ROOTS: On The (In-)Security Of JavaScript Object Signing and Encryption – Dennis Detering

Posted on **November 14,2017** by **sanna**

JavaScript Object Notation (JSON) has evolved to the de-facto standard file format in the web used for application configuration, cross- and same-origin data exchange, as well as in Single Sign-On (SSO) protocols such as OpenID Connect. To protect integrity, authenticity and confidentiality of sensitive data, JavaScript Object Signing and Encryption (JOSE) was created to apply cryptographic mechanisms directly in JSON messages. We investigated the security of JOSE and present different applicable attacks on several popular libraries. We introduce JOSEPH (JavaScript Object Signing and Encryption Pentesting Helper) – our newly developed Burp Suite extension, which automatically performs security analysis on targeted applications. JOSEPH's automatic vulnerability detection ranges from executing simple signature exclusion or signature faking techniques, which neglect JSON message integrity, up to highly complex cryptographic Bleichenbacher attacks breaking the confidentiality of encrypted JSON messages. We found severe vulnerabilities in six popular JOSE libraries. We responsibly disclosed all weaknesses to the developers and helped them to provide fixes.

We asked Dennis a few questions about his topic of choice.
Please tell us the top 5 facts about your talk.

- In our talk we present our research on the new JavaScript Object Signing and Encryption (JOSE) standards, which were created to apply cryptographic mechanisms directly in JSON messages to protect integrity, authenticity and confidentiality of sensitive data.
- We investigated the applicability of known attacks ranging from simple signature exclusion or signature faking techniques, which neglect JSON message integrity, up to highly complex cryptographic Bleichenbacher attacks breaking the confidentiality of encrypted JSON messages.
- We found severe vulnerabilities in six popular JOSE libraries. We responsibly disclosed all weaknesses to the developers and helped them to provide fixes.
- We introduce JOSEPH (JavaScript Object Signing and Encryption Pentesting Helper) – our newly developed open source Burp Suite extension, which performs (semi-)automatic security checks on targeted applications and aids in manual manipulation and inspection.

How did you come up with it? Was there something like an initial spark that set your mind on creating this talk?

This talk summarizes the results of our research, which was conducted as a Master's thesis at the Ruhr University in Bochum in cooperation with the CSPi GmbH. The Extensible Markup Language (XML) already enjoys great popularity and allows for cryptographic mechanisms by applying the XML Signature and XML Encryption standards. XML implementations already suffered from several practically applicable attacks and we wanted to check whether JOSE implementations are more secure.

Why do you think this is an important topic?

JavaScript Object Notation (JSON) has evolved to the de-facto standard file format in the web and is used for application configuration, cross- and same-origin data exchange, as well as Single Sign-On (SSO) protocols

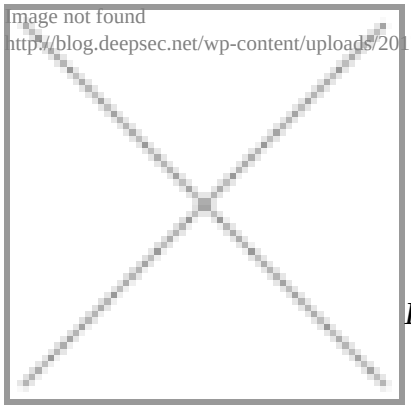
such as OpenID Connect. Thus, JOSE implementations are used for sensitive processes and data, such as authentication mechanisms, password resets, confidential storage and sensitive data transfer. If those implementations contain weaknesses that allow for any bypass, this probably results in a compromise of user accounts, personal data or full systems.

Is there something you want everybody to know - some good advice for our readers maybe?

Usually, it's not a good idea to implement your own cryptography. Most weaknesses in the field of cryptography result from implementation issues and missing knowledge of known and possible attacks. Especially companies should invest a lot more in security analyses and audits.

A prediction for the future - what do you think will be the next innovations or future downfalls when it comes to your field of expertise / the topic of your talk in particular?

There exist more known attacks against cryptographic systems and possible pitfalls. Such attacks are, for example, adaptive chosen-ciphertext attacks on the CBC mode and invalid curve attacks. With respect to future work, the analysis of such attacks on JOSE is considered essential. Furthermore, the usage of JOSE in complex systems like JSON-based web services and protocols like OpenID Connect should be in the scope of further researches. Similar to the security analysis of XML-based services an in-depth evaluation could lead to the discovery of completely new attacks. Additionally, JOSE's advantages of being simple, self-contained and designed for usage in space constrained environments opens future use-cases in the field of the Internet of Things and Industry 4.0.



Dennis has a Master's degree of IT security from the Ruhr-University Bochum and works as a penetration tester at the CSPi GmbH in Cologne. He has an avid interest in web, network and industrial security and loves to research and hunt for bugs.

Posted in:Security | Tagged:DeepSec,JOSE,JOSEPH,JSON,ROOTs,SSO,Vulnerability | With 0 comments