Files\\sec14\_full\_proceedingsEpub - § 8 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

Mobile apps frequently demand access to private information.

Reference 2 - 0.01% Coverage

Today’s consumer mobile platforms such as Android and iOS manage large ecosystems of untrusted third-party applications called “apps.”

Reference 3 - 0.01% Coverage

Users are often advised or required to choose passwords that comply with certain policies.

Reference 4 - 0.01% Coverage

Binary analysis has many security applications.

Reference 5 - 0.01% Coverage

Software bugs are expensive.

Reference 6 - 0.01% Coverage

Consumer operating systems are changing.

Reference 7 - 0.01% Coverage

The confidentiality and integrity of applications’ GUI content are well recognized to be critical in achieving end-to-end security [1–4].

Reference 8 - 0.01% Coverage

Modern smartphones and mobile devices have many sensors that enable rich user experience.

Files\\sec15\_full\_proceedingsEpub - § 16 references coded [ 0.02% Coverage]

Reference 1 - 0.01% Coverage

The majority of modern commerce relies on cashless payment systems.

Reference 2 - 0.01% Coverage

Software bugs pervade every level of the modern software stack, degrading both stability and security.

Reference 3 - 0.01% Coverage

TLS in all current versions allows RC4 to be used as its bulk encryption mechanism.

Reference 4 - 0.01% Coverage

Attacking software systems by exploiting memory-corruption vulnerabilities is one of the most common attack methods today according to the list of Common Vulnerabilities and Exposures.

Reference 5 - 0.01% Coverage

Many computing systems generate data with graph structure, e.g., social networks, collaboration networks, and email networks [2–4].

Reference 6 - 0.01% Coverage

Operating system integrity relies on the correctness of 1) trusted computing base (TCB) code and 2) access control policy protecting the TCB code and OS resources.

Reference 7 - 0.01% Coverage

Software tokens on modern phones are replacing dedicated hardware tokens in two-factor authentication (2FA) mechanisms.

Reference 8 - 0.01% Coverage

Online services, such as online social networks (OSNs), webmail, and blogs, are frequently abused by cybercriminals.

Reference 9 - 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 10 - 0.01% Coverage

Mobile users are increasingly aware of the privacy threats caused by apps’ access of their location [12, 42].

Reference 11 - 0.01% Coverage

Mobile users run apps for various purposes, and exhibit very different or even unrelated behaviors in running different apps.

Reference 12 - 0.01% Coverage

Modern web-based software applications rely on a number of core network services that provide the basic communication between software components.

Reference 13 - 0.01% Coverage

In spite of extensive industrial and academic efforts (e.g., [3, 41, 42]), distributed denial-of-service (DDoS) attacks continue to plague the Internet.

Reference 14 - 0.01% Coverage

Security-aware organizations take various steps to prevent possible theft or leakage of sensitive information.

Reference 15 - 0.01% Coverage

Covert and side channels have for a long time remained an open threat to information flow control and isolation techniques in a variety of contexts including cloud and mobile computing [50, 71, 76].

Reference 16 - 0.01% Coverage

Recent data breaches, such as those at Target [35], JP Morgan [25], and Home Depot [49] highlight the increasing social and economic impact of such cyber incidents.

Files\\sec16\_full\_proceedingsEpub - § 10 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

TCP and networking stacks have recently been shown to leak various types of information via side channels, to a blind off-path attacker [22, 14, 12, 21, 11, 29, 5].

Reference 2 - 0.01% Coverage

The last decade in cryptography has seen the birth of numerous constructions of cryptosystems based on lattice problems, achieving functionalities that were previously unreachable (e.g., fully homomorphic cryptography [38]).

Reference 3 - 0.01% Coverage

Most modern malware infections happen via the browser, typically triggered   
by social engineering [9] or drive-by download attacks [33].

Reference 4 - 0.01% Coverage

The Network Time Protocol (NTP) is one of the Internet’s oldest protocols, dating back to RFC 958 [15] published in 1985.

Reference 5 - 0.01% Coverage

In recent years, commodity CPU architectures have started to offer built-in features for trusted computing.

Reference 6 - 0.01% Coverage

Today’s systems rely on an operating system kernel, or a hypervisor (such as Linux or Xen, respectively) for software isolation.

Reference 7 - 0.01% Coverage

The RSA key pair generation process is a crucial part of RSA algorithm usage, and there are many existing (and sometimes conflicting) recommendations regarding how to select suitable primes p and q [11, 13, 14, 17, 18] to be later used to compute the private key and public modulus.

Reference 8 - 0.01% Coverage

For several decades, car keys have been used to physically secure vehicles.

Reference 9 - 0.01% Coverage

Modern telephony systems include a wide array of end-user devices.

Reference 10 - 0.01% Coverage

When vendors, such as Samsung, LG and HTC, put Android AOSP OS on their devices, they usually conduct extensive customization on the system.