Files\\sec14\_full\_proceedingsEpub - § 14 references coded [ 0.03% Coverage]

Reference 1 - 0.01% Coverage

Information privacy law in the U.S. and many other countries is based on the free market notice-andchoice principle [28].

Reference 2 - 0.01% Coverage

Internet-wide scanning is a powerful technique used by researchers to study and measure the Internet and by attackers to discover vulnerable hosts en masse.

Reference 3 - 0.01% Coverage

Traditionally, digital investigations have aimed to recover evidence of a cyber-crime or perform incident response via analysis of non-volatile storage.

Reference 4 - 0.01% Coverage

In today’s practice of analyzing malware [3, 14, 16, 26, 23], system virtual machines are widely used to facilitate fine-grained dissection of malware functionalities (e.g., Anubis [4], TEMU [6, 24], and Bochs [17]).

Reference 5 - 0.01% Coverage

Code reuse attacks manage to re-direct control flow through a program with the intent of imposing malicious behavior on an otherwise benign program.

Reference 6 - 0.01% Coverage

Civil society organizations (CSOs), working on human rights issues around the globe, face a spectrum of politically-motivated information security threats that seek to deny (e.g. Internet filtering, denialof-service attacks), manipulate (e.g. website defacements) or monitor (e.g. targeted malware) information related to their work.

Reference 7 - 0.01% Coverage

Online criminal activities take many different forms, ranging from advertising counterfeit goods through spam email [21], to hosting “drive-by-downloads” services [29] that surreptitiously install malicious software (“malware”) on the victim machine, to distributed denial-of-service attacks [27], to only name a few.

Reference 8 - 0.01% Coverage

To reduce the memory footprint of a system, the system software shares identical memory pages between processes running on the system.

Reference 9 - 0.01% Coverage

Verifiable Computation (VC) is a cryptographic protocol that allows a client to outsource expensive computation tasks to a worker (e.g., a cloud server), such that the client can verify the result of the computation in less time than that required to perform the computation itself.

Reference 10 - 0.01% Coverage

Private set intersection (PSI) allows two parties P1 and P2 holding sets X and Y, respectively, to identify the intersection X Y without revealing any information about elements that are not in the intersection.

Reference 11 - 0.01% Coverage

Secure two-party computation allows two parties to process their sensitive data in such a way that its privacy is protected.

Reference 12 - 0.01% Coverage

Mobile social applications discover nearby users and provide services based on user activity (what the user is doing) and context (who and what is nearby).

Reference 13 - 0.01% Coverage

Processes retrieve a variety of resources from the operating system to function.

Reference 14 - 0.01% Coverage

Third-party libraries provide a convenient way for mobile application developers to integrate external services in the application code base.

Files\\sec15\_full\_proceedingsEpub - § 16 references coded [ 0.03% Coverage]

Reference 1 - 0.01% Coverage

Taint analysis is a kind of program analysis that tracks some selected data of interest (taint seeds), e.g., data originated from untrusted sources, propagates them along program execution paths according to a customized policy (taint   
propagation policy), and then checks the taint status at certain critical location (taint sinks).

Reference 2 - 0.01% Coverage

Redaction of sensitive information from documents has been used since ancient times as a means of concealing and removing secrets from texts intended for public release.

Reference 3 - 0.01% Coverage

In a memory error exploit, attackers often seek to execute arbitrary malicious code, which gives them the ultimate freedom in perpetrating damage with the victim program’s privileges.

Reference 4 - 0.01% Coverage

HMAC is a cryptographic authentication algorithm, the “Keyed-Hash Message Authentication Code,” widely used in conjunction with the SHA-256 cryptographic hashing primitive.

Reference 5 - 0.01% Coverage

Anonymity systems aim to protect user identities from untrusted destinations and third parties on the Internet.

Reference 6 - 0.01% Coverage

A provenance-aware system automatically gathers and reports metadata that describes the history of each object being processed on the system.

Reference 7 - 0.01% Coverage

Mobile platform permission models regulate how applications access certain resources, such as users’ personal information or sensor data (e.g., camera, GPS, etc.).

Reference 8 - 0.01% Coverage

Private set intersection (PSI) allows two parties P1 and P2 with respective input sets X and Y to compute the intersection X ∩ Y of their sets without revealing any information but the intersection itself.

Reference 9 - 0.01% Coverage

Binary analysis enables many useful applications in computer security, given the plethora of possible situations in which the original high-level source code is unavailable, has been lost, or is otherwise inconvenient to use.

Reference 10 - 0.01% Coverage

In computer security, many techniques and applications depend on binary reverse engineering, i.e., analyzing and retrofitting software binaries with the source code unavailable.

Reference 11 - 0.01% Coverage

With large touch screens, modern mobile devices typically   
feature software keyboards to allow users to enter text input.

Reference 12 - 0.01% Coverage

The same-origin policy (SOP) is a corner stone of web security, guarding the web content of one domain from the access from another domain.

Reference 13 - 0.01% Coverage

Sensors are devices that detect physical properties in nature and convert them to   
quantitative values for actuators and control systems.

Reference 14 - 0.01% Coverage

Public cloud computing offers easy access to relatively cheap compute and storage resources.

Reference 15 - 0.01% Coverage

In the PC world, computer multitasking means multiple processes are running at the same period of time.

Reference 16 - 0.01% Coverage

Malware sandboxes are automated dynamic analysis tools that execute samples in an isolated and instrumented environment.

Files\\sec16\_full\_proceedingsEpub - § 18 references coded [ 0.03% Coverage]

Reference 1 - 0.01% Coverage

Security of software systems is built upon correctly implemented and executed hardware-software contracts.

Reference 2 - 0.01% Coverage

Rootkits are used by attackers for malicious activities on compromised machines by running software without being detected [47].

Reference 3 - 0.01% Coverage

Code-reuse attacks, such as Return-Oriented Programming (ROP), enable an attacker to bypass Execute-XOR-Write (X W) policies by suitably chaining existing small code fragments (so-called gadgets).

Reference 4 - 0.01% Coverage

Botnets are networks of malware-affected machines (bots) that are remotely controlled by an adversary (botmaster) through a command and control (C&C) communication channel.

Reference 5 - 0.01% Coverage

Bitcoin [47] is a decentralized cryptocurrency providing an open, selfregulating alternative to classic currencies managed by central authorities such as banks.

Reference 6 - 0.01% Coverage

Secure two-party computation (2PC) allows mutually distrusting parties to   
perform a computation on their combined inputs, while revealing only the result.

Reference 7 - 0.01% Coverage

A Version Control System (VCS) is a crucial component of any large   
software development project, presenting to developers fundamental features that aid in the improvement and maintenance of a project’s codebase.

Reference 8 - 0.01% Coverage

The Universal Serial Bus (USB) provides an easy-to-use, hot-pluggable architecture for attaching external devices ranging from cameras to network interfaces to a single host computer.

Reference 9 - 0.01% Coverage

Web browsers download and run JavaScript code from sites a user visits as well as third-party sites like ad networks, granting that code access to system resources through the DOM.

Reference 10 - 0.01% Coverage

The Internet of Things (IoT) consists of several data-producing devices (e.g., activity trackers, presence detectors, door state sensors), and data-consuming apps that optionally actuate physical devices.

Reference 11 - 0.01% Coverage

Machine learning (ML) aims to provide automated extraction of insights from data by means of a predictive model.

Reference 12 - 0.01% Coverage

Online data retrieval systems typically serve a searchable corpus of documents, web pages, blogs, personal emails, online social network (OSN) profiles and posts, along with real-time microblogs, stock and news tickers.

Reference 13 - 0.01% Coverage

The goal of searchable encryption (SE) is to enable a client to perform keyword searches over encrypted files stored on an untrusted server while still guaranteeing some measure of privacy for both the files themselves as well as the client’s queries.

Reference 14 - 0.01% Coverage

Potentially unwanted programs (PUP) are a category of undesirable software that includes adware and rogue software (i.e., rogueware).

Reference 15 - 0.01% Coverage

Current network security devices classify large amounts of the malicious network traffic and report the results in many individually-identified incidents, some of which are false alerts.

Reference 16 - 0.01% Coverage

Third-party web tracking is the practice by which third parties like advertisers, social media widgets, and website analytics engines—embedded in the first party sites that users visit directly—re-identify users across domains as they browse the web.

Reference 17 - 0.01% Coverage

Android’s application framework—i.e., the middleware code that implements the bulk of the Android SDK on top of which Android apps are developed—is responsible for the enforcement of Android’s permission-based privilege model and as such is also a popular subject of recent research on security extensions to the Android OS.

Reference 18 - 0.01% Coverage

In a Sybil attack, an attacker controls many virtual identities to obtain disproportionately large influence in a network.