Introduction to Cybersecurity (650.030)

Padding Oracle Attack: PoC Implementation

Lecturer: *Arnab Roy*

1 Simple version

The objective is to implement the full padding oracle attack for up to two blocks of messages. The main function that you need to implement towards this is - `PaddingOracle` that returns 0 or 1 corresponding to failed or successful padding check/decryption. Then you write the function that will recover the last block, starting with the right most byte. Note that no MAC check is performed in this simple version.

2 Version 2

In this task, the objective is to simulate the TLS protocol behaviour to construct the padding oracle. Instead of writing a simple padding oracle function, you should construct the padding oracle from the successful padding check or failed MAC check. The success or fail message is encrypted. In order to implement the attack based on the such a padding oracle you have to distinguish the success failure depending on the time taken to receive the returning value from padding oracle function.

3 Version 3 (Advanced)

In this task the objective is to simulate the Lucky 13 attack with the corresponding TLS protocol behaviour to construct the padding oracle. Here both the MAC check and padding check are performed for all queries sent to a padding oracle. In order to distinguish the returning values from padding oracle and recover the corresponding padding value you need to consider 4 plaintext blocks and follow the attack procedure of Lucky 13.