PHYS ORG

Team finds many of mobile applications are open to web API hijacking

July 12 2018, by Deana Totzke

Credit: CC0 Public Domain

Smartphones, tablets, iPads—mobile devices have become invaluable to the everyday consumer. But few consider the security issues that occur when using these devices.

Modern mobile applications or "apps" use cloud-hosted HTTP-based application programming interface (API) services and heavily rely on the internet infrastructure for data communication and storage. To improve performance and leverage the power of the mobile device, input validation and other business logic required for interfacing with web API services are typically implemented on the mobile client. However, when a web service implementation fails to thoroughly replicate input validation, it gives rise to inconsistencies that could lead to attacks that can compromise user security and privacy. Developing automatic methods of auditing web APIs for security remains challenging.

Dr. Guofei Gu, associate professor in the Department of Computer Science and Engineering at Texas A&M University and director of the SUCCESS lab, together with his doctoral students Abner Mendoza and Guangliang Yang, are working to combat these security issues.

Gu and his team analyzed 10,000 mobile apps and found that many of them are open to web API hijacking—something that potentially affects the privacy and security of tens of millions of business users and consumers globally.

The root of the threat lies in the inconsistencies that are often found between app and server logic in web API implementations for mobile apps. Gu's team created the WARDroid framework to crawl applications, automatically carrying out reconnaissance and uncovering these kinds of inconsistencies, using static analysis along with what kinds of HTTP requests are accepted by the server. Once an attacker has the information on what these requests look like, he or she can carry out their own actions by tweaking a few parameters.

As a simple example, Gu explains in a vulnerable shopping app/server, a malicious user could shop for free by making some of the item prices in the shopping cart as negative (with tweaking some HTTP parameters), which should not be allowed by the app but unfortunately can be accepted by the server.

After identifying many vulnerable real-world mobile apps/servers that affect millions of users, Gu's team has communicated with the developers to help them fix the vulnerabilities. Their research paper was published in proceedings of the 2018 Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security & Privacy (S&P'18), one of the most prestigious top conferences in cybersecurity.

This is just one example of Gu's research on mobile app security. At the same conference Gu's team had another research paper on mobile app security that identifies a new type of vulnerability named Origin Stripping Vulnerabilities (OSV) in modern hybrid mobile apps and introduces a new mitigation solution OSV-Free (which is released as open source at http://success.cse.tamu.edu/lab/osv-free.php).

More information: DOI: 10.1109/SP.2018.00039

Provided by Texas A&M University

Citation: Team finds many of mobile applications are open to web API hijacking (2018, July 12) retrieved 19 April 2024 from https://phys.org/news/2018-07-team-mobile-applications-web-api.html