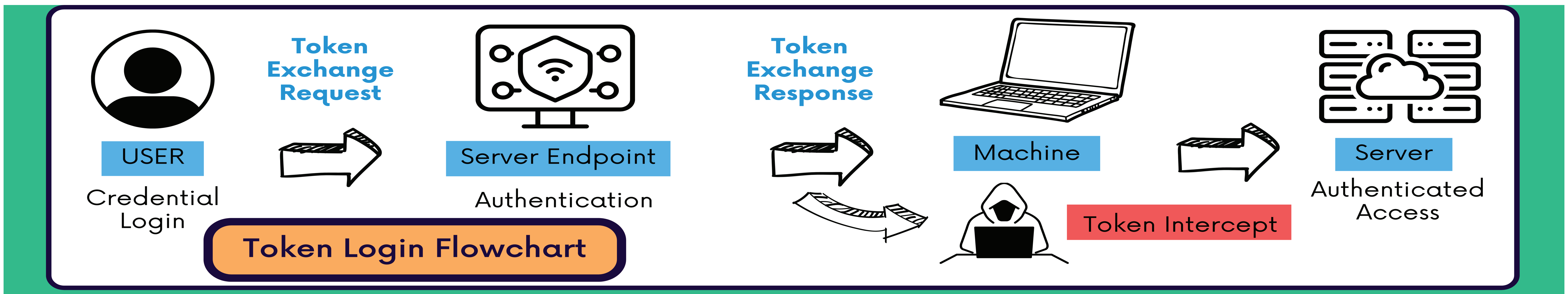
HOW TO HACK:
UNVEILING AN AUTOMATED WEB IMPERSONATION ATTACK



Token Login Flowchart

THE ISSUE

Many web services use single sign-on which allows users to <u>log in once</u> and are **remembered** with cookies

Many websites use **insecure** HTTP

As you login, LOGIN

Hackers can **intercept** your login cookies ...

and **impersonate** your accounts

THE AUTOMATED EXPLOIT

1 An **<u>Arp Poisoning</u>** attack

Redirects network traffic intended for the victim's device to the attacker's machine. The attacker can eavesdrop on the data passing through

2 **<u>Network Scan</u>** for the victim's login cookies

3 Victim account **<u>Login</u>**, with cookies

The above exploit acts as an **<u>Audit Tool</u>** to identify vulnerable Keycloak implementations

AUDIT

WAYS TO MITIGATE THIS ATTACK

1 Avoid Unknown Wi-Fi

Don't use unsecured Wi-Fi networks for sensitive transactions, such as online banking or shopping. Attackers can easily intercept your information.

2 Always Use HTTPS

HTTPS://

When using an internet browser, e.g. Edge, Chrome, Safari, etc... click on the icon at the left of the URL address bar. Ensure that the website is on HTTPS and has a valid SSL certificate to secure your connections.

To Developers

Secure Applications

Use HTTPS for secure communication. This encrypts the data in transit between the client and server, making it difficult for attackers to intercept and manipulate.

Member:
Lucas Chin Yee Seng, Hwa Chong Institution
Mentor:
Lim Seh Leng, Defence Science and Technology Agency

YDSP Young Defence Scientists Programme
DSTA Defence Science & Technology Agency
DSO National Laboratories