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

Reference 1 - 0.01% Coverage

The black-market economy for purchasing Facebook likes,1 Twitter followers, and Yelp and Amazon reviews has been widely acknowledged in both industry and academia [6, 27, 37, 58, 59].

Reference 2 - 0.01% Coverage

Both in practice and in the academic literature, we see an increasing number of applications demanding encryption schemes whose ciphertexts abide by specific formatting requirements.

Reference 3 - 0.01% Coverage

The computer security research community has developed several widely-adopted techniques that successfully protect return addresses and other critical stack data [13, 20].

Files\\sec15\_full\_proceedingsEpub - § 4 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

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 3 - 0.01% Coverage

Cache-based side-channel attacks have gained increasing attention among the scientific community.

Reference 4 - 0.01% Coverage

Protecting the privacy of user data within mobile applications (apps for short) has always been at the spotlight of mobile security research.

Files\\sec16\_full\_proceedingsEpub - § 2 references coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

To secure our computer systems, considerable effort has been devoted to techniques such as encryption, access control, and information flow analysis.

Reference 2 - 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.