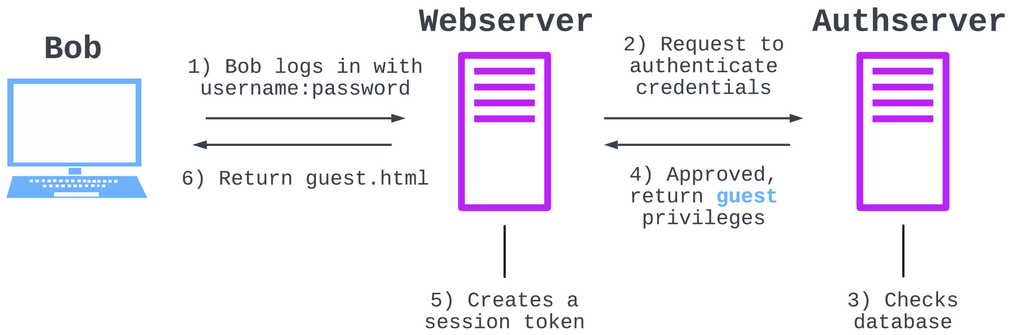
The ARP of War

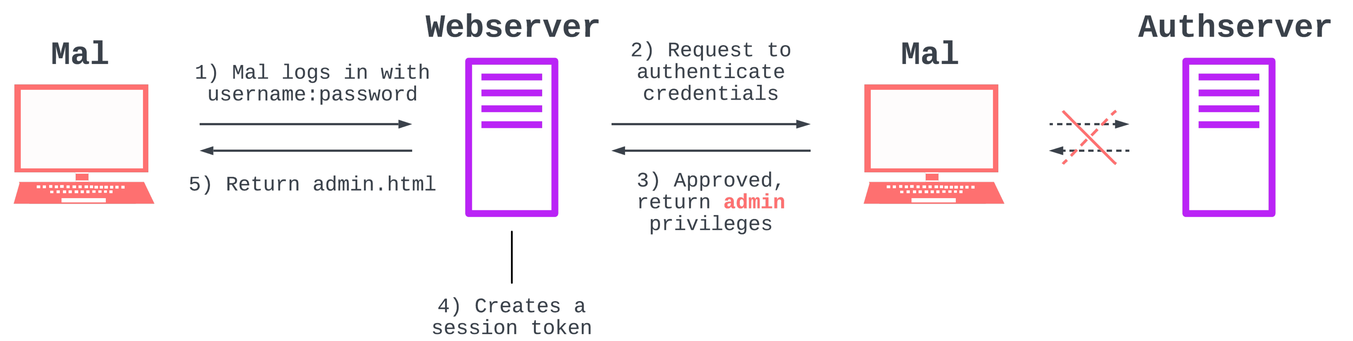
Cole Weinstein, Robbie Young

References

System Setup



Attack Plan



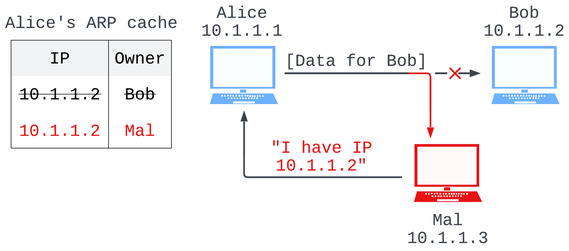
ARP Spoofing

ARP Cache: connects IP and hardware addresses

ARP Poisoning: lying about controlling an IP address to other machines on the network

Used by an attacker to insert themselves between two computers and read/edit their data

ARP was not designed for security; responses are taken at face value, even when unprompted



Regular webserver ARP cache

```
webmaster@gaggleweb:~$ arp
Address                  HWtype  HWaddress
_gateway                 ether   00:50:56:ea:c5:10
192.168.240.128          ether   00:0c:29:f4:78:16
192.168.240.136          ether   00:0c:29:38:11:e5
```

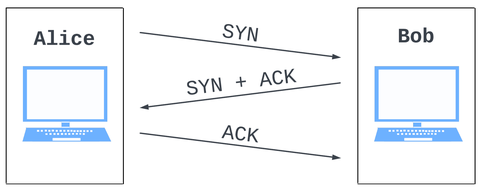
Poisoned webserver ARP cache

```
webmaster@gaggleweb:~$ arp
Address                  HWtype  HWaddress
_gateway                 ether   00:50:56:ea:c5:10
192.168.240.128          ether   00:0c:29:f4:78:16
192.168.240.136          ether   00:0c:29:f4:78:16
```

Denial of Service (DoS)

Denial of Service: overwhelm a victim server with traffic to prevent it from providing its services to clients

- *Application-layer attacks* make simple requests that require long responses
- *Protocol attacks* exploit lower-level Internet protocols, overwhelming the server's network systems
- *Volumetric attacks* flood a server with long requests, consuming the server's bandwidth



The TCP Handshake

Client: SYN packet
"Hi! Can we talk?"

Server: SYN + ACK packet
"Hello! Yes, we can talk."

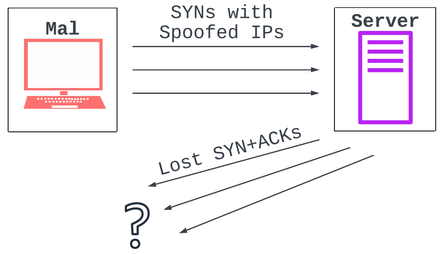
Client: ACK packet
"Great."

TCP SYN Flood

Attacker sends a bunch of AYN packets and never responds to the server's SYN + ACK

Server left storing garbage data for each half-open connection

Attacker users random IPs to prevent their own computer from waiting for half-open connections



Exploiting Diffie-Hellman

Adversary in the Middle (AITM): an attacker places themselves between two communicating parties

Victims will continue to believe they're talking over a direct connection

The attacker eavesdrops on all data going between the two victims, and can modify the communications as they wish

Only works when the parties do not have to verify their identifies

Symmetric Encryption: using a secret key and some math, scramble your data in a way that only other people with the same key can unscramble and read it

Our webserver and authserver use symmetric encryption to communicate without exposing user credentials to eavesdroppers

Diffie-Hellman: protocol used to generate a shared secret

Alice and Bob can determine **K**, while eavesdroppers cannot

Vulnerable to *AITM* as an attacker creates separate shared secrets with both Alice and Bob