# IEEE S&P 2018 Accepted Papers

**Label IMPORTANT 重要**

**Source:** [**https://www.ieee-security.org/TC/SP2018/program-papers.html**](https://www.ieee-security.org/TC/SP2018/program-papers.html)

**\*\*\*\*\***

A Formal Treatment of Accountable Proxying over TLS   
Karthikeyan Bhargavan (INRIA de Paris, France), Ioana Boureanu (Univ. of Surrey, SCCS, UK), Antoine Delignat-Lavaud (Microsoft Research, UK), Pierre-Alain Fouque (Univ. of Rennes 1, IRISA, France), Cristina Onete (Univ. of Limoges, XLIM, CNRS, France)

Much of Internet traffic nowadays passes through active proxies, whose role is to inspect, filter, cache, or transform data exchanged between two endpoints. To perform their tasks, such proxies modify channel-securing protocols, like TLS, **resulting in serious vulnerabilities**. Such problems are exacerbated by the fact that middleboxes are often invisible to one or both endpoints, leading to **a lack of accountability**. A recent protocol, called mcTLS, pioneered accountability for proxies, which are authorized by the endpoints and **given limited read/write permissions** to application traffic.  
  
Unfortunately, we show that **mcTLS is insecure**: the protocol modifies the TLS protocol, exposing it to a new class of **middlebox-confusion attacks**. Such attacks went unnoticed mainly because mcTLS lacked a formal analysis and security proofs. Hence, our second contribution is to formalize the goal of accountable proxying over secure channels. Third, we propose a **provably-secure alternative** to soon-to-be-standardized mcTLS: a generic and modular protocol-design that care- fully composes generic secure channel-establishment protocols, which we prove secure. Finally, we present a proof-of-concept implementation of our design, **instantiated with unmodified TLS 1.3**, and evaluate its overheads.

**\*\*\*\*\***

**IMPORTANT**

A Machine Learning Approach To Prevent Malicious Calls Over Telephony Networks   
Huichen Li (Shanghai Jiao Tong University), Xiaojun Xu (Shanghai Jiao Tong University), Chang Liu (University of California, Berkeley), Teng Ren (TouchPal Inc.), Kun Wu (TouchPal Inc.), Xuezhi Cao (Shanghai Jiao Tong University), Weinan Zhang (Shanghai Jiao Tong University), Yong Yu (Shanghai Jiao Tong University), Dawn Song (University of California, Berkeley)

Malicious calls, i.e., telephony spams and scams, have been a long-standing challenging issue that **causes billions of dollars of annual financial loss worldwide**. This work presents the first machine learning-based solution **without relying on any particular assumptions on the underlying telephony network infrastructures**.  
  
The main challenge of this decade-long problem is that it is unclear **how to construct effective features** without the access to the telephony networks' infrastructures. We solve this problem by combining several innovations. We first develop a **TouchPal** user interface on top of a mobile App to allow users tagging malicious calls. This allows us to maintain **a large-scale call log database**. We then conduct a measurement study over three months of call logs, including **9 billion records**. We **design 29 features** based on the results, so that **machine learning algorithms can be used to predict malicious calls**. We extensively evaluate different state-of-the-art machine learning approaches using the **proposed features**, and the results show that the best approach can **reduce up to 90% unblocked malicious calls while maintaining a precision over 99.99% on the benign call traffic.** The results also show the models are **efficient to implement without incurring a significant latency overhead**. We also conduct **ablation analysis**, which reveals that **using 10 out of the 29 features** can reach a performance comparable to using all features.

\*\*\*\*\*

A Tale of Two Studies: The Best and Worst of YubiKey Usability   
Joshua Reynolds (University of Illinois at Urbana-Champaign), Trevor Smith (Brigham Young University), Ken Reese (Brigham Young University), Luke Dickinson (Brigham Young University), Scott Ruoti (MIT Lincoln Laboratory), Kent Seamons (Brigham Young University)

Two-factor authentication (2FA) significantly improves the security of password-based authentication. Recently, there has been increased interest in Universal 2nd Factor (U2F) security keys-small hardware devices that require users to press a button on the security key to authenticate. To examine the usability of security keys in non-enterprise usage, we conducted two user studies of the YubiKey, a popular line of U2F security keys. The first study tasked 31 participants with configuring a Windows, Google, and Facebook account to authenticate using a YubiKey. This study revealed problems with setup instructions and workflow including users locking themselves out of their operating system or thinking they had successfully enabled 2FA when they had not. In contrast, the second study had 25 participants use a YubiKey in their daily lives over a period of four weeks, revealing that participants generally enjoyed the experience. Conducting both a laboratory and longitudinal study yielded insights into the usability of security keys that would not have been evident from either study in isolation. Based on our analysis, we recommend standardizing the setup process, enabling verification of success, allowing shared accounts, integrating with operating systems, and preventing lockouts.

\*\*\*\*\*

**IMPORTANT**

AI2: Safety and Robustness Certification of Neural Networks with Abstract Interpretation   
Timon Gehr (ETH Zürich), Matthew Mirman (ETH Zürich), Dana Drachsler Cohen (ETH Zürich), Petar Tsankov (ETH Zürich), Swarat Chaudhuri (Rice University), Martin Vechev (ETH Zürich)

We present AI2, the first sound and scalable analyzer for deep neural networks. Based on overapproximation, AI2 can automatically prove safety properties (e.g., robustness) of realistic neural networks (e.g., convolutional neural networks).

The key insight behind AI2 is to phrase reasoning about safety and robustness of neural networks in terms of classic abstract interpretation, enabling us to leverage decades of advances in that area. Concretely, we introduce abstract transformers that capture the behavior of fully connected and convolutional neural network layers with rectified linear unit activations (ReLU), as well as max pooling layers. This allows us to handle real-world neural networks, which are often built out of those types of layers.

We present a complete implementation of AI2 together with an extensive evaluation on 20 neural networks. Our results demonstrate that: (i) AI2 is precise enough to prove useful specifications (e.g., robustness), (ii) AI2 can be used to certify the effectiveness of state-of-the-art defenses for neural networks, (iii) AI2 is significantly faster than existing analyzers based on symbolic analysis, which often take hours to verify simple fully connected networks, and (iv) AI2 can handle deep convolutional networks, which are beyond the reach of existing methods.

\*\*\*\*\*

## Angora: Efficient Fuzzing by Principled Search Peng Chen (ShanghaiTech University), Hao Chen (University of California, Davis)

Abstract-Fuzzing is a popular technique for finding software bugs. However, the performance of the state-of-the-art fuzzers leaves a lot to be desired. Fuzzers based on symbolic execution produce quality inputs but run slow, while fuzzers based on random mutation run fast but have difficulty producing quality inputs. We propose Angora, a new mutation-based fuzzer that outperforms the state-of-the-art fuzzers by a wide margin. The main goal of Angora is to increase branch coverage by solving path constraints without symbolic execution. To solve path constraints efficiently, we introduce several key techniques: scalable byte-level taint tracking, context-sensitive branch count, search based on gradient descent, and input length exploration. On the LAVA-M data set, Angora found almost all the injected bugs, found more bugs than any other fuzzer that we compared with, and found eight times as many bugs as the second-best fuzzer in the program who. Angora also found 103 bugs that the LAVA authors injected but could not trigger. We also tested Angora on eight popular, mature open source programs. Angora found 6, 52, 29, 40 and 48 new bugs in file, jhead, nm, objdump and size, respectively. We measured the coverage of Angora and evaluated how its key techniques contribute to its impressive performance.

\*\*\*\*\*

Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency --- Choose Two   
Debajyoti Das (Purdue University), Sebastian Meiser (University College London), Esfandiar Mohammadi (ETH Zurich), Aniket Kate (Purdue University)

This work investigates the **fundamental constraints of anonymous communication (AC) protocols**. We analyze the relationship between bandwidth overhead, latency overhead, and sender anonymity or recipient anonymity against the global passive (network-level) adversary. We confirm the trilemma that an AC protocol can only achieve two out of the following three properties: strong anonymity (i.e., anonymity up to a negligible chance), low bandwidth overhead, and low latency overhead.   
  
We further study anonymity against a stronger global passive adversary that can additionally passively compromise some of the AC protocol nodes. For a given number of compromised nodes, we derive necessary constraints between bandwidth and latency overhead whose violation make it impossible for an AC protocol to achieve strong anonymity. We analyze prominent AC protocols from the literature and depict to which extent those satisfy our necessary constraints. Our fundamental necessary constraints offer a guideline not only for improving existing AC systems but also for designing novel AC protocols with non-traditional bandwidth and latency overhead choices.

\*\*\*\*\*

Another Flip in the Wall of Rowhammer Defenses   
Daniel Gruss (Graz University of Technology, Graz, Austria), Moritz Lipp (Graz University of Technology, Graz, Austria), Michael Schwarz (Graz University of Technology, Graz, Austria), Daniel Genkin (University of Pennsylvania and University of Maryland, USA), Jonas Juffinger (Graz University of Technology, Graz, Austria), Sioli O'Connell (University of Adelaide, Adelaide, Australia), Wolfgang Schoechl (Graz University of Technology, Graz, Austria), Yuval Yarom (University of Adelaide and Data61, Adelaide, Australia)

The Rowhammer bug allows unauthorized modification of bits in DRAM cells from unprivileged software, enabling powerful privilege-escalation attacks. Sophisticated Rowhammer countermeasures have been presented, aiming at mitigating the Rowhammer bug or its exploitation. However, the state of the art provides insufficient insight on the completeness of these defenses. In this paper, we present novel Rowhammer attack and exploitation primitives, showing that even a combination of all defenses is ineffective. Our new attack technique, one-location hammering, breaks previous assumptions on requirements for triggering the Rowhammer bug, i.e., we do not hammer multiple DRAM rows but only keep one DRAM row constantly open. Our new exploitation technique, opcode flipping, bypasses recent isolation mechanisms by flipping bits in a predictable and targeted way in userspace binaries. We replace conspicuous and memory-exhausting spraying and grooming techniques with a novel reliable technique called memory waylaying. Memory waylaying exploits system-level optimizations and a side channel to coax the operating system into placing target pages at attacker-chosen physical locations. Finally, we abuse Intel SGX to hide the attack entirely from the user and the operating system, making any inspection or detection of the attack infeasible. Our Rowhammer enclave can be used for coordinated denial-of-service attacks in the cloud and for privilege escalation on personal computers. We demonstrate that our attacks evade all previously proposed countermeasures for commodity systems.

\*\*\*\*\*

Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems   
Connor Bolton (University of Michigan), Sara Rampazzi (University of Michigan), Chaohao Li (Zhejiang University), Andrew Kwong (University of Michigan), Wenyuan Xu (Zhejiang University), Kevin Fu (University of Michigan)

Intentional acoustic interference causes unusual errors in the mechanics of magnetic hard disk drives in desktop and laptop computers, leading to damage to integrity and availability in both hardware and software such as file system corruption and operating system reboots. An adversary without any special purpose equipment can co-opt built-in speakers or nearby emitters to cause persistent errors. Our work traces the deeper causality of these risks from the physics of materials to the I/O request stack in operating systems for audible and ultrasonic sound. Our experiments show that audible sound causes the head stack assembly to vibrate outside of operational bounds; ultrasonic sound causes false positives in the shock sensor, which is designed to prevent a head crash.  
  
The problem poses a challenge for legacy magnetic disks that remain stubbornly common in safety critical applications such as medical devices and other highly utilized systems difficult to sunset. Thus, we created and modeled a new feedback controller that could be deployed as a firmware update to attenuate the intentional acoustic interference. Our sensor fusion method prevents unnecessary head parking by detecting ultrasonic triggering of the shock sensor.

\*\*\*\*\*

Bulletproofs: Short Proofs for Confidential Transactions and More   
Benedikt Bünz (Stanford University), Jonathan Bootle (University College London), Dan Boneh (Stanford University), Andrew Poelstra (Blockstream), Pieter Wuille (Blockstream), Greg Maxwell

We propose Bulletproofs, **a new non-interactive zero-knowledge proof protocol with very short proofs and without a trusted setup**; the proof size is only logarithmic in the witness size. Bulletproofs are especially well suited for efficient range proofs on committed values: they enable proving that a committed value is in a range using only 2 log\_2(n)+9 group and field elements, where n is the bit length of the range. Proof generation and verification times are linear in n.  
  
Bulletproofs greatly improve on the linear (in n) sized range proofs in existing proposals for confidential transactions in Bitcoin and other cryptocurrencies. Moreover, Bulletproofs supports aggregation of range proofs, so that a party can prove that m commitments lie in a given range by providing only an additive O(log(m)) group elements over the length of a single proof. To aggregate proofs from multiple parties, we enable the parties to generate a single proof without revealing their inputs to each other via a simple multi-party computation (MPC) protocol for constructing Bulletproofs. This MPC protocol uses either a constant number of rounds and linear communication, or a logarithmic number of rounds and logarithmic communication. We show that verification time, while asymptotically linear, is very efficient in practice. The marginal cost of batch verifying 32 aggregated range proofs is less than the cost of verifying 32 ECDSA signatures. Bulletproofs build on the techniques of Bootle et al. (EUROCRYPT 2016). Beyond range proofs, Bulletproofs provide short zero-knowledge proofs for general arithmetic circuits while only relying on the discrete logarithm assumption and without requiring a trusted setup. We discuss many applications that would benefit from Bulletproofs, primarily in the area of cryptocurrencies. The efficiency of Bulletproofs is particularly well suited for the distributed and trustless nature of blockchains. The full version of this article is available on ePrint.

\*\*\*\*\*

CollAFL: Path Sensitive Fuzzing  
Shuitao Gan (State Key Laboratory of Mathematical Engineering and Advanced Computing), Chao Zhang (Tsinghua University), Xiaojun Qin (State Key Laboratory of Mathematical Engineering and Advanced Computing), Xuwen Tu (State Key Laboratory of Mathematical Engineering and Advanced Computing), Kang Li (Cyber Immunity Lab), Zhongyu Pei (Tsinghua University), Zuoning Chen (National Research Center of Parallel Computer Engineering and Technology)

**Coverage-guided fuzzing is a widely used and effective solution to find software vulnerabilities**. Tracking code coverage and utilizing it to guide fuzzing are crucial to coverage- guided fuzzers. However, tracking full and accurate path coverage is infeasible in practice due to the high instrumentation overhead. Popular fuzzers (e.g., AFL) often use coarse coverage information, e.g., edge hit counts stored in a compact bitmap, to achieve highly efficient greybox testing. Such inaccuracy and incompleteness in coverage introduce serious limitations to fuzzers. First, it causes path collisions, which prevent fuzzers from discovering potential paths that lead to new crashes. More importantly, it prevents fuzzers from making wise decisions on fuzzing strategies.  
In this paper, we propose a coverage sensitive fuzzing solution CollAFL. It mitigates path collisions by providing more accurate coverage information, while still preserving low instrumentation overhead. It also utilizes the coverage information to apply three new fuzzing strategies, promoting the speed of discovering new paths and vulnerabilities. We emented a prototype of CollAFL based on the popular fuzzer AFL and evaluated it on 24 popular applications. The results showed that path collisions are common, i.e., up to 75% of edges could collide with others in some applications, and CollAFL could reduce the edge collision ratio to nearly zero. Moreover, armed with the three fuzzing strategies, CollAFL outperforms AFL in terms of both code coverage and vulnerability discovery. On average, CollAFL covered 20% more program paths, found 320% more unique crashes and 260% more bugs than AFL in 200 hours. In total, CollAFL found 157 new security bugs with 95 new CVEs assigned.

\*\*\*\*\*

Compiler-assisted Code Randomization   
Hyungjoon Koo (Stony Brook University), Yaohui Chen (Northeastern University), Long Lu (Northeastern University), Vasileios P. Kemerlis (Brown University), Michalis Polychronakis (Stony Brook University)

**Despite decades of research on software diversification, only address space layout randomization has seen widespread adoption. Code randomization, an effective defense against return-oriented programming exploits**, has remained an academic exercise mainly due to i) the lack of a transparent and streamlined deployment model that does not disrupt existing software distribution norms, and ii) the inherent incompatibility of program variants with error reporting, whitelisting, patching, and other operations that rely on code uniformity. In this work we present compiler-assisted code randomization (CCR), a hybrid approach that relies on compiler-rewriter cooperation to enable fast and robust fine-grained code randomization on end-user systems, while maintaining compatibility with existing software distribution models. The main concept behind CCR is to augment binaries with a minimal set of transformation- assisting metadata, which i) facilitate rapid fine-grained code transformation at installation or load time, and ii) form the basis for reversing any applied code transformation when needed, to maintain compatibility with existing mechanisms that rely on referencing the original code. We have implemented a prototype of this approach by extending the LLVM compiler toolchain, and developing a simple binary rewriter that leverages the embedded metadata to generate randomized variants using basic block reordering. The results of our experimental evaluation demonstrate the feasibility and practicality of CCR, as on average it incurs a modest file size increase of 11.46% and a negligible runtime overhead of 0.28%, while it is compatible with link-time optimization and control flow integrity.

\*\*\*\*\*

Computer Security and Privacy for Refugees in the United States   
Lucy Simko (University of Washington), Ada Lerner (Wellesley College), Samia Ibtasam (University of Washington), Franziska Roesner (University of Washington), Tadayoshi Kohno (University of Washington)

In this work, we consider the computer security and privacy practices and needs of recently resettled refugees in the United States. We ask: How do refugees use and rely on technology as they settle in the US? What computer security and privacy practices do they have, and what barriers do they face that may put them at risk? And how are their computer security mental models and practices shaped by the advice they receive? We study these questions through in-depth qualitative interviews with case managers and teachers who work with refugees at a local NGO, as well as through focus groups with refugees themselves. We find that refugees must rely heavily on technology (e.g., email) as they attempt to establish their lives and find jobs; that they also rely heavily on their case managers and teachers for help with those technologies; and that these pressures can push security practices into the background or make common security "best practices'' infeasible. At the same time, we identify fundamental challenges to computer security and privacy for refugees, including barriers due to limited technical expertise, language skills, and cultural knowledge--for example, we find that scams as a threat are a new concept for many of the refugees we studied, and that many common security practices (e.g., password creation techniques and security questions) rely on US cultural knowledge. From these and other findings, we distill recommendations for the computer security community to better serve the computer security and privacy needs and constraints of refugees, a potentially vulnerable population that has not been previously studied in this context.

\*\*\*\*\*

Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks   
Kai Jansen (Ruhr-University Bochum), Matthias Schäfer (University of Kaiserslautern), Daniel Moser (ETH Zurich), Vincent Lenders (armasuisse), Christina Pöpper (New York University Abu Dhabi), Jens Schmitt (University of Kaiserslautern)

The aviation industry's increasing reliance on GPS to facilitate navigation and air traffic monitoring opens new attack vectors with the purpose of hijacking UAVs or interfering with air safety. We propose Crowd-GPS-Sec to detect and localize GPS spoofing attacks on moving airborne targets such as UAVs or commercial airliners. Unlike previous attempts to secure GPS, Crowd-GPS-Sec neither requires any updates of the GPS infrastructure nor of the airborne GPS receivers, which are both unlikely to happen in the near future. In contrast, Crowd-GPS-Sec leverages crowdsourcing to monitor the air traffic from GPS-derived position advertisements that aircraft periodically broadcast for air traffic control purposes. Spoofing attacks are detected and localized by an independent infrastructure on the ground which continuously analyzes the contents and the times of arrival of these advertisements. We evaluate our system with real-world data from a crowdsourced air traffic monitoring sensor network and by simulations. We show that Crowd-GPS-Sec is able to globally detect GPS spoofing attacks in less than two seconds and to localize the attacker up to an accuracy of 150 meters after 15 minutes of monitoring time.

\*\*\*\*\*

DEEPSEC: Deciding Equivalence Properties in Security Protocols -- Theory and Practice   
Vincent Cheval (Inria Nancy & Loria), Steve Kremer (Inria Nancy & Loria), Itsaka Rakotonirina (Inria Nancy & Loria)

Automated verification has become an essential part in the security evaluation of cryptographic protocols. Recently, there has been a considerable effort to lift the theory and tool support that existed for reachability properties to the more complex case of equivalence properties. In this paper we contribute both to the theory and practice of this ver- ification problem. We establish new complexity results for static equivalence, trace equivalence and labelled bisimilarity and provide a decision procedure for these equivalences in the case of a bounded number of sessions. Our procedure is the first to decide trace equivalence and labelled bisimilarity exactly for a large variety of cryptographic primitives-those that can be represented by a subterm convergent destructor rewrite system. We implemented the procedure in a new tool, DEEPSEC. We showed through extensive experiments that it is significantly more efficient than other similar tools, while at the same time raises the scope of the protocols that can be analysed.

\*\*\*\*\*

Distance-Bounding Protocols: Verification without Time and Location   
Sjouke Mauw (CSC/SnT, University of Luxembourg), Zach Smith (CSC, University of Luxembourg), Jorge Toro-Pozo (CSC, University of Luxembourg), Rolando Trujillo-Rasua (SnT, University of Luxembourg)

Distance-bounding protocols are cryptographic protocols that securely establish an upper bound on the physical distance between the participants. Existing symbolic verification frameworks for distance-bounding protocols consider timestamps and the location of agents. In this work we introduce a causality-based characterization of secure distance-bounding that discards the notions of time and location. This allows us to verify the correctness of distance-bounding protocols with standard protocol verification tools. That is to say, we provide the first fully automated verification framework for distance-bounding protocols. By using our framework, we confirmed known vulnerabilities in a number of protocols and discovered unreported attacks against two recently published protocols.

\*\*\*\*\*

Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing using Different Sensor Types   
Jun Han (Carnegie Mellon University), Albert Jin Chung (Carnegie Mellon University), Manal Kumar Sinha (Carnegie Mellon University), Madhumitha Harishankar (Carnegie Mellon University), Shijia Pan (Carnegie Mellon University), Hae Young Noh (Carnegie Mellon University), Pei Zhang (Carnegie Mellon University), Patrick Tague (Carnegie Mellon University)

Context-based pairing solutions increase the usability of IoT device pairing by eliminating any human involvement in the pairing process. This is possible by utilizing on-board sensors (with same sensing modalities) to capture a common physical context (e.g., ambient sound via each device's microphone). However, in a smart home scenario, it is impractical to assume that all devices will share a common sensing modality. For example, a motion detector is only equipped with an infrared sensor while Amazon Echo only has microphones. In this paper, we develop a new context-based pairing mechanism called Perceptio that uses time as the common factor across differing sensor types. By focusing on the event timing, rather than the specific event sensor data, Perceptio creates event fingerprints that can be matched across a variety of IoT devices. We propose Perceptio based on the idea that devices co-located within a physically secure boundary (e.g., single family house) can observe more events in common over time, as opposed to devices outside. Devices make use of the observed contextual information to provide entropy for Perceptio's pairing protocol. We design and implement Perceptio, and evaluate its effectiveness as an autonomous secure pairing solution. Our implementation demonstrates the ability to sufficiently distinguish between legitimate devices (placed within the boundary) and attacker devices (placed outside) by imposing a threshold on fingerprint similarity. Perceptio demonstrates an average fingerprint similarity of 94.9% between legitimate devices while even a hypothetical impossibly well-performing attacker yields only 68.9% between itself and a valid device.

\*\*\*\*\*

Doubly-efficient zkSNARKs without trusted setup   
Riad S. Wahby (Stanford), Ioanna Tzialla (New York University), Abhi Shelat (Northeastern), Justin Thaler (Georgetown), Michael Walfish (New York University)

\*\*\*\*\*

EnclaveDB: A Secure Database using SGX   
Christian Priebe (Imperial College London), Kapil Vaswani (Microsoft Research), Manuel Costa (Microsoft Research)

We propose EnclaveDB, a database engine that guarantees confidentiality, integrity, and freshness for data and queries. EnclaveDB guarantees these properties even when the database administrator is malicious, when an attacker has compromised the operating system or the hypervisor, and when the database runs in an untrusted host in the cloud. EnclaveDB achieves this by placing sensitive data (tables, indexes and other metadata) in enclaves protected by trusted hardware (such as Intel SGX). EnclaveDB has a small trusted computing base, which includes an in-memory storage and query engine, a transaction manager and pre-compiled stored procedures. A key component of EnclaveDB is an efficient protocol for checking integrity and freshness of the database log. The protocol supports concurrent, asynchronous appends and truncation, and requires minimal synchronization between threads. Our experiments using standard database benchmarks and a performance model that simulates large enclaves show that EnclaveDB achieves strong security with low overhead (up to 40% for TPC-C) compared to an industry strength in-memory database engine.

\*\*\*\*\*

Enumerating Active IPv6 Hosts for Large-scale Security Scans via DNSSEC-signed Reverse Zones   
Kevin Borgolte (University of California, Santa Barbara), Shuang Hao (University of Texas at Dallas), Tobias Fiebig (Delft University of Technology), Giovanni Vigna (University of California, Santa Barbara)

Security research has made extensive use of exhaustive Internet-wide scans over the recent years, as they can provide significant insights into the overall state of security of the Internet, and ZMap made scanning the entire IPv4 address space practical. However, the IPv4 address space is exhausted, and a switch to IPv6, the only accepted long-term solution, is inevitable. In turn, to better understand the security of devices connected to the Internet, including in particular Internet of Things devices, it is imperative to include IPv6 addresses in security evaluations and scans. Unfortunately, it is practically infeasible to iterate through the entire IPv6 address space, as it is 2^96 times larger than the IPv4 address space. Therefore, enumeration of active hosts prior to scanning is necessary. Without it, we will be unable to investigate the overall security of Internet-connected devices in the future.  
  
In this paper, we introduce a novel technique to enumerate an active part of the IPv6 address space by walking DNSSEC-signed IPv6 reverse zones. Subsequently, by scanning the enumerated addresses, we uncover significant security problems: the exposure of sensitive data, and incorrectly controlled access to hosts, such as access to routing infrastructure via administrative interfaces, all of which were accessible via IPv6. Furthermore, from our analysis of the differences between accessing dual-stack hosts via IPv6 and IPv4, we hypothesize that the root cause is that machines automatically and by default take on globally routable IPv6 addresses. This is a practice that the affected system administrators appear unaware of, as the respective services are almost always properly protected from unauthorized access via IPv4.  
  
Our findings indicate (i) that enumerating active IPv6 hosts is practical without a preferential network position contrary to common belief, (ii) that the security of active IPv6 hosts is currently still lagging behind the security state of IPv4 hosts, and (iii) that unintended IPv6 connectivity is a major security issue for unaware system administrators.

\*\*\*\*\*

EyeTell: Video-Assisted Touchscreen Keystroke Inference from Eye Movements   
Yimin Chen (Arizona State University), Tao Li (Arizona State University), Rui Zhang (University of Delaware), Yanchao Zhang (Arizona State University), Terri Hedgpeth (Arizona State University)

Keystroke inference attacks pose an increasing threat to ubiquitous mobile devices. This paper presents EyeTell, a novel video-assisted attack that can infer a victim's keystrokes on his touchscreen device from a video capturing his eye movements. EyeTell explores the observation that human eyes naturally focus on and follow the keys they type, so a typing sequence on a soft keyboard results in a unique gaze trace of continuous eye movements. In contrast to prior work, EyeTell requires neither the attacker to visually observe the victim's inputting process nor the victim device to be placed on a static holder. Comprehensive experiments on iOS and Android devices confirm the high efficacy of EyeTell for inferring PINs, lock patterns, and English words under various environmental conditions.

\*\*\*\*\*

FP-STALKER: Tracking Browser Fingerprint Evolutions Along Time   
Antoine Vastel (University of Lille / INRIA), Pierre Laperdrix (INSA / INRIA), Walter Rudametkin (University of Lille / INRIA), Romain Rouvoy (University of Lille / INRIA)

Browser fingerprinting has emerged as a technique to track users without their consent. Unlike cookies, fingerprinting is a stateless technique that does not store any information on devices, but instead exploits unique combinations of attributes handed over freely by browsers. The uniqueness of fingerprints allows them to be used for identification. However, browser fingerprints change over time and the effectiveness of tracking users over longer durations has not been properly addressed.  
  
In this paper, we show that browser fingerprints tend to change frequently-from every few hours to days-due to, for example, software updates or configuration changes. Yet, despite these frequent changes, we show that browser fingerprints can still be linked, thus enabling long-term tracking.  
  
FP-STALKER is an approach to link browser fingerprint evolutions. It compares fingerprints to determine if they originate from the same browser. We created two variants of FP-STALKER, a rule-based variant that is faster, and a hybrid variant that exploits machine learning to boost accuracy. To evaluate FP-STALKER , we conduct an empirical study using 98,598 fingerprints we collected from 1, 905 distinct browser instances. We compare our algorithm with the state of the art and show that, on average, we can track browsers for 54.48 days, and 26 % of browsers can be tracked for more than 100 days.

\*\*\*\*\*

FPGA-Based Remote Power Side-Channel Attacks   
Mark Zhao (Cornell University), G. Edward Suh (Cornell University)

The rapid adoption of heterogeneous computing has driven the integration of Field Programmable Gate Arrays (FPGAs) into cloud datacenters and flexible System-on-Chips (SoCs). This paper shows that the integrated FPGA introduces a new security vulnerability by enabling software-based power side-channel attacks without physical proximity to a target system. We first demonstrate that an on-chip power monitor can be built on a modern FPGA using ring oscillators (ROs), and characterize its ability to observe the power consumption of other modules on the FPGA or the SoC. Then, we show that the RO- based FPGA power monitor can be used for a successful power analysis attack on an RSA cryptomodule on the same FPGA. Additionally, we show that the FPGA-based power monitor can observe the power consumption of a CPU on the same SoC, and demonstrate that the FPGA-to-CPU power side-channel attack can break timing-channel protection for a RSA program running on a CPU. This work introduces and demonstrates remote power side-channel attacks using an FPGA, showing that the common assumption that power side-channel attacks require specialized equipment and physical access to the victim hardware is not true for systems with an integrated FPGA.

\*\*\*\*\*

FuturesMEX: Secure, Distributed Futures Market Exchange   
Fabio Massacci (University of Trento, IT), Chan Nam Ngo (University of Trento, IT), Jing Nie (University of International Business and Economics Beijing, CN), Daniele Venturi (University of Rome "La Sapienza", IT), Julian Williams (University of Durham, UK)

In a Futures-Exchange, such as the Chicago Mercantile Exchange, traders buy and sell contractual promises (futures) to acquire or deliver, at some future pre-specified date, assets ranging from wheat to crude oil and from bacon to cash in a desired currency. The interactions between economic and security properties and the exchange's essentially non-monotonic security behavior; a valid trader's valid action can invalidate other traders' previously valid positions, are a challenge for security research.  
  
We show the security properties that guarantee an Exchange's economic viability (availability of trading information, liquidity, confidentiality of positions, absence of price discrimination, risk-management) and an attack when traders' anonymity is broken.  
  
We describe all key operations for a secure, fully distributed Futures-Exchange, hereafter referred to as simply the "Exchange". Our distributed, asynchronous protocol simulates the centralized functionality under the assumptions of anonymity of the physical layer and availability of a distributed ledger. We consider security with abort (in absence of honest majority) and extend it to penalties. Our proof of concept implementation and its optimization (based on zk-SNARKs and SPDZ) demonstrate that the computation of actual trading days (along Thomson-Reuters Tick History DB) is feasible for low-frequency markets; however, more research is needed for high-frequency ones.

\*\*\*\*\*

Grand Pwning Unit: Accelerating Microarchitectural Attacks with the GPU   
Pietro Frigo (Vrije Universiteit Amsterdam), Kaveh Razavi (Vrije Universiteit Amsterdam), Cristiano Giuffrida (Vrije Universiteit Amsterdam), Herbert Bos (Vrije Universiteit Amsterdam)

\*\*\*\*\*

Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes   
Daniel Votipka (University of Maryland), Rock Stevens (University of Maryland), Elissa Redmiles (University of Maryland), Jeremy Hu (University of Maryland), Michelle Mazurek (University of Maryland)

Identifying security vulnerabilities in software is a critical task that requires significant human effort. Currently, vulnerability discovery is often the responsibility of software testers before release and white-hat hackers (often within bug bounty programs) afterward. This arrangement can be ad-hoc and far from ideal; for example, if testers could identify more vulnerabilities, software would be more secure at release time. Thus far, however, the processes used by each group - and how they compare to and interact with each other - have not been well studied. This paper takes a first step toward better understanding, and eventually improving, this ecosystem: we report on a semi-structured interview study (n=25) with both testers and hackers, focusing on **how each group finds vulnerabilities**, how they develop their skills, and the challenges they face. The results suggest that hackers and testers follow similar processes, but get different results due largely to differing experiences and therefore different underlying knowledge of security concepts. Based on these results, **we provide recommendations to support improved security training for testers, better communication between hackers and developers, and smarter bug bounty policies to motivate hacker participation.**

\*\*\*\*\*

Implementing Conjunction Obfuscation under Entropic Ring LWE   
David Bruce Cousins (Raytheon BBN Technologies), Giovanni Di Crescenzo (Applied Communication Sciences / Vencore Labs), Kamil Doruk Gür (NJIT Cybersecurity Research Center, New Jersey Institute of Technology), Kevin King (Massachusetts Institute of Technology), Yuriy Polyakov (NJIT Cybersecurity Research Center, New Jersey Institute of Technology), Kurt Rohloff (NJIT Cybersecurity Research Center, New Jersey Institute of Technology), Gerard W. Ryan (NJIT Cybersecurity Research Center, New Jersey Institute of Technology), Erkay Savaş (NJIT Cybersecurity Research Center, New Jersey Institute of Technology)

We address the practicality challenges of secure program obfuscation \revised{by implementing, optimizing, and experimentally assessing an approach to securely obfuscate conjunction programs proposed in [1]. Conjunction programs evaluate functions $f\left(x\_1,\ldots,x\_L\right) = \bigwedge\_{i \in I} y\_i$, where $y\_i$ is either $x\_i$ or $\lnot x\_i$ and $I \subseteq \left[L\right]$, and can be used as classifiers. Our obfuscation approach satisfies distributional Virtual Black Box (VBB) security based on reasonable hardness assumptions, namely an entropic variant of the Ring Learning with Errors (Ring-LWE) assumption. Prior implementations of secure program obfuscation techniques support either trivial programs like point functions, or support the obfuscation of more general but less efficient branching programs to satisfy Indistinguishability Obfuscation (IO), a weaker security model. Further, the more general implemented techniques, rather than relying on standard assumptions, base their security on conjectures that have been shown to be theoretically vulnerable.  
  
Our work is the first implementation of non-trivial program obfuscation based on polynomial rings. Our contributions include multiple design and implementation advances resulting in reduced program size, obfuscation runtime, and evaluation runtime by many orders of magnitude. We implement our design in software and experimentally assess performance in a commercially available multi-core computing environment. Our implementation achieves runtimes of 6.7 hours to securely obfuscate a 64-bit conjunction program and 2.5 seconds to evaluate this program over an arbitrary input. We are also able to obfuscate a 32-bit conjunction program with \revised{53 bits} of security in 7 minutes and evaluate the obfuscated program in 43 milliseconds on a commodity desktop computer, which implies that 32-bit conjunction obfuscation is already practical. Our graph-induced (directed) encoding implementation runs up to 25 levels, which is higher than previously reported in the literature for this encoding. Our design and implementation advances are applicable to obfuscating more general compute-and-compare programs and can also be used for many cryptographic schemes based on lattice trapdoors.

\*\*\*\*\*

Impossibility of Precise and Sound Termination-Sensitive Security Enforcements   
Minh Ngo (INRIA, France), Frank Piessens (imec-DistriNet, KU Leuven, Belgium), Tamara Rezk (INRIA, France)

An information flow policy is termination-sensitive if it imposes that the termination behavior of programs is not influenced by confidential input. Termination-sensitivity can be statically or dynamically enforced. On one hand, existing static enforcement mechanisms for termination-sensitive policies are typically quite conservative and impose strong constraints on programs like absence of while loops whose guard depends on confidential information. On the other hand, dynamic mechanisms can enforce termination-sensitive policies in a less conservative way. Secure Multi-Execution (SME), one of such mechanisms, was even claimed to be sound and precise in the sense that the enforcement mechanism will not modify the observable behavior of programs that comply with the termination-sensitive policy. However, termination-sensitivity is a subtle policy, that has been formalized in different ways. A key aspect is whether the policy talks about actual termination, or observable termination.  
  
This paper proves that termination-sensitive policies that talk about actual termination are not enforceable in a sound and precise way. For static enforcements, the result follows directly from a reduction of the decidability of the problem to the halting problem. However, for dynamic mechanisms the insight is more involved and requires a diagonalization argument.   
  
In particular, our result contradicts the claim made about SME. We correct these claims by showing that SME enforces a subtly different policy that we call indirect termination-sensitive noninterference and that talks about observable termination instead of actual termination. We construct a variant of SME that is sound and precise for indirect termination-sensitive noninterference. Finally, we also show that static methods can be adapted to enforce indirect termination-sensitive information flow policies (but obviously not precisely) by constructing a sound type system for an indirect termination-sensitive policy.

\*\*\*\*\*

Improved Reconstruction Attacks on Encrypted Data Using Range Query Leakage   
Marie-Sarah Lacharite (Royal Holloway, University of London), Brice Minaud (Royal Holloway, University of London), Kenneth G. Paterson (Royal Holloway, University of London)

We analyse the security of database encryption schemes supporting range queries against persistent adversaries. The bulk of our work applies to a generic setting, where the adversary's view is limited to the set of records matched by each query (known as access pattern leakage). We also consider a more specific setting where rank information is also leaked, which is inherent inherent to multiple recent encryption schemes supporting range queries. We provide three attacks.  
  
First, we consider full reconstruction, which aims to recover the value of every record, fully negating encryption. We show that for dense datasets, full reconstruction is possible within an expected number of queries N log N + O(N), where N is the number of distinct plaintext values.  
This directly improves on a quadratic bound in the same setting by Kellaris et al. (CCS 2016).  
  
Second, we present an approximate reconstruction attack recovering all plaintext values in a dense dataset within a constant ratio of error, requiring the access pattern leakage of only O(N) queries.   
  
Third, we devise an attack in the common setting where the adversary has access to an auxiliary distribution for the target dataset. This third attack proves highly effective on age data from real-world medical data sets. In our experiments, observing only 25 queries was sufficient to reconstruct a majority of records to within 5 years.  
  
In combination, our attacks show that current approaches to enabling range queries offer little security when the threat model goes beyond snapshot attacks to include a persistent server-side adversary.

\*\*\*\*\*

Learning from Mutants: Using Code Mutation to Learn and Monitor Invariants of a Cyber-Physical System   
Yuqi Chen (Singapore University of Technology and Design), Christopher M. Poskitt (Singapore University of Technology and Design), Jun Sun (Singapore University of Technology and Design)

Cyber-physical systems (CPS) consist of sensors, actuators, and controllers all communicating over a network; if any subset becomes compromised, an attacker could cause significant damage. With access to data logs and a model of the CPS, the physical effects of an attack could potentially be detected before any damage is done. Manually building a model that is accurate enough in practice, however, is extremely difficult. In this paper, we propose a novel approach for constructing models of CPS automatically, by applying supervised machine learning to data traces obtained after systematically seeding their software components with faults ("mutants"). We demonstrate the efficacy of this approach on the simulator of a real-world water purification plant, presenting a framework that automatically generates mutants, collects data traces, and learns an SVM-based model. Using cross-validation and statistical model checking, we show that the learnt model characterises an invariant physical property of the system. Furthermore, we demonstrate the usefulness of the invariant by subjecting the system to 55 network and code-modification attacks, and showing that it can detect 85% of them from the data logs generated at runtime.

\*\*\*\*\*

Locally Differentially Private Frequent Itemset Mining   
Tianhao Wang (Purdue University), Ninghui Li (Purdue University), Somesh Jha (University of Wisconsin-Madison)

The notion of Local Differential Privacy (LDP) enables users to respond to sensitive questions while preserving their privacy. The basic LDP frequent oracle (FO) protocol enables an aggregator to estimate the frequency of any value. But when each user has a set of values, one needs an additional padding and sampling step to find the frequent values and estimate their frequencies. In this paper, we formally define such padding and sample based frequency oracles (PSFO). We further identify the privacy amplification property in PSFO. As a result, we propose SVIM, a protocol for finding frequent items in the set-valued LDP setting. Experiments show that under the same privacy guarantee and computational cost, SVIM significantly improves over existing methods. With SVIM to find frequent items, we propose SVSM to effectively find frequent itemsets, which to our knowledge has not been done before in the LDP setting.

\*\*\*\*\*

**IMPORTANT**

Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning   
Matthew Jagielski (Northeastern University), Alina Oprea (Northeastern University), Battista Biggio (University of Cagliari, Italy; Pluribus One, Italy), Chang Liu (UC Berkeley), Cristina Nita-Rotaru (Northeastern University), Bo Li (UC Berkeley)

As machine learning becomes widely used for automated decisions, attackers have strong incentives to manipulate the results and models generated by machine learning algorithms. In this paper, we perform the first systematic study of poisoning attacks and their countermeasures for linear regression models. In poisoning attacks, attackers deliberately influence the training data to manipulate the results of a predictive model. We propose a theoretically-grounded optimization framework specifically designed for linear regression and demonstrate its effectiveness on a range of datasets and models. We also introduce a fast statistical attack that requires limited knowledge of the training process. Finally, we design a new principled defense method that is highly resilient against all poisoning attacks. We provide formal guarantees about its convergence and an upper bound on the effect of poisoning attacks when the defense is deployed. We evaluate extensively our attacks and defenses on three realistic datasets from health care, loan assessment, and real estate domains.

\*\*\*\*\*

Mobile Application Web API Reconnaissance: Web-to-Mobile Inconsistencies & Vulnerabilities   
Abner Mendoza (Texas A&M; University), Guofei Gu (Texas A&M; University)

Modern mobile apps use cloud-hosted HTTP-based API services and heavily rely on the Internet infrastructure for data communication and storage. To improve performance and leverage the power of the mobile device, input validation and other business logic required for interfacing with web API services are typically implemented on the mobile client. However, when a web service implementation fails to thoroughly replicate input validation, it gives rise to inconsistencies that could lead to attacks that can compromise user security and privacy. Developing automatic methods of auditing web APIs for security remains challenging.  
  
In this paper, we present a novel approach for automatically analyzing mobile app-to-web API communication to detect inconsistencies in input validation logic between apps and their respective web API services. We present our system, \sysname, which implements a static analysis-based web API reconnaissance approach to uncover inconsistencies on real world API services that can lead to attacks with severe consequences for potentially millions of users throughout the world. Our system utilizes program analysis techniques to automatically extract HTTP communication templates from Android apps that encode the input validation constraints imposed by the apps on outgoing web requests to web API services. WARDroid is also enhanced with blackbox testing of server validation logic to identify inconsistencies that can lead to attacks.   
  
We evaluated our system on a set of 10,000 popular free apps from the Google Play Store. We detected problematic logic in APIs used in over 4,000 apps, including 1,743 apps that use unencrypted HTTP communication. We further tested 1,000 apps to validate web API hijacking vulnerabilities that can lead to potential compromise of user privacy and security and found that millions of users are potentially affected from our sample set of tested apps.

\*\*\*\*\*

**IMPORTANT**

Oblix: An Efficient Oblivious Search Index   
Pratyush Mishra (UC Berkeley), Rishabh Poddar (UC Berkeley), Jerry Chen (UC Berkeley), Alessandro Chiesa (UC Berkeley), Raluca Ada Popa (UC Berkeley)

Search indices are fundamental building blocks of many systems, and there is great interest in running them on encrypted data. Unfortunately, many known schemes that enable search queries on encrypted data achieve efficiency at the expense of security, as they reveal access patterns to the encrypted data.  
  
In this paper we present Oblix, a search index for encrypted data that is oblivious (provably hides access patterns), is dynamic (supports inserts and deletes), and has good efficiency.  
  
Oblix relies on a combination of novel oblivious-access techniques and recent hardware enclave platforms (e.g., Intel SGX). In particular, a key technical contribution is the design and implementation of doubly-oblivious data structures, in which the client's accesses to its internal memory are oblivious, in addition to accesses to its external memory at the server. These algorithms are motivated by hardware enclaves like SGX, which leak access patterns to both internal and external memory.  
  
We demonstrate the usefulness of Oblix in several applications: private contact discovery for Signal, private retrieval of public keys for Key Transparency, and searchable encryption that hides access patterns and result sizes.

\*\*\*\*\*

OmniLedger: A Secure, Scale-Out, Decentralized Ledger via **Sharding**  
Eleftherios Kokoris-Kogias (École Polytechnique Fédérale de Lausanne), Philipp Jovanovic (École Polytechnique Fédérale de Lausanne), Linus Gasser (École Polytechnique Fédérale de Lausanne), Nicolas Gailly (École Polytechnique Fédérale de Lausanne), Ewa Syta (Trinity College), Bryan Ford (École Polytechnique Fédérale de Lausanne)

Designing a secure permissionless distributed ledger (blockchain) that performs on par with centralized payment processors, such as Visa, is a challenging task. Most existing distributed ledgers are unable to scale-out, i.e., to grow their total processing capacity with the number of validators; and those that do, compromise security or decentralization. We present OmniLedger, a novel scale-out distributed ledger that preserves long- term security under permissionless operation. It ensures security and correctness by using a bias-resistant public-randomness protocol for choosing large, statistically representative shards that process transactions, and by introducing an efficient cross- shard commit protocol that atomically handles transactions affecting multiple shards. OmniLedger also optimizes performance via parallel intra-shard transaction processing, ledger pruning via collectively-signed state blocks, and low-latency "trust-but- verify" validation for low-value transactions. An evaluation of our experimental prototype shows that OmniLedger's throughput scales linearly in the number of active validators, supporting Visa-level workloads and beyond, while confirming typical transactions in under two seconds.

\*\*\*\*\*

On Enforcing the Digital Immunity of a Large Humanitarian Organization   
Stevens Le Blond (École Polytechnique Fédérale de Lausanne), Alejandro Cuevas (École Polytechnique Fédérale de Lausanne), Juan Ramón Troncoso-Pastoriza (École Polytechnique Fédérale de Lausanne), Philipp Jovanovic (École Polytechnique Fédérale de Lausanne), Bryan Ford (École Polytechnique Fédérale de Lausanne), Jean-Pierre Hubaux (École Polytechnique Fédérale de Lausanne)

Humanitarian action, the process of aiding individuals in situations of crises, poses unique information-security challenges due to natural or manmade disasters, the adverse environments in which it takes place, and the scale and multi-disciplinary nature of the problems. Despite these challenges, humanitarian organizations are transitioning towards a strong reliance on the digitization of collected data and digital tools, which improves their effectiveness but also exposes them to computer security threats. In this paper, we conduct a qualitative analysis of the computer-security challenges of the International Committee of the Red Cross (ICRC), a large humanitarian organization with over sixteen thousand employees, an international legal personality, which involves privileges and immunities, and over 150 years of experience with armed conflicts and other situations of violence worldwide. To investigate the computer security needs and practices of the ICRC from an operational, technical, legal, and managerial standpoint by considering individual, organizational, and governmental levels, we interviewed 27 field workers, IT staff, lawyers, and managers. Our results provide a first look at the unique security and privacy challenges that humanitarian organizations face when collecting, processing, transferring, and sharing data to enable humanitarian action for a multitude of sensitive activities. These results highlight, among other challenges, the trade offs between operational security and requirements stemming from all stakeholders, the legal barriers for data sharing among jurisdictions; especially, the need to complement privileges and immunities with robust technological safeguards in order to avoid any leakages that might hinder access and potentially compromise the neutrality, impartiality, and independence of humanitarian action.

\*\*\*\*\*

**On the Economics of Offline Password Cracking**  
Jeremiah Blocki (Purdue University), Benjamin Harsha (Purdue University), Samson Zhou (Purdue University)

We develop an economic model of an offline password cracker which allows us to make quantitative predictions about the fraction of accounts that a rational password attacker would crack in the event of an authentication server breach. We apply our economic model to analyze recent massive password breaches at Yahoo!, Dropbox, LastPass and AshleyMadison. All four organizations were using key-stretching to protect user passwords. In fact, LastPass' use of PBKDF2-SHA256 with $10^5$ hash iterations exceeds 2017 NIST minimum recommendation by an order of magnitude. Nevertheless, our analysis paints a bleak picture: the adopted key-stretching levels provide insufficient protection for user passwords. In particular, we present strong evidence that most user passwords follow a Zipf's law distribution, and characterize the behavior of a rational attacker when user passwords are selected from a Zipf's law distribution. We show that there is a finite threshold which depends on the Zipf's law parameters that characterizes the behavior of a rational attacker --- if the value of a cracked password (normalized by the cost of computing the password hash function) exceeds this threshold then the adversary's optimal strategy is *always* to continue attacking until each user password has been cracked. In all cases (Yahoo!, Dropbox, LastPass and AshleyMadison) we find that the value of a cracked password almost certainly exceeds this threshold meaning that a rational attacker would crack all passwords that are selected from the Zipf's law distribution (i.e., most user passwords). This prediction holds even if we incorporate an aggressive model of diminishing returns for the attacker (e.g., the total value of $500$ million cracked passwords is less than $100$ times the total value of $5$ million passwords). On a positive note our analysis demonstrates that memory hard functions (MHFs) such as SCRYPT or Argon2i can significantly reduce the damage of an offline attack. In particular, we find that because MHFs substantially increase guessing costs a rational attacker will give up well before he cracks most user passwords and this prediction holds even if the attacker does not encounter diminishing returns for additional cracked passwords. Based on our analysis we advocate that password hashing standards should be updated to require the use of memory hard functions for password hashing and disallow the use of non-memory hard functions such as BCRYPT or PBKDF2.

\*\*\*\*\*

PIR with compressed queries and probabilistic codes   
Sebastian Angel (UT Austin and NYU), Hao Chen (Microsoft Research), Kim Laine (Microsoft Research), Srinath Setty (Microsoft Research)

Private information retrieval (PIR) is a key building block in many privacy-preserving systems. Unfortunately, existing constructions remain very expensive. This paper introduces two techniques that make the computational variant of PIR (CPIR) more efficient in practice. The first technique targets a recent class of CPU-efficient CPIR protocols where the query sent by the client contains a number of ciphertexts proportional to the size of the database. We show how to compresses this query, achieving size reductions of up to 274X. The second technique is a new data encoding called probabilistic batch codes (PBCs). We use PBCs to build a multi query PIR scheme that allows the server to amortize its computational cost when processing a batch of requests from the same client. This technique achieves up to 40× speedup over processing queries one at a time, and is significantly more efficient than related encodings. We apply our techniques to the Pung private communication system, which relies on a custom multi-query CPIR protocol for its privacy guarantees. By porting our techniques to Pung, we find that we can simultaneously reduce network costs by 36× and increase throughput by 3X.

\*\*\*\*\*

Precise and Scalable Detection of Double-Fetch Bugs in OS Kernels   
Meng Xu (Georgia Institute of Technology), Chenxiong Qian (Georgia Institute of Technology), Kangjie Lu (University of Minnesota), Michael Backes (CISPA Helmholtz Center i.G.), Taesoo Kim (Georgia Institute of Technology)

During system call execution, it is common for operating system kernels to read userspace memory multiple times (multi-reads). A critical bug may exist if the fetched userspace memory is subject to change across these reads, i.e., a race condition, which is known as a double-fetch bug. Prior works have attempted to detect these bugs both statically and dynamically. However, due to their improper assumptions and imprecise definitions regarding double-fetch bugs, their multi-read detection is inherently limited and suffers from significant false positives and false negatives. For example, their approach is unable to support device emulation, inter-procedural analysis, loop handling, etc. More importantly, they completely leave the task of finding real double-fetch bugs from the haystack of multi-reads to manual verification, which is expensive if possible at all.  
  
In this paper, we first present a formal and precise definition of double-fetch bugs and then implement a static analysis system -Deadline - to automatically detect double-fetch bugs in OS kernels. Deadline uses static program analysis techniques to systematically find multi-reads throughout the kernel and employs specialized symbolic checking to vet each multi-read for double-fetch bugs. We apply Deadline to Linux and FreeBSD kernels and find 23 new bugs in Linux and one new bug in FreeBSD. We further propose four generic strategies to patch and prevent double-fetch bugs based on our study and the discussion with kernel maintainers.

\*\*\*\*\*

**Privacy Risks with Facebook's PII-based Targeting: Auditing a Data Broker's Advertising Interface**  
Giridhari Venkatadri (Northeastern University), Athanasios Andreou (EURECOM), Yabing Liu (Northeastern University), Alan Mislove (Northeastern University), Krishna P. Gummadi (MPI-SWS), Patrick Loiseau (Univ. Grenoble Alpes, CNRS, Inria, Grenoble INP, LIG and MPI-SWS), Oana Goga (Univ. Grenoble Alpes, CNRS, Inria, Grenoble INP, LIG)

Sites like Facebook and Google now serve as de facto data brokers, aggregating data on users for the purpose of implementing powerful advertising platforms. Historically, these services allowed advertisers to select which users see their ads via targeting attributes. Recently, most advertising platforms have begun allowing advertisers to target users directly by uploading the personal information of the users who they wish to advertise to (e.g., their names, email addresses, phone numbers, etc.); these services are often known as custom audiences. Custom audiences effectively represent powerful linking mechanisms, allowing advertisers to leverage any PII (e.g., from customer data, public records, etc.) to target users.  
  
In this paper, we focus on Facebook's custom audience implementation and demonstrate attacks that allow an adversary to exploit the interface to infer users' PII as well as to infer their activity. Specifically, we show how the adversary can infer users' full phone numbers knowing just their email address, determine whether a particular user visited a website, and de-anonymize all the visitors to a website by inferring their phone numbers en masse. These attacks can be conducted without any interaction with the victim(s), cannot be detected by the victim(s), and do not require the adversary to spend money or actually place an ad. We propose a simple and effective fix to the attacks based on reworking the way Facebook de-duplicates uploaded information. Facebook's security team acknowledged the vulnerability and has put into place a fix that is a variant of the fix we propose. Overall, our results indicate that advertising platforms need to carefully consider the privacy implications of their interfaces.

\*\*\*\*\*

**Protecting the Stack with Metadata Policies and Tagged Hardware**   
Nick Roessler (University of Pennsylvania), Andre DeHon (University of Pennsylvania)

The program call stack is a major source of exploitable security vulnerabilities in low-level, unsafe languages like C. In conventional runtime implementations, the underlying stack data is exposed and unprotected, allowing programming errors to turn into security violations. In this work, we design novel metadata-tag based, stack-protection security policies for a general-purpose tagged architecture. Our policies specifically exploit the natural locality of dynamic program call graphs to achieve cacheability of the metadata rules that they require. Our simple Return Address Protection policy has a performance overhead of 1.2% but just protects return addresses. The two richer policies we present, Static Authorities and Depth Isolation, provide object-level protection for all stack objects. When enforcing memory safety, our Static Authorities policy has a performance overhead of 5.7% and our Depth Isolation policy has a performance overhead of 4.5%. When enforcing data-flow integrity (DFI), in which we only detect a violation when a corrupted value is read, our Static Authorities policy has a performance overhead of 3.6% and our Depth Isolation policy has a performance overhead of 2.4%. To characterize our policies, we provide a stack threat taxonomy and show which threats are prevented by both prior work protection mechanisms and our policies.

\*\*\*\*\*

**Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races**  
Guoxing Chen (The Ohio State University), Wenhao Wang (Indiana University Bloomington & SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences), Tianyu Chen (Indiana University Bloomington), Sanchuan Chen (The Ohio State University), Yinqian Zhang (The Ohio State University), XiaoFeng Wang (Indiana University Bloomington), Ten-Hwang Lai (The Ohio State University), Dongdai Lin (SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences)

In this paper, we present HYPERRACE, an LLVM-based tool for instrumenting SGX enclave programs to eradicate all side-channel threats due to Hyper-Threading. HYPERRACE creates a shadow thread for each enclave thread and asks the underlying untrusted operating system to schedule both threads on the same physical core whenever enclave code is invoked, so that Hyper-Threading side channels are closed completely. Without placing additional trust in the operating system's CPU scheduler, HYPERRACE conducts a physical-core co-location test: it first constructs a communication channel between the threads using a shared variable inside the enclave and then measures the communication speed to verify that the communication indeed takes place in the shared L1 data cache-a strong indicator of physical-core co-location. The key novelty of the work is the measurement of communication speed without a trustworthy clock; instead, relative time measurements are taken via contrived data races on the shared variable. It is worth noting that the emphasis of HYPERRACE's defense against Hyper-Threading side channels is because they are open research problems. In fact, HYPERRACE also detects the occurrence of exception- or interrupt-based side channels, the solutions of which have been studied by several prior works.

\*\*\*\*\*

**Routing Around Congestion: Defeating DDoS Attacks and Adverse Network Conditions via Reactive BGP Routing**  
Jared M Smith (University of Tennessee, Knoxville), Max Schuchard (University of Tennessee, Knoxville)

In this paper, we present Nyx, the first system to both effectively mitigate modern Distributed Denial of Service (DDoS) attacks regardless of the amount of traffic under adversarial control and function without outside cooperation or an Internet redesign. Nyx approaches the problem of DDoS mitigation as a routing problem rather than a filtering problem. This conceptual shift allows Nyx to avoid many of the common shortcomings of existing academic and commercial DDoS mitigation systems. By leveraging how Autonomous Systems (ASes) handle route advertisement in the existing Border Gateway Protocol (BGP), Nyx allows the deploying AS to achieve isolation of traffic from a critical upstream AS off of attacked links and onto alternative, uncongested, paths. This isolation removes the need for filtering or de-prioritizing attack traffic. Nyx controls outbound paths through normal BGP path selection, while return paths from critical ASes are controlled through the use of specific techniques we developed using existing traffic engineering principles and require no outside coordination. Using our own realistic Internet-scale simulator, we find that in more than 98% of cases our system can successfully route critical traffic around network segments under transit-link DDoS attacks; a new form of DDoS attack where the attack traffic never reaches the victim AS, thus invaliding defensive filtering, throttling, or prioritization strategies. More significantly, in over 95% of those cases, the alternate path provides complete congestion relief from transit-link DDoS. Nyx additionally provides complete congestion relief in over 75% of cases when the deployer is being directly attacked.

\*\*\*\*\*

**Secure Device Bootstrapping without Secrets Resistant to Signal Manipulation Attacks**   
Nirnimesh Ghose (University of Arizona), Loukas Lazos (University of Arizona), Ming Li (University of Arizona)

In this paper, we address the fundamental problem of securely bootstrapping a group of wireless devices to a hub, when none of the devices share prior associations (secrets) with the hub or between them. This scenario aligns with the secure deployment of body area networks, IoT, medical devices, industrial automation sensors, autonomous vehicles, and others. We develop VERSE, a physical-layer group message integrity verification primitive that effectively detects advanced wireless signal manipulations that can be used to launch man-in-the-middle (MitM) attacks over wireless. Without using shared secrets to establish authenticated channels, such attacks are notoriously difficult to thwart and can undermine the authentication and key establishment processes. VERSE exploits the existence of multiple devices to verify the integrity of the messages exchanged within the group. We then use VERSE to build a bootstrapping protocol, which securely introduces new devices to the network. Compared to the state-of-the-art, VERSE achieves in-band message integrity verification during secure pairing using only the RF modality without relying on out-of-band channels or extensive human involvement. It guarantees security even when the adversary is capable of fully controlling the wireless channel by annihilating and injecting wireless signals. We study the limits of such advanced wireless attacks and prove that the introduction of multiple legitimate devices can be leveraged to increase the security of the pairing process. We validate our claims via theoretical analysis and extensive experimentations on the USRP platform. We further discuss various implementation aspects such as the effect of time synchronization between devices and the effects of multipath and interference. Note that the elimination of shared secrets, default passwords, and public key infrastructures effectively addresses the related key management challenges when these are considered at scale.

\*\*\*\*\*

**Secure Two-party Threshold ECDSA from ECDSA Assumptions**  
Jack Doerner (Northeastern University), Yashvanth Kondi (Northeastern University), Eysa Lee (Northeastern University), abhi shelat (Northeastern University)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is one of the most widely used schemes in deployed cryptography. Through its applications in code and binary authentication, web security, and cryptocurrency, it is likely one of the few cryptographic algorithms encountered on a daily basis by the average person. However, its design is such that executing multi-party or threshold signatures in a secure manner is challenging: unlike other, less widespread signature schemes, secure multi-party ECDSA requires custom protocols, which has heretofore implied reliance upon additional cryptographic assumptions such as the Paillier encryption scheme.  
  
We propose new protocols for multi-party ECDSA key-generation and signing with a threshold of two, which we prove secure against malicious adversaries in the random oracle model using only the Computational Diffie-Hellman Assumption and the assumptions already implied by ECDSA itself. Our scheme requires only two messages, and via implementation we find that it outperforms the best prior results in practice by a factor of 55 for key generation and 16 for signing, coming to within a factor of 12 of local signatures. Concretely, two parties can jointly sign a message in just over two milliseconds.

\*\*\*\*\*

**SoK: "Plug & Pray" Today - Understanding USB Insecurity in Versions 1 through C**  
Jing Tian (University of Florida), Nolen Scaife (University of Florida), Deepak Kumar (University of Illinois at Urbana-Champaign), Michael Bailey (University of Illinois at Urbana-Champaign), Adam Bates (University of Illinois at Urbana-Champaign), Kevin Butler (University of Florida)

USB-based attacks have increased in complexity in recent years. Modern attacks now incorporate a wide range of attack vectors, from social engineering to signal injection. To address these challenges, the security community has responded with a growing set of fragmented defenses. In this work, we survey and categorize USB attacks and defenses, unifying observations from both peer-reviewed research and industry. Our systematization extracts offensive and defensive primitives that operate across layers of communication within the USB ecosystem. Based on our taxonomy, we discover that USB attacks often abuse the trust-by-default nature of the ecosystem, and transcend different layers within a software stack; none of the existing defenses provide a complete solution, and solutions expanding multiple layers are most effective. We then develop the first formal verification of the recently released USB Type- C Authentication specification, and uncover fundamental flaws in the specification's design. Based on the findings from our systematization, we observe that while the spec has successfully pinpointed an urgent need to solve the USB security problem, its flaws render these goals unattainable. We conclude by outlining future research directions to ensure a safer computing experience with USB.

\*\*\*\*\*

**SoK: Keylogging Side Channels**  
John Monaco (U.S. Army Research Laboratory)

The first keylogging side channel attack was discovered over 50 years ago when Bell Laboratory researchers noticed an electromagnetic spike emanating from a Bell 131-B2 teletype terminal. This spike, emitted upon each key press, enabled up to 75% of plaintext communications to be recovered in field conditions. Since then, keylogging attacks have come to leverage side channels emanating from the user's finger and hand movements, countless keyboard electromagnetic and acoustic emanations, microarchitectural attacks on the host computer, and encrypted network traffic. These attacks can each be characterized by the type of information the side channel leaks: a spatial side channel reveals physical key locations or the similarity between key pairs, and a temporal side channel leverages key press and release timings. We define and evaluate the performance of idealized spatial and temporal keylogging side channels and find that, under the assumption of typing English words, nontrivial information gains can be achieved even in the presence of substantial measurement error. For temporal side channels, we find that the information gained by different temporal features strongly correlates to typing speed and style. Finally, to help drive future research, we review the current state-of-the-art keylogging side channel attacks and discuss some of the mitigation techniques that can be applied.

\*\*\*\*\*

**Sonar: Detecting SS7 Redirection Attacks With Audio-Based Distance Bounding**  
Christian Peeters (University of Florida), Hadi Abdullah (University of Florida), Nolen Scaife (University of Florida), Jasmine Bowers (University of Florida), Patrick Traynor (University of Florida), Bradley Reaves (North Carolina State University), Kevin Butler (University of Florida)

The global telephone network is relied upon by billions every day. Central to its operation is the Signaling System 7 (SS7) protocol, which is used for setting up calls, managing mobility, and facilitating many other network services. This protocol was originally built on the assumption that only a small number of trusted parties would be able to directly communicate with its core infrastructure. As a result, SS7 *--- as a feature ---*allows all parties with core access to redirect and intercept calls for any subscriber anywhere in the world. Unfortunately, increased interconnectivity with the SS7 network has led to a growing number of illicit call redirection attacks. We address such attacks with Sonar, a system that detects the presence of SS7 redirection attacks by securely measuring call audio round-trip times between telephony devices. This approach works because redirection attacks force calls to travel longer physical distances than usual, thereby creating longer end-to-end delay. We design and implement a distance bounding-inspired protocol that allows us to securely characterize the round-trip time between the two endpoints. We then use custom hardware deployed in 10 locations across the United States and a redirection testbed to characterize how distance affects round trip time in phone networks. We develop a model using this testbed and show Sonar is able to detect 70.9% of redirected calls between call endpoints of varying attacker proximity (300--7100 miles) with low false positive rates (0.3%). Finally, we ethically perform actual SS7 redirection attacks on our own devices with the help of an industry partner to demonstrate that Sonar detects 100% of such redirections in a real network (*with no false positives*). As such, we demonstrate that telephone users can reliably detect SS7 redirection attacks and protect the integrity of their calls.

\*\*\*\*\*

**Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors**   
S Abhishek Anand (University of Alabama at Birmingham), Nitesh Saxena (University of Alabama at Birmingham)

According to recent research, motion sensors available on current smartphone platforms may be sensitive to speech signals. From a security and privacy perspective, this raises a serious concern regarding sensitive speech reconstruction, and speaker or gender identification by a malicious application having unrestricted access to motion sensor readings, without using the microphone.  
  
In this paper, we revisit this important line of research and closely inspect the effect of speech on smartphone motion sensors, in particular, gyroscope and accelerometer. First, we revisit the previously studied scenario (Michalevsky et al.; USENIX Security 2014), where the smartphone shares a common surface with a loudspeaker (with subwoofer) generating speech signals. We observe some effect on the motion sensor signals, which may indeed allow speaker and gender recognition to an extent. However, we also argue that the recorded effect on the sensor readings is possibly from conductive vibrations through the shared surface instead of direct acoustic vibrations due to speech as perceived in previous work. Second, we further extend the previous work by analyzing the effect of speech produced by (1) other less powerful speakers like the in-built laptop and smartphone speakers, and (2) live humans. Our experiments show that in-built laptop speakers were only able to affect the accelerometer when the laptop and the motion sensor shared a surface. Smartphone speakers were not found to be powerful enough to invoke a response in the motion sensors through aerial vibrations. We also report that in the presence of live human speech, we did not notice any effect on the motion sensor readings.  
  
Our results have two-fold implications. First, human-rendered speech seems potentially incapacitated to trigger smartphone motion sensors within the limited sampling rates imposed by the smartphone operating systems. Second, it seems that even machine-rendered speech may not be powerful enough to affect smartphone motion sensors through the aerial medium, although it may induce vibrations through a conductive surface that these sensors, especially accelerometer, could pick up if a relatively powerful speaker is used. Overall, our results suggest that smartphone motion sensors may pose a threat to speech privacy only in some limited scenarios.

\*\*\*\*\*

**Static Evaluation of Noninterference using Approximate Model Counting**   
Ziqiao Zhou (University of North Carolina at Chapel Hill), Zhiyun Qian (University of California, Riverside), Michael K. Reiter (University of North Carolina at Chapel Hill), Yinqian Zhang (The Ohio State University)

\*\*\*\*\*

**IMPORTANT**

**Stealing Hyperparameters in Machine Learning**  
Binghui Wang (ECE Department, Iowa State University), Neil Zhenqiang Gong (ECE Department, Iowa State University)

Hyperparameters are critical in machine learning, as different hyperparameters often result in models with significantly different performance. Hyperparameters **may be deemed confidential because of their commercial value and the confidentiality of the proprietary algorithms that the learner uses to learn them**. In this work, we propose attacks on stealing the hyperparameters that are learned by a learner. We **call our attacks hyperparameter stealing attacks**. Our attacks are applicable to a variety of popular machine learning algorithms such as **ridge regression, logistic regression, support vector machine, and neural network**. We evaluate the effectiveness of our attacks both theoretically and empirically. For instance, we evaluate our attacks on Amazon Machine Learning. Our results demonstrate that **our attacks can accurately steal hyperparameters**. We also study countermeasures. Our results highlight the need for new defenses against our hyperparameter stealing attacks for certain machine learning algorithms.

\*\*\*\*\*

**Study and Mitigation of Origin Stripping Vulnerabilities in Hybrid-postMessage Enabled Mobile Applications**  
Guangliang Yang (Texas A&M; University), Jeff Huang (Texas A&M; University), Guofei Gu (Texas A&M; University), Abner Mendoza (Texas A&M; University)

**postMessage is popular in HTML5 based web apps to allow the communication between different origins.** With the increasing popularity of the embedded browser (i.e., WebView) in mobile apps (i.e., hybrid apps), postMessage has found utility in these apps. However, different from web apps, hybrid apps have a unique requirement that their native code (e.g., Java for Android) also needs to exchange messages with web code loaded in WebView. To bridge the gap, developers typically extend postMessage by treating the native context as a new frame, and allowing the communication between the new frame and the web frames. We term such extended postMessage "hybrid postMessage" in this paper. We find that hybrid postMessage introduces new critical security flaws: all origin information of a message is not respected or even lost during the message delivery in hybrid postMessage. If adversaries inject malicious code into WebView, the malicious code may leverage the flaws to passively monitor messages that may contain sensitive information, or actively send messages to arbitrary message receivers and access their internal functionalities and data. We term the novel security issue caused by hybrid postMessage "Origin Stripping Vulnerability" (OSV).  
  
In this paper, our contributions are fourfold. First, we conduct the first systematic study on OSV. Second, we propose a lightweight detection tool against OSV, called OSV-Hunter. Third, we evaluate OSV-Hunter using a set of popular apps. We found that 74 apps implemented hybrid postMessage, and all these apps suffered from OSV, which might be exploited by adversaries to perform remote real-time microphone monitoring, data race, internal data manipulation, denial of service (DoS) attacks and so on. Several popular development frameworks, libraries (such as the Facebook React Native framework, and the Google cloud print library) and apps (such as Adobe Reader and WPS office) are impacted. Lastly, to mitigate OSV from the root, we design and implement three new postMessage APIs, called OSV-Free. Our evaluation shows that OSV-Free is secure and fast, and it is generic and resilient to the notorious Android fragmentation problem. We also demonstrate that OSV-Free is easy to use, by applying OSV-Free to harden the complex "Facebook React Native" framework. OSV-Free is open source, and its source code and more implementation and evaluation details are available online.

**\*\*\*\*\***

**IMPORTANT**

Surveylance: Automatically Detecting Online Survey Scams   
Amin Kharraz (University of Illinois Urbana-Champaign), William Robertson (Northeastern University), Engin Kirda (Northeastern University)

**Online surveys** are a popular mechanism for **performing market research** in exchange for monetary compensation. Unfortunately, fraudulent survey websites are similarly rising in popularity among cyber-criminals as a means for **executing social engineering attacks**. In addition to the sizable population of users that participate in online surveys as a secondary revenue stream, unsuspecting users who search the web for free content or access codes to commercial software can **also be exposed to survey scams**. This occurs through redirection to websites that ask the user to complete a survey in order to receive the promised content or a reward.  
  
In this paper, we present **SURVEYLANCE** , the first system that automatically **identifies survey scams** using **machine learning techniques**. Our evaluation demonstrates that SURVEYLANCE works well in practice by identifying 8,623 unique websites involved in online survey attacks. We show that SURVEYLANCE is suitable for assisting human analysts in survey scam detection at scale. Our work also provides the first systematic analysis of the survey scam ecosystem by investigating the capabilities of these services, mapping all the parties involved in the ecosystem, and quantifying the consequences to users that are exposed to these services. Our analysis reveals that a large number of **survey scams** are easily reachable through the Alexa top 30K websites, and expose users to a wide range of security issues including **identity fraud, deceptive advertisements, potentially unwanted programs (PUPs), malicious extensions, and malware**.

\*\*\*\*\*

**T-Fuzz: fuzzing by program transformation**   
Hui Peng (Purdue University), Yan Shoshitaishvili (Arizona State University), Mathias Payer (Purdue University)

Abstract-Fuzzing is a simple yet effective approach to discover software bugs utilizing randomly generated inputs. However, it is limited by coverage and cannot find bugs hidden in deep execution paths of the program because the randomly generated inputs fail complex sanity checks, e.g., checks on magic values, checksums, or hashes. To improve coverage, existing approaches rely on imprecise heuristics or complex input mutation techniques (e.g., symbolic execution or taint analysis) to bypass sanity checks. Our novel method tackles coverage from a different angle: by removing sanity checks in the target program. T-Fuzz leverages a coverage-guided fuzzer to generate inputs. Whenever the fuzzer can no longer trigger new code paths, a light-weight, dynamic tracing based technique detects the input checks that the fuzzer-generated inputs fail. These checks are then removed from the target program. Fuzzing then continues on the transformed program, allowing the code protected by the removed checks to be triggered and potential bugs discovered. Fuzzing transformed programs to find bugs poses two challenges: (1) removal of checks leads to over-approximation and false positives, and (2) even for true bugs, the crashing input on the transformed program may not trigger the bug in the original program. As an auxiliary post-processing step, T-Fuzz leverages a symbolic execution-based approach to filter out false positives and reproduce true bugs in the original program. By transforming the program as well as mutating the input, T-Fuzz covers more code and finds more true bugs than any existing technique. We have evaluated T-Fuzz on the DARPA Cyber Grand Challenge dataset, LAVA-M dataset and 4 real-world programs (pngfix, tiffinfo, magick and pdftohtml). For the CGC dataset, T-Fuzz finds bugs in 166 binaries, Driller in 121, and AFL in 105. In addition, found 3 new bugs in previously-fuzzed programs and libraries.

\*\*\*\*\*

**The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter**  
Nolen Scaife (University of Florida), Christian Peeters (University of Florida), Camilo Velez (University of Florida), Hanqing Zhao (University of Florida), Patrick Traynor (University of Florida), David Arnold (University of Florida)

Gift cards are an increasingly popular payment platform. Much like credit cards, gift cards rely on a magnetic stripe to encode account information. Unlike credit cards, however, the EMV standard is entirely infeasible for gift cards due to compatibility and cost. As such, much of the fraud that has plagued credit cards has started to move towards gift cards, resulting in billions of dollars of loss annually. In this paper, we present a system for detecting counterfeit magnetic stripe gift cards that does not require the original card to be measured at the time of manufacture. Our system relies on a phenomenon known as jitter, which is present on all ISO/IEC-standard magnetic stripe cards. Variances in bit length are induced by the card encoding hardware and are difficult and expensive to reduce. We verify this hypothesis with a high-resolution magneto-optical microscope, then build our detector using inexpensive, commodity card readers. We then partnered with Walmart to evaluate their gift cards and distinguished legitimate gift cards from our clones with up to 99.3% accuracy. Our results show that measurement and detection of jitter increases the difficulty for adversaries to produce undetectable counterfeits, thereby creating significant opportunity to reduce gift card fraud.

\*\*\*\*\*

**The Rise of the Citizen Developer: Assessing the Security Impact of Online App Generators**  
Marten Oltrogge (CISPA, Saarland University), Erik Derr (CISPA, Saarland University), Christian Stransky (CISPA, Saarland University), Yasemin Acar (Leibniz University Hannover), Sascha Fahl (Leibniz University Hannover), Christian Rossow (CISPA, Saarland University), Giancarlo Pellegrino (CISPA, Saarland University, Stanford University), Sven Bugiel (CISPA, Saarland University), Michael Backes (CISPA, Saarland University)

Mobile apps are increasingly created using online application generators (OAGs) that automate app development, distribution, and maintenance. These tools significantly lower the level of technical skill that is required for app development, which makes them particularly appealing to citizen developers, i.e., developers with little or no software engineering background. However, as the pervasiveness of these tools increases, so does their overall influence on the mobile ecosystem's security, as security lapses by such generators affect thousands of generated apps. The security of such generated apps, as well as their impact on the security of the overall app ecosystem, has not yet been investigated.   
  
We present the first comprehensive classification of commonly used OAGs for Android and show how to fingerprint uniquely generated apps to link them back to their generator. We thereby quantify the market penetration of these OAGs based on a corpus of 2,291,898 free Android apps from Google Play and discover that at least 11.1% of these apps were created using OAGs. Using a combination of dynamic, static, and manual analysis, we find that the services' app generation model is based on boilerplate code that is prone to reconfiguration attacks in 7/13 analyzed OAGs. Moreover, we show that this boilerplate code includes well-known security issues such as code injection vulnerabilities and insecure WebViews. Given the tight coupling of generated apps with their services' backends, we further identify security issues in their infrastructure. Due to the blackbox development approach, citizen developers are unaware of these hidden problems that ultimately put the end-users sensitive data and privacy at risk and violate the user's trust assumption. A particular worrisome result of our study is that OAGs indeed have a significant amplification factor for those vulnerabilities, notably harming the health of the overall mobile app ecosystem.

\*\*\*\*\*

**The Spyware Used in Intimate Partner Violence**   
Rahul Chatterjee (Cornell Tech), Periwinkle Doerfler (NYU), Hadas Orgad (Technion), Sam Havron (Cornell Univ), Jackeline Palmer (Hunter College), Diana Freed (Cornell Tech), Karen Levy (Cornell Tech), Nicola Dell (Cornell Tech), Damon McCoy (NYU), Thomas Ristenpart (Cornell Tech)

Survivors of intimate partner violence increasingly report that abusers install spyware on devices to track their location, monitor communications, and cause emotional and physical harm. To date there has been only cursory investigation into the spyware used in such intimate partner surveillance (IPS). We provide the first in-depth study of the IPS spyware ecosystem. We design, implement, and evaluate a measurement pipeline that combines web and app store crawling with machine learning to find and label apps that are potentially dangerous in IPS contexts. Ultimately we identify several hundred such IPS-relevant apps. While we find dozens of overt spyware tools, the majority are "dual-use" apps - they have a legitimate purpose (e.g., child safety or anti-theft), but are easily and effectively repurposed for spying on a partner. We document that a wealth of online resources are available to educate abusers about exploiting apps for IPS. We also show how some dual-use app developers are encouraging their use in IPS via advertisements, blogs, and customer support services. We analyze existing anti-virus and anti-spyware tools, which universally fail to identify dual-use apps as a threat.

\*\*\*\*\*

**Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users**  
Kiron Lebeck (University of Washington), Kimberly Ruth (University of Washington), Tadayoshi Kohno (University of Washington), Franziska Roesner (University of Washington)

Immersive augmented reality (AR) technologies are becoming a reality. Prior works have identified security and privacy risks raised by these technologies, primarily considering individual users or AR devices. However, we make two key observations: (1) users will not always use AR in isolation, but also in ecosystems of other users, and (2) since immersive AR devices have only recently become available, the risks of AR have been largely hypothetical to date.   
To provide a foundation for understanding and addressing the security and privacy challenges of emerging AR technologies, grounded in the experiences of real users, we conduct a qualitative lab study with an immersive AR headset, the Microsoft HoloLens. We conduct our study in pairs - 22 participants across 11 pairs - wherein participants engage in paired and individual (but physically co-located) HoloLens activities. Through semi-structured interviews, we explore participants' security, privacy, and other concerns, raising key findings. For example, we find that despite the HoloLens's limitations, participants were easily immersed, treating virtual objects as real (e.g., stepping around them for fear of tripping). We also uncover numerous security, privacy, and safety concerns unique to AR (e.g., deceptive virtual objects misleading users about the real world), and a need for access control among users to manage shared physical spaces and virtual content embedded in those spaces. Our findings give us the opportunity to identify broader lessons and key challenges to inform the design of emerging single- and multi-user AR technologies.

\*\*\*\*\*

**Tracking Certificate Misissuance in the Wild**  
Deepak Kumar (University of Illinois, Urbana-Champaign), Zhengping Wang (University of Illinois, Urbana-Champaign), Matthew Hyder (University of Illinois, Urbana-Champaign), Joseph Dickinson (University of Illinois, Urbana-Champaign), Gabrielle Beck (University of Michigan), David Adrian (University of Michigan), Joshua Mason (University of Illinois, Urbana-Champaign), Zakir Durumeric (University of Michigan), J. Alex Halderman (University of Michigan), Michael Bailey (University of Illinois, Urbana-Champaign)

Certificate Authorities (CAs) regularly make mechanical errors when issuing certificates. To quantify these errors, we introduce ZLint, a certificate linter that codifies the policies set forth by the CA/Browser Forum Baseline Requirements and RFC 5280 that can be tested in isolation. We run ZLint on browser-trusted certificates in Censys and systematically analyze how well CAs construct certificates. We find that the number errors has drastically reduced since 2012. In 2017, only 0.02% of certificates have errors. However, this is largely due to a handful of large authorities that consistently issue correct certificates. There remains a long tail of small authorities that regularly issue non-conformant certificates. We further find that issuing certificates with errors is correlated with other types of mismanagement and for large authorities, browser action. Drawing on our analysis, we conclude with a discussion on how the community can best use lint data to identify authorities with worrisome organizational practices and ensure long-term health of the Web PKI.

\*\*\*\*\*

**IMPORTANT**

**Tracking Ransomware End-to-end**  
Danny Yuxing Huang (Princeton University), Maxwell Matthaios Aliapoulios (New York University), Vector Guo Li (University of California, San Diego), Luca Invernizzi (Google), Elie Bursztein (Google), Kylie McRoberts (Google), Jonathan Levin (Chainalysis), Kirill Levchenko (University of California, San Diego), Alex C. Snoeren (University of California, San Diego), Damon McCoy (New York University)

**Ransomware is a type of malware that encrypts the files of infected hosts and demands payment, often in a crypto-currency like Bitcoin.** In this paper, we create a measurement framework that we use to perform a large-scale, two-year, end-to-end measurement of ransomware payments, victims, and operators. By combining an array of data sources, including ransomware binaries, seed ransom payments, victim telemetry from infections, and a large database of bitcoin addresses annotated with their owners, we sketch the outlines of this burgeoning ecosystem and associated third-party infrastructure. **In particular, we are able to trace the financial transactions, from the acquisition of bitcoins by victims, through the payment of ransoms, to the cash out of bitcoins by the ransomware operators.** We find that many ransomware operators cashed out using BTC-e, a now-defunct Bitcoin exchange. In total we are able to track over **$16 million USD** in likely ransom payments made by **19,750 potential victims during a two-year period**. While our study focuses on ransomware, our methods are potentially applicable to other cybercriminal operations that have similarly adopted Bitcoin as their payment channel.

\*\*\*\*\*

**IMPORTANT**

**Understanding Linux Malware**  
Emanuele Cozzi (Eurecom), Mariano Graziano (Cisco Systems, Inc.), Yanick Fratantonio (Eurecom), Davide Balzarotti (Eurecom)

For the past two decades, the security community has been fighting malicious programs for Windows-based operating systems. However, the recent surge in adoption of **embedded devices and the IoT revolution are rapidly changing the malware landscape**. Embedded devices are profoundly different than traditional personal computers. In fact, while personal computers run predominantly on x86-flavored architectures, embedded systems rely on **a variety of different architectures**. In turn, this aspect causes a large number of these systems to run some variants of the Linux operating system, pushing malicious actors to give birth to "**Linux malware**."  
  
To the best of our knowledge, there is currently no comprehensive study attempting to characterize, analyze, and understand Linux malware. The majority of resources on the topic are available as **sparse reports often published as blog posts**, while the few systematic studies focused on the analysis of **specific families of malware (e.g., the Mirai botnet) mainly by looking at their network-level behavior, thus leaving the main challenges of analyzing Linux malware unaddressed.**  
  
This work constitutes the first step towards filling this gap. After a systematic exploration of the challenges involved in the process, we present the design and implementation details of **the first malware analysis pipeline specifically tailored for Linux malware**. We then present the results of the first large-scale measurement study conducted on **10,548 malware samples (collected over a time frame of one year)** documenting detailed statistics and insights that can help directing future work in the area.

\*\*\*\*\*

**When Your Fitness Tracker Betrays You: Quantifying the Predictability of Biometric Features Across Contexts**  
Simon Eberz (University of Oxford), Giulio Lovisotto (University of Oxford), Andrea Patanè (University of Oxford), Marta Kwiatkowska (University of Oxford), Vincent Lenders (armasuisse), Ivan Martinovic (University of Oxford)

Attacks on behavioral biometrics have become increasingly popular. Most research has been focused on presenting a previously obtained feature vector to the biometric sensor, often by the attacker training themselves to change their behavior to match that of the victim. However, obtaining the victim's biometric information may not be easy, especially when the user's template on the authentication device is adequately secured. As such, if the authentication device is inaccessible, the attacker may have to obtain data elsewhere. In this paper, we present an analytic framework that enables us to measure how easily features can be predicted based on data gathered in a different context (e.g., different sensor, performed task or environment). This framework is used to assess how resilient individual features or entire biometrics are against such cross-context attacks. In order to be able to compare existing biometrics with regard to this property, we perform a user study to gather biometric data from 30 participants and ?ve biometrics (ECG, eye movements, mouse movements, touchscreen dynamics and gait) in a variety of contexts. We make this dataset publicly available online. Our results show that many attack scenarios are viable in practice as features are easily predicted from a variety of contexts. All biometrics include features that are particularly predictable (e.g., amplitude features for ECG or curvature for mouse movements). Overall, we observe that cross-context attacks on eye movements, mouse movements and touchscreen inputs are comparatively easy while ECG and gait exhibit much more chaotic cross-context changes.

\*\*\*\*\*

**vRAM: Faster Verifiable RAM With Program-Independent Preprocessing**  
Yupeng Zhang (University of Maryland), Daniel Genkin (University of Maryland and University of Pennsylvania), Jonathan Katz (University of Maryland), Dimitrios Papadopoulos (Hong Kong University of Science and Technology), Charalampos Papamanthou (University of Maryland)

We study the problem of verifiable computation (VC) for RAM programs, where a computationally weak verifier outsources the execution of a program to a powerful (but untrusted) prover. Existing efficient implementations of VC protocols require an expensive preprocessing phase that binds the parties to a single circuit. (While there are schemes that avoid preprocessing entirely, their performance remains significantly worse than constructions with preprocessing.) Thus, a prover and verifier are forced to choose between two approaches: (1) Allow verification of arbitrary RAM programs, at the expense of efficiency, by preprocessing a universal circuit which can handle all possible instructions during each CPU cycle; or (2) Sacrifice expressiveness by preprocessing an efficient circuit which is tailored to the verification of a single specific RAM program.  
  
We present vRAM, a VC system for RAM programs that avoids both the above drawbacks by having a preprocessing phase that is entirely circuit-independent (other than an upper bound on the circuit size). During the proving phase, once the program to be verified and its inputs are chosen, the circuit-independence of our construction allows the parties to use a smaller circuit tailored to verifying the specific program on the chosen inputs, i.e., without needing to encode all possible instructions in each cycle. Moreover, our construction is the first with asymptotically optimal prover overhead; i.e., the work of the prover is a constant multiplicative factor of the time to execute the program.  
  
Our experimental evaluation demonstrates that vRAM reduces the prover's memory consumption by 55-110x and its running time by 9-30x compared to existing schemes with universal preprocessing. This allows us to scale to RAM computations with more than 2 million CPU cycles, a 65x improvement compared to the state of the art. Finally, vRAM has performance comparable to (and sometimes better than) the best existing scheme with program-specific preprocessing despite the fact that the latter can deploy program-specific optimizations (and has to pay a separate preprocessing cost for every new program).

\*\*\*\*\*

**xJsnark: A Framework for Efficient Verifiable Computation**  
Ahmed Kosba (University of Maryland), Charalampos Papamanthou (University of Maryland), Elaine Shi (Cornell University)

Many cloud and cryptocurrency applications rely on verifying the integrity of outsourced computations, in which a verifier can efficiently verify the correctness of a computation made by an untrusted prover. State-of-the-art protocols for verifiable computation require that the computation task be expressed as arithmetic circuits, and the number of multiplication gates in the circuit is the primary metric that determines performance. At the present, a programmer could rely on two approaches for expressing the computation task, either by composing the circuits directly through low-level development tools; or by expressing the computation in a high-level program and rely on compilers to perform the program-to-circuit transformation. The former approach is difficult to use but on the other hand allows an expert programmer to perform custom optimizations that minimize the resulting circuit. In comparison, the latter approach is much more friendly to non-specialist users, but existing compilers often emit suboptimal circuits.  
  
We present xJsnark, a programming framework for verifiable computation that aims to achieve the best of both worlds: offering programmability to non-specialist users, and meanwhile automating the task of circuit size minimization through a combination of techniques. Specifically, we present new circuit-friendly algorithms for frequent operations that achieve constant to asymptotic savings over existing ones; various globally aware optimizations for short- and long- integer arithmetic; as well as circuit minimization techniques that allow us to reduce redundant computation over multiple expressions. We illustrate the savings in different applications, and show the framework's applicability in developing large application circuits, such as ZeroCash, while minimizing the circuit size as in low-level implementations.