Elitenetzwerk Bayern

Einblicke in die Forschungsarbeit

MASTERARBEIT

„Verifying integrity of web applications“

PHILIP LENZEN

Elitestudiengang Software Engineering

University of Augsburg, December 2018

Verifying integrity of web applications

Philip Lenzen is an alumnus of the Elite Graduate Program „Software Engineering" at the University of Augsburg, Ludwig Maximilian University of Munich and the Technical University of Munich. In his master's thesis at Secomba GmbH and the University of Augsburg, he worked on protecting sensitive data of users of a web application not only from third parties, but also from unauthorized access by the service provider. By making application resources visible to everyone in a verifiable manner, he removed the need of a trusted party to ensure that users and security analysts work with the same application.

Web services - what you see is (not always) what you get

Zero Knowledge – at least since Edward Snowden, this term has been known to more than just die-hard security researchers. Regarding user data, it means that a service provider cannot gain access to it under any circumstances. For example, in the case of cloud storage services used by companies, the company secrets should never be accessible to others. However, it also affects services of daily life: Would you like a government or even your email provider to look at the family photos you recently sent? Or at the bill of your last online purchase? Fortunately, there are a bunch of service providers who promise zero knowledge – unfortunately, there is no reliable way to be sure.

Consider one that already encrypts your data in your browser with your password (and someone who is familiar with security even confirmed that). The provider could show only you a modified version of its web service at any time without you or anyone else being able to notice it – for instance, to steal your password.

Philip Lenzen developed a decentralized network infrastructure to detect such attacks. Providers willing to guarantee the user that they are using the "secure" service can register fingerprints of the service's resource files on the network. Since they must be kept available by the provider, this allows them to be both examined by analysts for security vulnerabilities and compared by users to those they received when using the service.

Attack Prevention due to a Public Key Infrastructure

A single server that logs the service resources already seems to be enough if it is not controlled by the potentially malicious provider – but what if the provider itself was only a victim of a powerful organization that can compromise multiple arbitrary entities, including the log server? And what should prevent the provider from registering the harmful version and the original one again shortly after the attack? Lenzen answers these questions with a public key infrastructure: He defines several roles and policies to publish the fingerprints, which guarantee non-repudiation and accountability of all changes by any party through means of public key cryptography.

Authorities for supervising the registration and query process as well as log servers for storing the fingerprints are the key roles of the architecture. They are orchestrated in such a way that each party approves the actual change and the authorization by the previous ones through a digital signature. A security analysis of the infrastructure has shown that assuming a secure connection, they all and

additionally the service provider must be compromised for an attack to remain undetected. Otherwise, the attacker can always be held accountable.

Proofs of correctness through Authenticated Data Structures

In order to track a history of changes, fingerprints of resource files are stored in append-only logs. To guarantee that operations on them are executed correctly, they are implemented as Authenticated Data Structures: These can construct unforgeable proofs which the other parties can use to verify correctness beyond any doubt. But not only the authorities do this – Lenzen developed a lightweight extension which can be easily installed in the user's browser. This verifies both the proofs and the signatures of all responsible parties. Thus, the integrity of the service's resource files is guaranteed, because in case of an attack even on several parties the verification fails.

Finally, Lenzen implemented a mechanism to publish the results of security analyses in the same way as fingerprints, which can also be checked by the extension. This creates confidence and additional security for the user.

More information:

https://www.researchgate.net/profile/Philip_Lenzen/research