DeepSec 2016 Talk: Systematic Fuzzing and Testing of TLS Libraries – Juraj Somorovsky

Posted on **November 08,2016** by **sanna**

In his talk Juraj Somorovsky presents TLS-Attacker, a novel framework for evaluating the security of TLS libraries. Using a simple interface, TLS-Attacker allows security engineers to create custom TLS message flows and arbitrarily modify TLS message contents in order to test the behavior of their TLS libraries. Based on TLS-Attacker, he and his team first developed a two-stage TLS fuzzing approach. This approach automatically searches for cryptographic failures and boundary violation vulnerabilities. It allowed him to find unusual padding oracle vulnerabilities and overflows/overreads in widely used TLS libraries, including OpenSSL, Botan , and MatrixSSL.

Juraj's findings encouraged the use of comprehensive test suites for the evaluation of TLS libraries, including positive as well as negative tests. He and his team used TLS-Attacker to create such a test suite framework, which finds further problems in TLS libraries.

TLS-Attacker is an open source tool, and is currently being deployed for internal tests in Botan and MatrixSSL. We asked Juraj Somorovsky some questions about his matter of interest.

Please tell us the top 5 facts about your talk.

- It gives an overview of the recent attacks on TLS (Transport Layer Security).
- It presents an open source framework for the evaluation of TLS libraries, which can be used by security researchers or developers: TLS-Attacker.
- It shows how to use TLS-Attacker to test and fuzz TLS libraries, or how to create custom proof-of-concept attacks.
- It presents vulnerabilities found with TLS-Attacker, including padding oracles in OpenSSL, Botan and MatrixSSL.
- It shows a video from South Park.

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

In the recent years we could observe many vulnerabilities in important TLS implementations. We saw attacks targeting improper encryption algorithms and configurations, complex state machine attacks, or buffer overflows and overreads. This motivated us to create a tool that allows security researchers to easily implement proof-of-concept attacks, or execute fuzzing and find such attacks automatically.

Why do you think this is an important topic?

TLS is arguably the most important cryptographic protocol. We use it every day in our browser to login on our favourite web sites or to execute secure payments. Its security evaluation is therefore of a huge importance.

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

This talk is for everybody who is interested in TLS and secure crypto protocols. As a security researcher or pentester you will learn how to execute specific attacks like padding oracles. As a security developer you will learn how to evaluate the security of your TLS servers.

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

The new TLS 1.3 standard is being developed. This standard will be integrated into new TLS libraries, including further novel TLS features and extensions. These new implementations will lead to novel security bugs and problems. We hope that with a careful systematic TLS fuzzing and testing new security problems can be eliminated.

photo_juraj

Dr. Juraj Somorovsky is a security researcher at the[*Ruhr University Bochum*]

Image not found
http://blog.deepsec.net/wp-content/uploads/2016/09/photo_juraj.jpg

, and co-founder of Hackmanit GmbH. He is a co-author of several TLS attacks (e.g., DROWN), and the main developer of a flexible tool for TLS analyses: TLS-Attacker (https://github.com/RUB-NDS/TLS-Attacker). He presented his work at many scientific and industry conferences, including Usenix Security, Blackhat, Deepsec or OWASP Europe.

Posted in:Conference,Development,Security | Tagged:Botan,Crypto,DeepSec,MatrixSSL,OpenSSL,Talk,TLS | With 15 comments