Files\\sec14\_full\_proceedingsEpub - § 12 references coded [ 0.02% Coverage]

Reference 1 - 0.01% Coverage

In recent years, technical advances have enabled inexpensive, high-fidelity molecular analyses that characterize the genetic make-up of an individual.

Reference 2 - 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 3 - 0.01% Coverage

Distributed Denial-of-Service (DDoS) attacks have been known since many years [8, 9, 24, 34] and they still constitute an important problem today.

Reference 4 - 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 5 - 0.01% Coverage

Repressive governments have deployed increasingly sophisticated technology to block disfavored Internet content [5, 50].

Reference 6 - 0.01% Coverage

The malware threat landscape is continuously evolving.

Reference 7 - 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 8 - 0.01% Coverage

In the last few years, a new class of cyber attacks has emerged that is more targeted at individuals and organizations.

Reference 9 - 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.

Reference 10 - 0.01% Coverage

Over the last decade, the sophistication and technical level of malicious software (malware) has increased dramatically.

Reference 11 - 0.01% Coverage

Although the operating system (OS) kernel has always been an appealing target, until recently attackers focused mostly on the exploitation of vulnerabilities in server and client applications— which often run with administrative privileges—as they are (for the most part) less complex to analyze and easier to compromise.

Reference 12 - 0.01% Coverage

Consumer operating systems are changing.

Files\\sec15\_full\_proceedingsEpub - § 9 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

For years, researchers have been working on methods to take over or disrupt the command-and-control (C&C) infrastructure of botnets

Reference 2 - 0.01% Coverage

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

Reference 3 - 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 4 - 0.01% Coverage

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

Reference 5 - 0.01% Coverage

In the thirty years since Yao’s seminal paper [34], Secure Multiparty Computation (MPC) and Secure Two-Party Computation (TPC) have transitioned from purely theoretic constructions to practical tools.

Reference 6 - 0.01% Coverage

Browsers have evolved over recent years to mediate a wealth of user   
interactions with sensitive data.

Reference 7 - 0.01% Coverage

Since the first widely-exploited buffer overflow used by the 1998 Morris worm [27], the prevention, exploitation, and mitigation of memory corruption vulnerabilities have occupied the time of security researchers and cybercriminals alike.

Reference 8 - 0.01% Coverage

Since its beginning in the early nineties, the Web evolved from a mechanism to publish and link static documents into a sophisticated platform for distributed Web applications.

Reference 9 - 0.01% Coverage

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

Files\\sec16\_full\_proceedingsEpub - § 14 references coded [ 0.02% Coverage]

Reference 1 - 0.01% Coverage

Despite years of study, memory corruption vulnerabilities still lead to controlflow hijacking attacks today.

Reference 2 - 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 3 - 0.01% Coverage

Over the last few years there have been numerous reports of ISPs that alter or   
proxy their customers’ traffic, including, for example, CMA Communications in 2013 [7], Comcast in 2012 [19], Mediacom in 2011 [10], WOW! in 2008 [31], and Rogers in 2007 [36].

Reference 4 - 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 5 - 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 6 - 0.01% Coverage

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

Reference 7 - 0.01% Coverage

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

Reference 8 - 0.01% Coverage

In recent years, unwanted software has risen to the forefront of threats facing users.

Reference 9 - 0.01% Coverage

Starting from Denning’s seminal work in 1986 [9], intrusion detection has evolved into a number of different approaches.

Reference 10 - 0.01% Coverage

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

Reference 11 - 0.01% Coverage

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

Reference 12 - 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 13 - 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 14 - 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.