Something Awesome Project for COMP6443: Padding Oracle Attack

Student Information: z5110172 Weitao Wang

Introduction of Project:

A padding oracle is a function of an application which decrypts encrypted data provided by the client, e.g. internal session state stored on the client, and leaks the state of the validity of the padding after decryption. The existence of a padding oracle allows an attacker to decrypt encrypted data and encrypt arbitrary data without knowledge of the key used for these cryptographic operations. This can lead to **leakage of sensible data** or to **privilege escalation vulnerabilities**, if integrity of the encrypted data is assumed by the application.

Block ciphers encrypt data only in blocks of certain sizes. Block sizes used by common ciphers are 8 and 16 bytes. Data where the size doesn't match a multiple of the block size of the used cipher has to be padded in a specific manner so the decryptor is able to **strip the padding**. A commonly used padding scheme is **PKCS#7**. It fills the remaining bytes with the value of the padding length.

In Web Security area, A Web hack that can endanger online banking transaction is ranked the **No. 1 new Web hacking technique for 2010** in a **top 10** list selected by a panel of experts and open voting.Called the **Padding Oracle Crypto Attack**, the hack takes advantage of how Microsoft's Web framework **ASP.NET** protects AES encryption cookies.

Hence I am going to self-learned what is Padding Oracle Attack and how it works in my something awesome project.

Initial Goals:

Using Python to implement how Padding Oracle Attack work. Design some exercises and write reasonable solutions to help me and others review the logic of Padding Oracle Attacks

Studying Methodology:

Youtube video, online blogs, programming, security engineering peers discussion, reading textbook.

Difficulties Analysis:

CBC Mode Encryption, PKC#7 Standard, Padding Operation, Oracle Attack, Initialisation Vector, DES, Intermediate Value.

Demonstration:

I used the python 2.7 to implement how padding oracle attacks cracking the cipher text to the plaintext

GitHub link: https://github.com/StephenLover/COMP6443SomethingAwesome

Reflection:

In this project, I found my passion about cryptography and web security during padding oracle attack research.

And I realised that the **theoretic knowledge** are extremely important in web security, for example, if you want to know how padding oracle attacks works, you have to be familiar with the CBC Encryption Mode, PKCS7 Standard, DES….

Also, I found the Padding Oracle vulnerability are very common, even exists in the big framework such as ASP.NET.

Reference and Tools:

https://blog.gdssecurity.com/labs/2010/9/14/automated-padding-oracle-attacks-with-padbuster.html

https://github.com/mpgn/Padding-oracle-attack

https://www.acunetix.com/vulnerabilities/web/asp-net-padding-oracle-vulnerability

https://docs.secureauth.com/display/KBA/ASP.NET+Padding+Oracle+Vulnerability

https://www.cio.com.au/article/374310/top_10_web_hacking_techniques_2010_revealed/?fp=4&fpid=2117012706

- Padding Oracle Attack Online Demo: http://erlend.oftedal.no/blog/poet/
- PadBuster: https://github.com/GDSSecurity/PadBuster