Files\\sec14\_full\_proceedingsEpub - § 14 references coded [ 0.02% Coverage]

Reference 1 - 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 2 - 0.01% Coverage

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

Reference 3 - 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 4 - 0.01% Coverage

Today’s computing networks and services are extremely complex systems with unpredictable interactions between numerous moving parts.

Reference 5 - 0.01% Coverage

Video is ineffably compelling.

Reference 6 - 0.01% Coverage

The battle for the living room is in full swing.

Reference 7 - 0.01% Coverage

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

Reference 8 - 0.01% Coverage

Computer security research devotes extensive efforts to protecting individuals against indiscriminate, large-scale attacks such as those used by cybercriminals.

Reference 9 - 0.01% Coverage

The dismissal of human memory by the security community reached the point of parody long ago.

Reference 10 - 0.01% Coverage

Public infrastructure-as-a-service (IaaS) clouds enable the increasingly realistic threat of malicious customers mounting side-channel attacks [35, 46].

Reference 11 - 0.01% Coverage

SSL/TLS is, due to its enormous importance, a major target for attacks.

Reference 12 - 0.01% Coverage

Cloud computing allows customers to outsource the burden of data management and benefit from economy of scale, but privacy concerns hinder its growth [3].

Reference 13 - 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 14 - 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.

Files\\sec15\_full\_proceedingsEpub - § 5 references coded [ 0.01% Coverage]

Reference 1 - 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 2 - 0.01% Coverage

Current mainstream engineering practices for specifying and implementing security protocols are not fit for purpose: as one can see from many recent compromises of sensitive services, they are not providing the security we need.

Reference 3 - 0.01% Coverage

The defacement and vandalism of websites is an attack that disrupts the   
operation of companies and organizations, tarnishes their brand, and plagues websites of all sizes, from those of large corporations to the websites of single individuals [1–3].

Reference 4 - 0.01% Coverage

The phenomenal growth of Android devices brings in a vibrant application ecosystem.

Reference 5 - 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.

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

Reference 1 - 0.01% Coverage

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