Files\\sec14\_full\_proceedingsEpub - § 9 references coded [ 0.03% Coverage]

Reference 1 - 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 2 - 0.01% Coverage

On September 5, 2013, the New York Times [23], the Guardian [3] and ProPublica [16] reported the existence of a secret National Security Agency SIGINT Enabling Project with the mission to “actively [engage] the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products’ designs.”

Reference 3 - 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 4 - 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 5 - 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 6 - 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 7 - 0.01% Coverage

Binary analysis is an essential security capability with extensive applications, including protecting binaries with control flow integrity (CFI) [1], extracting binary code sequences from malware [9], and hot patching vulnerabilities [25].

Reference 8 - 0.01% Coverage

As popular applications rely on personal, privacy-sensitive information about users, factors such as legal regulations, industry self-regulation, and a growing body of privacy-conscious users all pressure developers to respond to demands for privacy.

Reference 9 - 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.

Files\\sec15\_full\_proceedingsEpub - § 1 reference coded [ 0.01% 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.

Files\\sec16\_full\_proceedingsEpub - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 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.