Files\\sec14\_full\_proceedingsEpub - § 20 references coded [ 0.03% Coverage]

Reference 1 - 0.01% Coverage

A continuously increasing number of users now utilize mobile devices [2] to interact with public cloud services (PCS) (e.g. Gmail, Outlook, and WhatsApp) as an essential part of their daily lives.

Reference 2 - 0.01% Coverage

We live in a “big data” world.

Reference 3 - 0.01% Coverage

As one of the most popular mobile platforms, Apple iOS has been successful in preventing the distribution of malicious apps [23, 32].

Reference 4 - 0.01% Coverage

Embedded systems are omnipresent in our everyday life.

Reference 5 - 0.01% Coverage

Tor [21] is the most popular overlay network for communicating anonymously online.

Reference 6 - 0.01% Coverage

Privacy technologies are becoming more popular: Tor, a low-latency anonymity network, currently has 500,000 daily users and the number has been growing [21].

Reference 7 - 0.01% Coverage

Thousands of new domain names are registered daily that at first glance do not have completely legitimate uses: some contain random characters (possibly used by miscreants [23]), are a composite of two completely unrelated words (possibly used in spam [17]), contain keywords of highly-visible recent events (ex. hillaryclingon.com for political phishing in 2008 [28]) or are similar to other, typically well-known, domain names (ex. twtter.com [27, 32]).

Reference 8 - 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 9 - 0.01% Coverage

In response to evolving terrorist threats, including nonmetallic explosive devices and weapons, the U.S. Transportation Security Administration (TSA) has adopted advanced imaging technology (AIT), also known as whole-body imaging, as the primary passenger screening method at nearly 160 airports nationwide [50].

Reference 10 - 0.01% Coverage

The widespread adoption of DEP, which ensures that all writable pages in memory are nonexecutable, has largely killed classic code injection attacks.

Reference 11 - 0.01% Coverage

Today, runtime attacks remain one of the most prevalent attack vectors against software programs.

Reference 12 - 0.01% Coverage

Modern protection mechanisms like data execution protection (DEP) [2], address space layout randomization (ASLR) [26] and stack smashing protection (SSP) [9] are now available on most general-purpose operating systems.

Reference 13 - 0.01% Coverage

With the proliferation of Web services, ordinary users are setting up authentication credentials with   
a large number of sites.

Reference 14 - 0.01% Coverage

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

Reference 15 - 0.01% Coverage

Single Sign-On (SSO) services are increasingly used to implement authentication for modern applications.

Reference 16 - 0.01% Coverage

Passwords are the most widely used credentials for authenticating Web users around the world, including the users that do not speak English.

Reference 17 - 0.01% Coverage

Due to the growth in online services, many users now manage dozens of password-protected accounts.

Reference 18 - 0.01% Coverage

All major web browsers today support broad extension ecosystems that allow third parties to install a wide range of modified behavior or additional functionality.

Reference 19 - 0.01% Coverage

Ever since its initial discovery in the year 2000 [6], Cross-Site Scripting (XSS) is an ever-present security concern in Web applications.

Reference 20 - 0.01% Coverage

Web applications increasingly employ the TLS protocol to secure HTTP communication (i.e.,   
HTTP over TLS, or HTTPS) between a user’s browser and the web server.

Files\\sec15\_full\_proceedingsEpub - § 15 references coded [ 0.02% Coverage]

Reference 1 - 0.01% Coverage

The programming paradigm popularly known as object-oriented programming (OOP) is widely used for developing large and complex applications because it encapsulates the implementation details of data structures and algorithms into objects; this in turn facilitates cleaner software design, better code reuse, and easier software maintenance.

Reference 2 - 0.01% Coverage

RC4 is (still) one of the most widely used stream ciphers.

Reference 3 - 0.01% Coverage

While cryptocurrency has been studied since the 1980s [22, 25, 28], bitcoin is the first to see widespread adoption.

Reference 4 - 0.01% Coverage

TLS, short for Transport Layer Security, is widely used to secure network   
connections, for example in HTTPS.

Reference 5 - 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 6 - 0.01% Coverage

Android is the major platform for mobile users and mobile app developers.

Reference 7 - 0.01% Coverage

Billions of users now depend on online services for sensitive communication.

Reference 8 - 0.01% Coverage

In recent decades, improved digital communication technologies have reduced barriers to journalism worldwide.

Reference 9 - 0.01% Coverage

With cloud computing and storage gaining popularity, privacy of users’ sensitive data has become a large concern.

Reference 10 - 0.01% Coverage

Most of the over 2 billion Internet users [1] regularly access the World Wide Web, performing a wide variety of tasks that range from searching for information to the purchase of goods and online banking transactions.

Reference 11 - 0.01% Coverage

Cellular networks provide digital communications for more than five billion people around the globe.

Reference 12 - 0.01% Coverage

Entering the era of cloud computing, Infrastructure as a Service(IaaS) has become prevalent in providing Information Technology (IT) support.

Reference 13 - 0.01% Coverage

Smartphones have become the dominant kind of end-user devices with more units sold than traditional PCs.

Reference 14 - 0.01% Coverage

Remote malware downloads currently represent the most common infection vector.

Reference 15 - 0.01% Coverage

The number of software vulnerabilities discovered has grown significantly in recent years.

Files\\sec16\_full\_proceedingsEpub - § 16 references coded [ 0.02% Coverage]

Reference 1 - 0.01% Coverage

Passwords remain a key component of most online authentication systems [32], but the quest to replace them [20] is an active research area with a long history of false starts and renewed enthusiasm (recently e.g., [33]).

Reference 2 - 0.01% Coverage

Text passwords are currently the most common form of authentication, and they   
promise to continue to be so for the foreseeable future [53].

Reference 3 - 0.01% Coverage

Public key cryptography is a common method for authentication in secure endto-end communication and has been a part of the Internet throughout the last two decades [7, 11].

Reference 4 - 0.01% Coverage

Over the past few years, face authentication systems have become increasingly   
popular as an enhanced security feature in both mobile devices and desktop computers.

Reference 5 - 0.01% Coverage

Voice interfaces to computer systems are becoming ubiquitous, driven in part by their ease of use and in part by decreases in the size of modern mobile and wearable devices that make physical interaction difficult.

Reference 6 - 0.01% Coverage

Due to the popularity of cloud services, multiple tenants sharing the same   
physical server through different virtual machines (VMs) is now a common situation.

Reference 7 - 0.01% Coverage

The past several years have seen widespread adoption of end-to-end encrypted text messaging protocols.

Reference 8 - 0.01% Coverage

In the last decennia, Wi-Fi became a de facto standard for medium-range wireless communications.

Reference 9 - 0.01% Coverage

TLS [13] is one of the main protocols responsible for transport security on the modern Internet.

Reference 10 - 0.01% Coverage

Content sharing peer-to-peer (P2P) systems, especially P2P file-sharing applications such as BitTorrent [1], Storj [2] and Freenet [3] are popular among users for sharing files on the Internet.

Reference 11 - 0.01% Coverage

The large-scale detection of vulnerabilities in Web applications has become significantly more common over the course of the last years.

Reference 12 - 0.01% Coverage

Since their introduction in the 80s [16], zero-knowledge (ZK) arguments have been one of the main building blocks in the design of complex cryptographic protocols.

Reference 13 - 0.01% Coverage

Most efficient implementations for secure two-party computation in the semi-   
honest setting rely on garbled circuits.

Reference 14 - 0.01% Coverage

As smartphones become more pervasive in society, they are also increasingly involved in cyber and real world crimes.

Reference 15 - 0.01% Coverage

Bluetooth Low Energy (BLE) [4] has emerged as the de facto communication   
protocol in the new computing paradigm of the Internet of Things (IoTs) [8, 9, 15, 23, 24, 39].

Reference 16 - 0.01% Coverage

Since the first sequencing of the human genome in 2001, tens of thousands of   
genomes and over a million genotypes have been sequenced.