Files\\sec14\_full\_proceedingsEpub - § 6 references coded [ 0.01% Coverage]

Reference 1 - 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 2 - 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 3 - 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 4 - 0.01% Coverage

It is a truth universally acknowledged, that password-based authentication on the web is insecure.

Reference 5 - 0.01% Coverage

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

Reference 6 - 0.01% Coverage

Web applications are the driving force behind the modern Web since they enable all the services with which users interact.

Files\\sec15\_full\_proceedingsEpub - § 10 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

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

In today’s online world where gathering users’ personal data has become a business trend, Tor [14] has emerged as an important privacy-enhancing technology allowing Internet users to maintain their anonymity online.

Reference 4 - 0.01% Coverage

Many countries have begun to view encrypted network services as a threat to the enforcement of information control and security policies.

Reference 5 - 0.01% Coverage

Despite decades of research into alternative authentication schemes, text passwords have comparative advantages—familiarity, ease of implementation,   
nothing for users to carry—that make a world without text passwords unlikely in the near future [5].

Reference 6 - 0.01% Coverage

Security improves in a number of settings when applications can make use of a cryptographic key stored on a remote system.

Reference 7 - 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 8 - 0.01% Coverage

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

Reference 9 - 0.01% Coverage

Security research of the past five years has shown that the privacy of smartphone users—and in particular of Android OS users, due to Android’s popularity and open-source mindset—is jeopardized by a number of different threats.

Reference 10 - 0.01% Coverage

Electronic vehicle immobilizers have been very effective at reducing car theft.

Files\\sec16\_full\_proceedingsEpub - § 12 references coded [ 0.02% Coverage]

Reference 1 - 0.01% Coverage

Timing attacks pose a serious threat to otherwise secure software systems.

Reference 2 - 0.01% Coverage

The modern hypervisor stack is, by necessity, extensible.

Reference 3 - 0.01% Coverage

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

Reference 4 - 0.01% Coverage

While Address Space Layout Randomization (ASLR) by itself no longer ranks as a strong defense against advanced attacks due to the abundance of memory disclosure bugs [1], it is still an essential foundation for more sophisticated defenses that use randomization to provide fast pseudo-isolation.

Reference 5 - 0.01% Coverage

To most people, search engine is the entrance to all sorts of web sites on internet.

Reference 6 - 0.01% Coverage

Historically attackers have had more resources than defenders, which is still mostly true.

Reference 7 - 0.01% Coverage

Cache attacks represent a powerful means of exploiting the different access times within the memory hierarchy of modern system architectures.

Reference 8 - 0.01% Coverage

In many application domains, multiple parties would benefit from pooling their   
private datasets, training precise machine-learning models on the aggregate data, and sharing the benefits of using these models.

Reference 9 - 0.01% Coverage

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

Reference 10 - 0.01% Coverage

A secure Internet ecosystem requires continual discovery and remediation of software vulnerabilities and critical misconfigurations.

Reference 11 - 0.01% Coverage

The cloud promises a cost-effective alternative for small and medium enterprises to downscale/upscale their services without the need for huge upfront investments, e.g., to ensure high service availability.

Reference 12 - 0.01% Coverage

Application-based modern operating systems, such as Android, thrive on their rich application ecosystems.