YANG ZONGQI ▼ LIU JINJIAN

GUO ZIYUN ▼ XU ANJUN ▼ LI JUNLE

GROUP7

2023 NUS-SOC-SWS

DEFENSE OF THE ANCIENT BREACH

WHAT IS BREACH?

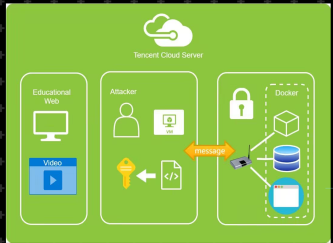
BREACH is an attack based on TLS compression which targets information compressed in HTTP response to obtain secrets.

MECHANISMS

The main steps are as follows:

1. **Injecting** his guesses of the secrets into the **HTTPresponse** bodies.
2. **Observing the time** when the responses would be highly compressed, and the output **length** differs, means the guess matches.
3. **Detecting** the secret information.
4. **Extracting** the complete secret.

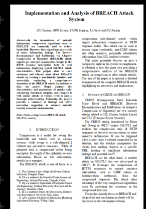
WHAT WE HAVE DONE?



SIMULATION

1. **Gain control** of the victim's network, enabling the attacker to **inject** code for execution.
2. The attack script issues. multiple requests to the target website, which are **sniffed** and **analyzed**.
3. The attacker script runs in a different context from website.
4. **Compare the encrypted lengths**, then information about the corresponding plaintext length relationships can be **deduced**.

WEBSITE & PAPER


Implementation and Analysis of BREACH Attack System

To explore our website and paper, please access http://49.232.151.94/BREACH/BREACH.html

We develop an interactive website and write a paper describing details of the implimentation of attack and our analysis.

ATTACK & EDUCATION