-Rust, Christof Paar

Remote IP Protection using Timing Channels

The 17th Annual International Conference on Information Security and Cryptology -- ICISC Seoul, Korea, Dezember 2014

Stefan Heyse, Ralf Zimmermann, Christof Paar

Attacking Code-Based Cryptosystems with Information Set Decoding Using Special-Purpose Hardware

Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Kanada, Oktober 2014

Gesine Hinterwälder, Amir Moradi, Michael Hutter, Peter Schwabe, Christof Paar

Full-Size High-Security ECC Implementation on MSP430 Microcontrollers

Third International Conference on Cryptology and Information Security in Latin America, Latincrypt 2014, Florianópolis, Brasilien, September 2014

Christian Zenger, Jürgen Förster, Christof Paar

POSTER: Implementation and Evaluation of Channel-based Key Establishment Systems

Workshop on Cryptographic Hardware and Embedded Systems, CHES 2014, Busan, Korea, September 2014

Daehyun Strobel, David Oswald, Bastian Richter, Falk Schellenberg, Christof Paar

Microcontrollers as (In)Security Devices for Pervasive Computing Applications

Proceedings of the IEEE, Band 102, Nummer 8, 1157-1173, 2014

Timo Kasper, David Oswald, Christof Paar

Sweet Dreams and Nightmares: Security in the Internet of Things

Information Security Theory and

Practice. Securing the Internet of Things - 8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Kreta, Griechenland, Juni 2014

Susanne Wetzel, Bernhard Borsch, Christof Paar, Thomas Pöppelmann

Proof-of-Concept: Using Homomorphic Cryptography to Provide for Privacy in Modern Vehicular Environments

escar Embedded Security in Cars Conference, Detroid Metropolitan, Michigan, USA, Juni 2014

Georg T. Becker, Francesco Regazzoni, Christof Paar, Wayne P. Burleson

Stealthy dopant-level hardware Trojans

Journal of Cryptographic Engineering 4.1 (2014): 19-31

Amir Moradi, Alexander Wild

Assessment of Hiding the Higher-Order Leakages in Hardware - what are the achievements versus overheads?

Workshop on Cryptographic Hardware and Embedded Systems, CHES 2015, Saint-Malo, Frankreich, September 2015

Pascal Sasdrich, Amir Moradi, Tim Güneysu

Affine Equivalence and its Application to Tightening Threshold Implementations

22nd International Conference on Selected Areas in Cryptography, SAC 2015, Mount Allison University Sackville, New Brunswick, Kanada, August 2015

Andreas Gornik, Amir Moradi, Jürgen Oehm, Christof Paar

A Hardware-based Countermeasure to Reduce Side-Channel Leakage - Design, Implementation, and Evaluation

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Alexander Wild, Amir Moradi, Tim Güneysu

Evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs

6th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2015, Berlin, April 2015

Amir Moradi, Gesine Hinterwälder

Side-Channel Security Analysis of Ultra-Low-Power FRAM-based MCUs

6th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2015, Berlin, April 2015

Best Paper Award

Santos Merino Del Pozo, François-Xavier Standaert, Dina Kamel, Amir Moradi

Side-Channel Attacks from Static Power: When Should we Care?

Design, Automation & Test in Europe Conference & Exhibition, DATE 2015, Grenoble, Frankreich, März 2015

Amir Moradi

Wire-Tap Codes as Side-Channel Countermeasure - an FPGA-based experiment

15th International Conference on Cryptology in India, Indocrypt 2014, Neu Delhi, Indien, Dezember 2014

Pawel Swierczynski, Amir Moradi, David Oswald, Christof Paar

Physical Security Evaluation of the Bitstream Encryption Mechanism of Altera Stratix II and Stratix III FPGAs

ACM Transactions on Reconfigurable Technology and Systems (TRETS), Band 7 Ausgabe 4, Dezember 2014

Gesine Hinterwälder, Amir Moradi, Michael Hutter, Peter Schwabe, Christof Paar

Full-Size High-Security ECC Implementation on MSP430 Microcontrollers

Third International Conference on Cryptology and Information Security in Latin America, Latincrypt 2014, Florianópolis, Brasilien, September 2014

Amir Moradi, Vincent Immler

Early Propagation and Imbalanced Routing, How to Diminish in FPGAs

Workshop on Cryptographic Hardware and Embedded Systems, CHES 2014, Busan, Korea, September 2014

Amir Moradi

Side-Channel Leakage through Static Power – Should We Care about in Practice?

Workshop on Cryptographic Hardware and Embedded Systems, CHES 2014, Busan, Korea, September 2014

Oliver Mischke, Amir Moradi, Tim Güneysu

Fault Sensitivity Analysis Meets Zero-Value Attack

Fault Diagnosis and Tolerance in Cryptography - FDTC 2014, Busan, Korea, September 2013

Amir Moradi, Sylvain Guilley, Annelie Heuser

Detecting Hidden Leakages

International Conference on Applied Cryptography and Network Security - ACNS 2014, Lausanne, Schweiz, Juni 2014

Best Student Paper Award

Alexander Wild, Tim Güneysu

Enabling SRAM-PUFs on Xilinx FPGAs

24th International Conference on Field Programmable Logic and Applications Munich, Germany; September 2014

Thomas Pöppelmann, Tobias Oder, Tim Güneysu

High-Performance Ideal Lattice-Based Cryptography on ATxmega 8-bit Microcontrollers

Latincrypt 2015, Bienvenido, Guadalajara, Mexiko, August 2015

Gunnar Alendal, Christian Kison

got HW crypto? On the (in)security of a Self-Encrypting Drive series

modg - Hardware Security Con-

ference and Training, Hardwear.io 2015, Den Haag, Niederlande, Oktober 2015

Georg T. Becker

The Gap Between Promise and Reality: On the Insecurity of XOR Arbiter PUFs

Workshop on Cryptographic Hardware and Embedded Systems, CHES 2015, Saint-Malo, Frankreich, September 2015

Shweta Malik, Georg T. Becker, Christof Paar, Wayne P. Burleson

Development of a Layout-Level Hardware Obfuscation Tool

IEEE Computer Society Annual Symposium on VLSI, ISVLSI 2015 (Invited Paper), Montpellier, Frankreich, Juli 2015

Johannes Tobisch, Georg T. Becker

On the Scaling of Machine Learning Attacks on PUFs with Application to Noise Bifurcation

11th Workshop on RFID Security (RFIDSec 2015), New York, USA, Juni 2015

Georg T. Becker

On the Pitfalls of using Arbiter-PUFs as Building Blocks

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems TCAD, 34 (8):1-13, August 2015

Georg T. Becker, Francesco Regazzoni, Christof Paar, Wayne P. Burleson

Stealthy dopant-level hardware Trojans

Journal of Cryptographic Engineering 4.1 (2014): 19-31

Yong Li, Sven Schäge, Zheng Yang, Christoph Bader, Jörg Schwenk

New Modular Compilers for Authenticated Key Exchange

ACNS 2014: 1-18

Christian Mainka, Vladislav Mlad-

enov, Florian Feldmann, Julian Krautwald, Jörg Schwenk

Your Software at my Service: Security Analysis of SaaS Single Sign-On Solutions in the Cloud

CCSW 2014: 93-104

Andreas Mayer, Marcus Niemietz, Vladislav Mladenov, Jörg Schwenk

Guardians of the Clouds: When Identity Providers Fail

CCSW 2014: 105-116

Florian Bergsma, Benjamin Dowling, Florian Kohlar, Jörg Schwenk, Douglas Stebila

Multi-Ciphersuite Security of the Secure Shell (SSH) Protocol

ACM Conference on Computer and Communications Security 2014: 369-381

Jörg Schwenk

Modelling Time for Authenticated Key Exchange Protocols

ESORICS (2) 2014: 277-294

Ashar Javed, Jens Riemer, Jörg Schwenk

SIACHEN: A Fine-Grained Policy Language for the Mitigation of Cross-Site Scripting Attacks

ISC 2014: 515-528

Andreas Mayer, Vladislav Mladenov, Jörg Schwenk, Florian Feldmann, Christopher Meyer

Strengthening Web Authentication through TLS - Beyond TLS Client Certificates

Open Identity Summit 2014: 97-108

Yong Li, Sven Schäge, Zheng Yang, Florian Kohlar, Jörg Schwenk

On the Security of the Pre-shared Key Ciphersuites of TLS

PublicKey Cryptography 2014: 669-684

Andreas Mayer, Vladislav Mladenov,

Jörg Schwenk

On the Security of Holder-of-Key Single Sign-On

Sicherheit 2014: 65-77

Ashar Javed, Christian Merz, Jörg Schwenk

TTPCookie: Flexible Third-Party Cookie Management for Increasing Online Privacy

TrustCom 2014: 37-44

Ashar Javed, Jörg Schwenk

Systematically Breaking Online WYSIWYG Editors

WISA 2014: 122-133

Christian Mainka, Vladislav Mladenov, Jörg Schwenk

Do not trust me: Using malicious IdPs for analyzing and attacking Single Sign-On

CoRR abs/1412.1623 (2014)

Tilman Frosch, Christian Mainka, Christoph Bader, Florian Bergsma, Jörg Schwenk, Thorsten Holz

How Secure is TextSecure?

IACR Cryptology ePrint Archive 2014: 904 (2014)

Abeer Elsafie, Jörg Schwenk

Semi-automated Fuzzy MCDM and Lattice Solutions for WSPolicy Intersection SERVICES 2015: 167-174

Vladislav Mladenov, Christian Mainka, Julian Krautwald, Florian Feldmann, Jörg Schwenk

On the security of modern Single Sign-On Protocols: OpenID

Connect 1.0.

CoRR abs/1508.04324 (2015)

Britta Hale, Tibor Jager, Sebastian Lauer, Jörg Schwenk

Speeding: On Low-Latency Key Exchange

IACR Cryptology ePrint Archive 2015: 1214 (2015)

Redaktion: Dr. Dominik Baumgarten
Layout: Jana Runde
Lektorat: Dipl.-Kffr. Inga Knapp

Druck: 500

ViSdP: Prof. Dr. Thorsten Holz,
Prof. Dr. Christof Paar

Kontakt

Ruhr-Universität Bochum

Horst Görtz Institut für
IT-Sicherheit

Gebäude ID 2/150
Universitätsstrasse 150
44780 Bochum

Telefon: +49 (0) 234 - 32 29287
Fax: +49 (0) 234 - 32 14886
Email: hgi-office@rub.de

www.hgi.rub.de

Redaktionsschluss: Juni 2016