Files\\sec14\_full\_proceedingsEpub - § 3 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

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

Reference 2 - 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 3 - 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.

Files\\sec15\_full\_proceedingsEpub - § 8 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

Software bugs pervade every level of the modern software stack, degrading both stability and security.

Reference 2 - 0.01% Coverage

Attacking software systems by exploiting memory-corruption vulnerabilities is one of the most common attack methods today according to the list of Common Vulnerabilities and Exposures.

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

In spite of extensive industrial and academic efforts (e.g., [3, 41, 42]), distributed denial-of-service (DDoS) attacks continue to plague the Internet.

Reference 7 - 0.01% Coverage

Covert and side channels have for a long time remained an open threat to information flow control and isolation techniques in a variety of contexts including cloud and mobile computing [50, 71, 76].

Reference 8 - 0.01% Coverage

Remote malware downloads currently represent the most common infection vector.

Files\\sec16\_full\_proceedingsEpub - § 6 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

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

Reference 2 - 0.01% Coverage

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

Reference 3 - 0.01% Coverage

Memory corruption vulnerabilities are currently one of the biggest threat to software and information security.

Reference 4 - 0.01% Coverage

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

Reference 5 - 0.01% Coverage

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

Reference 6 - 0.01% Coverage

Malware continues to remain one of the most important security threats on the Internet today.