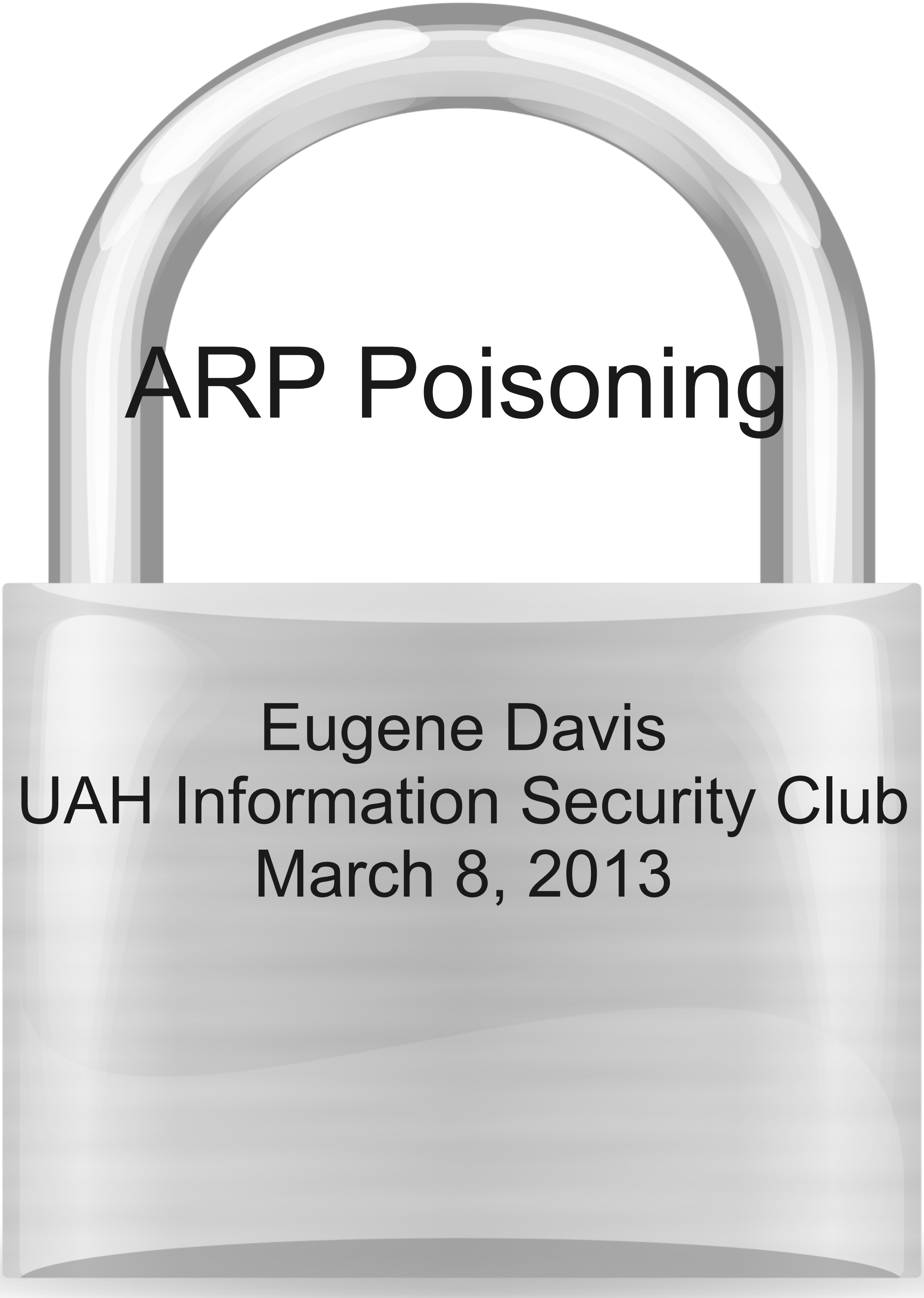


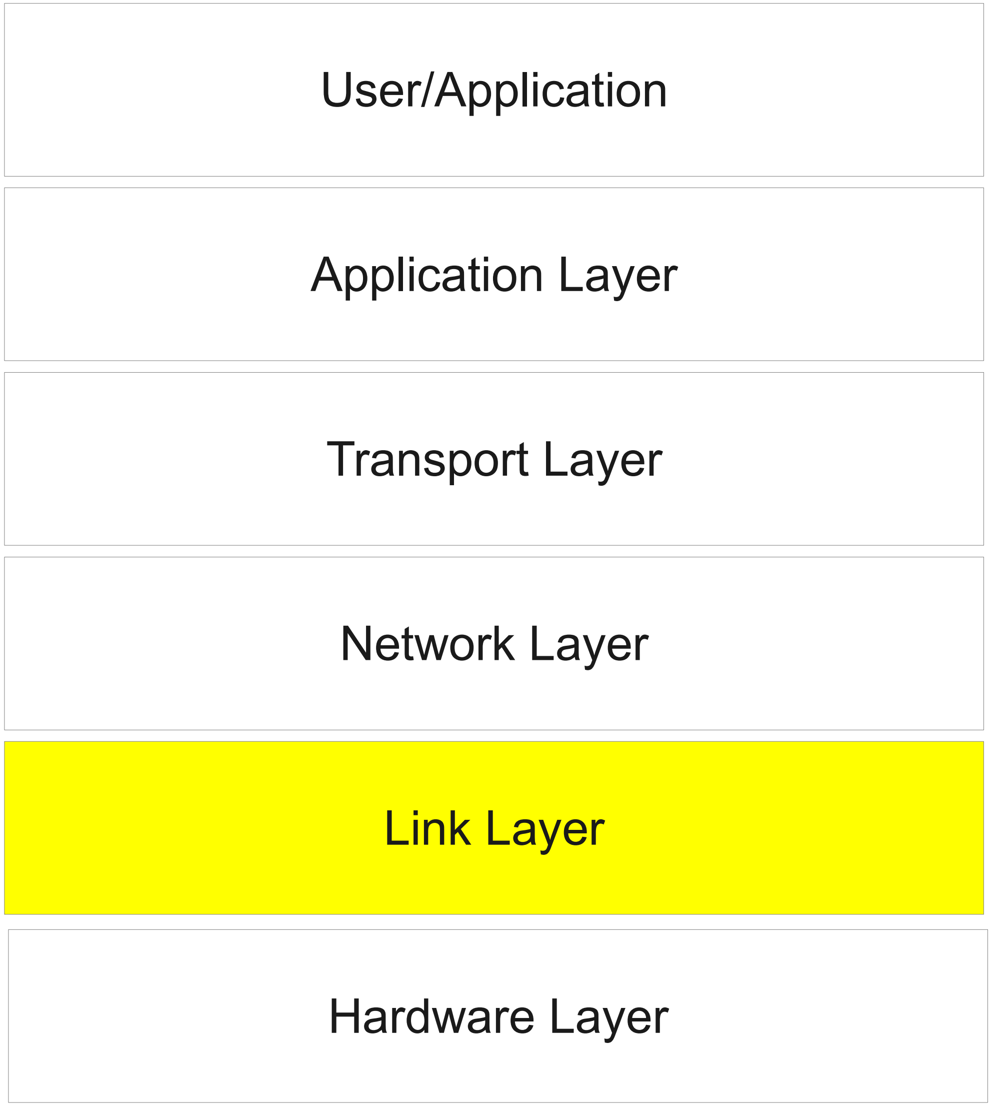
ARP Poisoning

Eugene Davis
UAH Information Security Club
March 8, 2013

What is ARP Poisoning?

- ARP poisoning, or ARP spoofing, is the exploitation of a low level networking protocol
- Using ARP poisoning, an attacker can redirect any traffic to a given IP address or set of IPs
- Can be used as as part of complex attacks
  - Session Hijacking
  - Man-in-the-Middle (MitM)
  - DoS

ARP's Place in the Network Stack



User/Application

Application Layer

Transport Layer

Network Layer

Link Layer

Hardware Layer

Address Resolution Protocol (ARP)

- ARP establishes the link between a MAC and IP address over a LAN
- Normally it is a request/response protocol
  - Sender says “Hey, who has IP *.*.*.*?”
  - Recipient says “Hi, I own IP *.*.*.*, my MAC is 01:23:45:67:89”
  - Then all machines hearing this (including switches) update their ARP tables to reflect it

ARP (Cont.)

- Unfortunately, ARP also supports a gratuitous broadcast
  - This allows a machine to announce ownership of an IP
  - Loudmouthed machine says “Hey, I'm MAC 01:23:45:67:89 and I own IP *.*.*.*”

ARP Poisoning

- ARP Poisoning relies on the ability to use gratuitous broadcasts

Short name	IP	MAC Address
Sender	192.168.0.3	01:23:45:67:89
Recipient	192.168.0.2	23:45:67:89:01
Attacker	N/A	45:67:89:01:23

An example of an ARP cache. This could be stored in a switch between the Sender and Recipient. Note that the Attacker has no IP.

- The Attacker, desiring to replace the Recipient, sends: “Hey, I'm MAC 45:67:89:01:23 and I own IP 192.168.0.2”
- After this, all ARP caches hearing this broadcast now point that IP address to the Attacker's MAC

ARP Poisoning (Cont.)

- As a result of the gratuitous broadcast, the Attacker now receives all traffic meant for the original recipient

Short name	IP	MAC Address
Sender	192.168.0.3	01:23:45:67:89
Recipient	N/A	23:45:67:89:01
Attacker	192.168.0.2	45:67:89:01:23

An example of an ARP cache after the Attacker has poisoned it

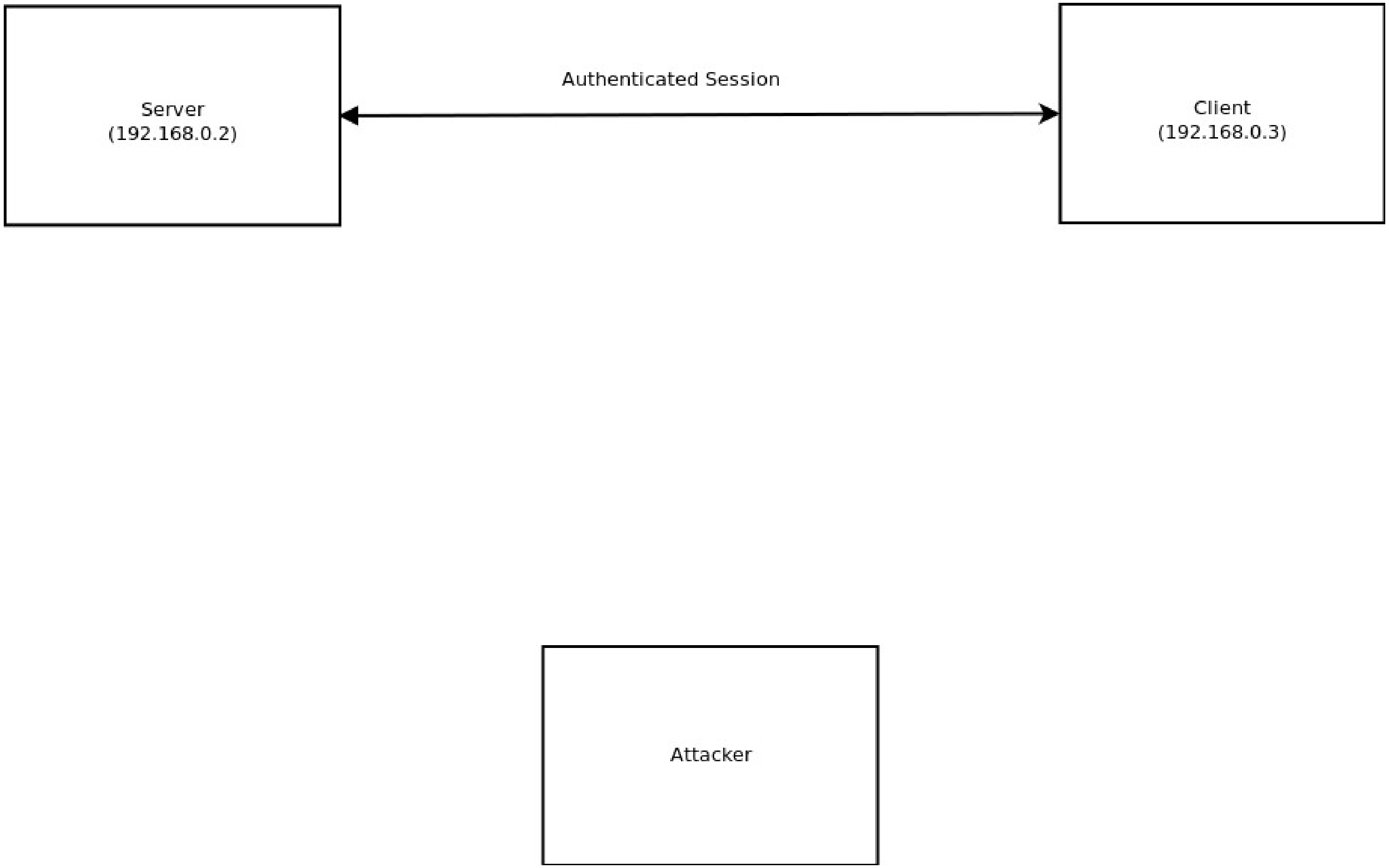
- The Attacker must refresh ARP caches with a broadcast regularly enough to ensure it does not get corrected
- Most networks have no defense against ARP poisoning

ARP Poisoning in Session Hijacking

- Session Hijacking is the process of replacing one of the parties that have established a session together
  - This includes a session that is authenticated but does not protect integrity, e.g. Telnet
- ARP poisoning allows the attacker to replace one of the two parties by stealing their IP
- Unless an attacker knows the proper responses to messages that are sent, the channel will often break

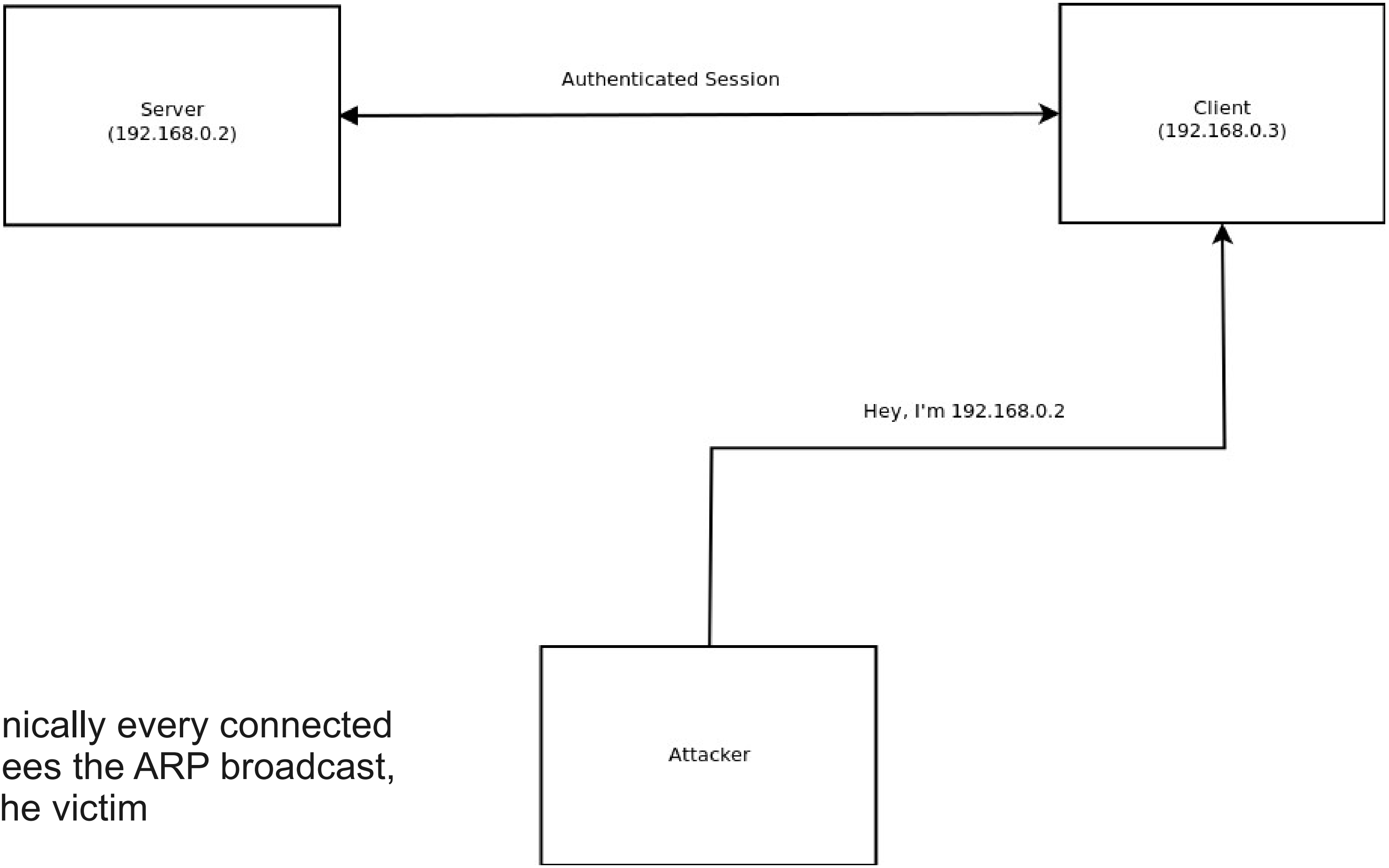
Session Hijacking Diagram

Attacker wants to hijack the session



Session Hijacking Diagram

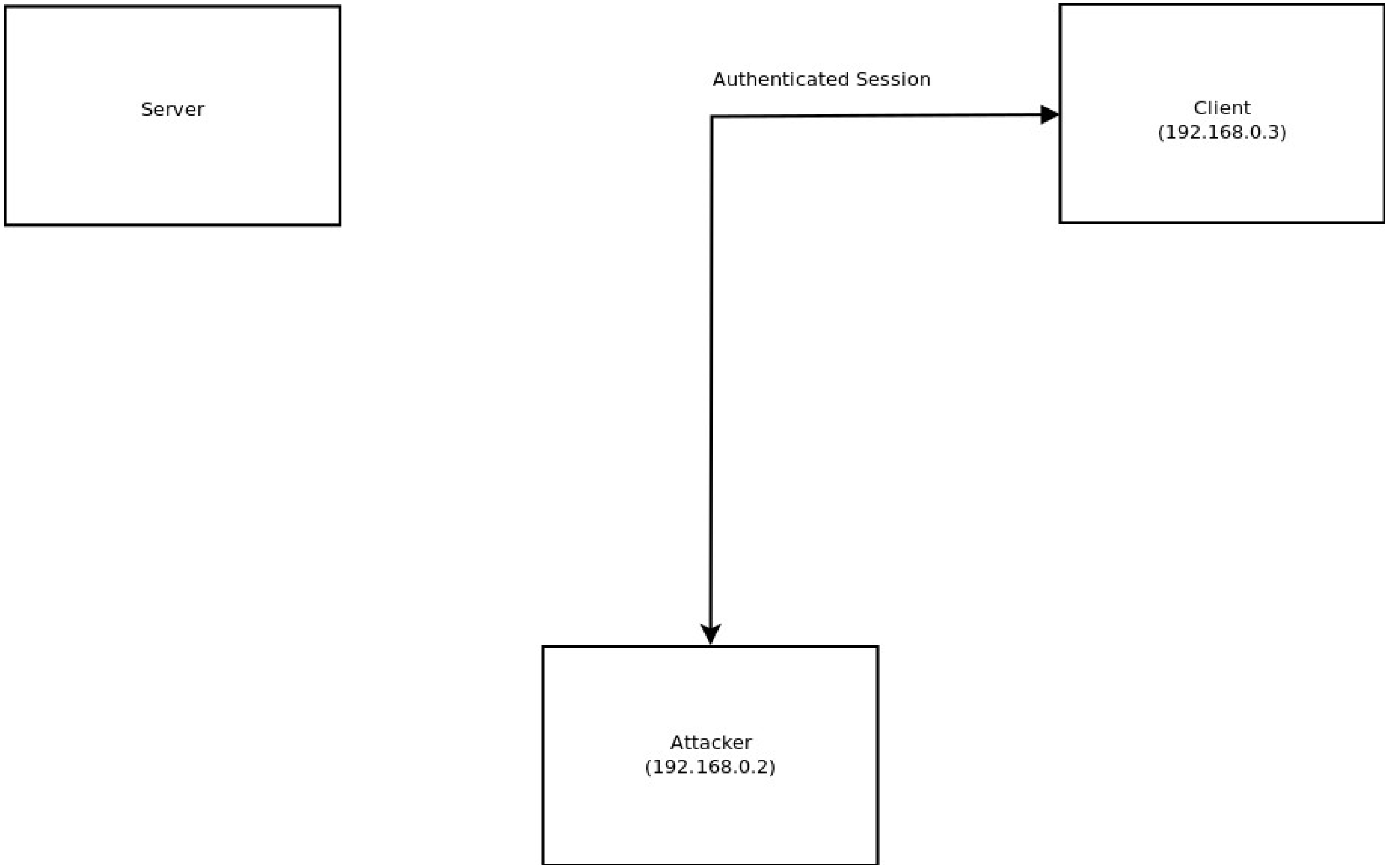
Attacker performs ARP poisoning



Note: technically every connected machine sees the ARP broadcast, including the victim

Session Hijacking Diagram

Attacker is now pretending to be the server

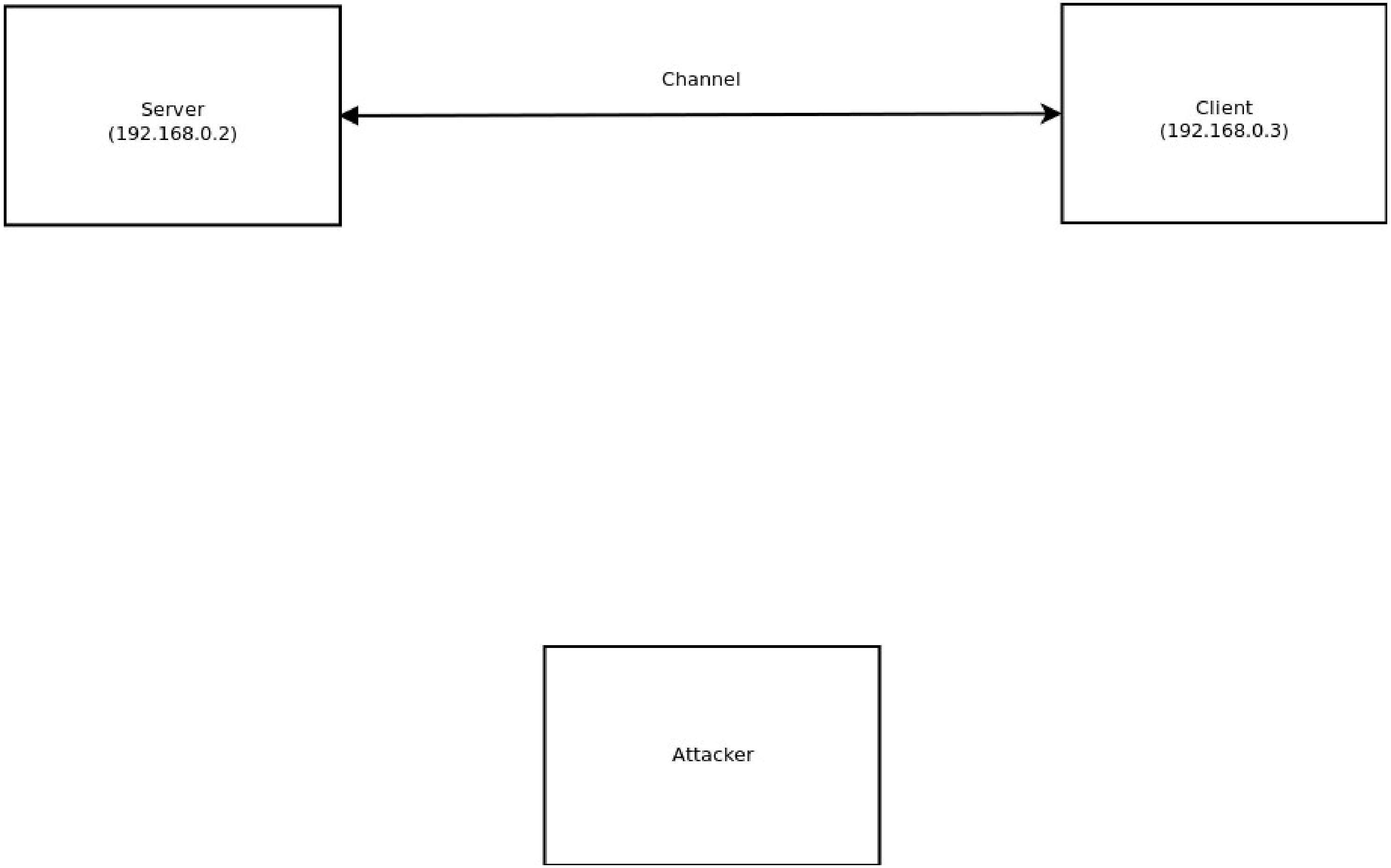


ARP Poisoning for MitM Attacks

- To overcome issues with generating the correct response, ARP poisoning can create a MitM attack
- Requires the Attacker to seize the IPs of both the Sender and Receiver
- Once ARP poisoning is done to both, the Attacker routes the traffic it receives to the correct destinations
  - This allows the attacker to sniff all traffic between two targets
  - Also this may allow an attacker to modify the data flowing between the targets

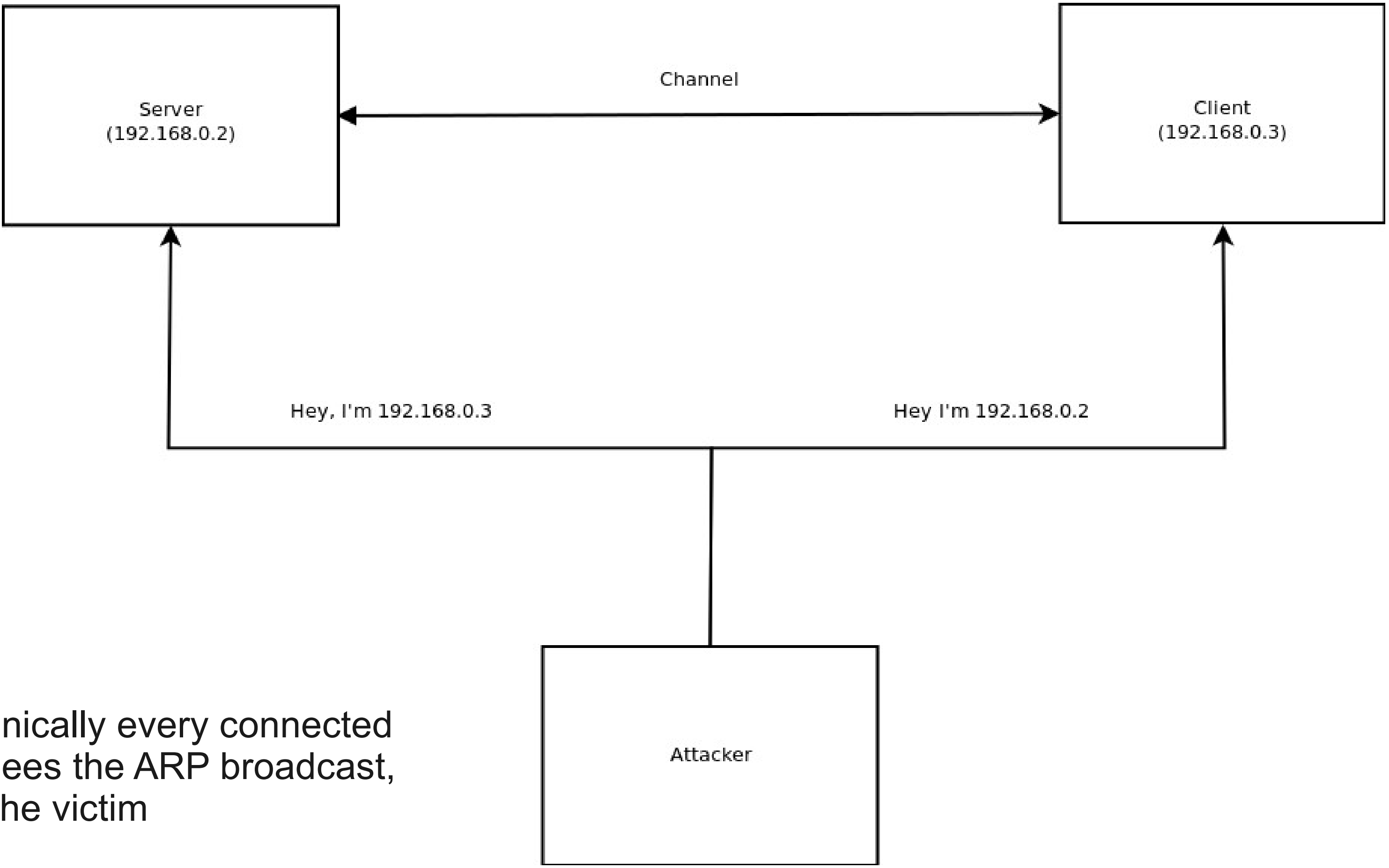
ARP Poisoning MitM Diagram

Attacker wants to view/modify the session



ARP Poisoning MitM Diagram

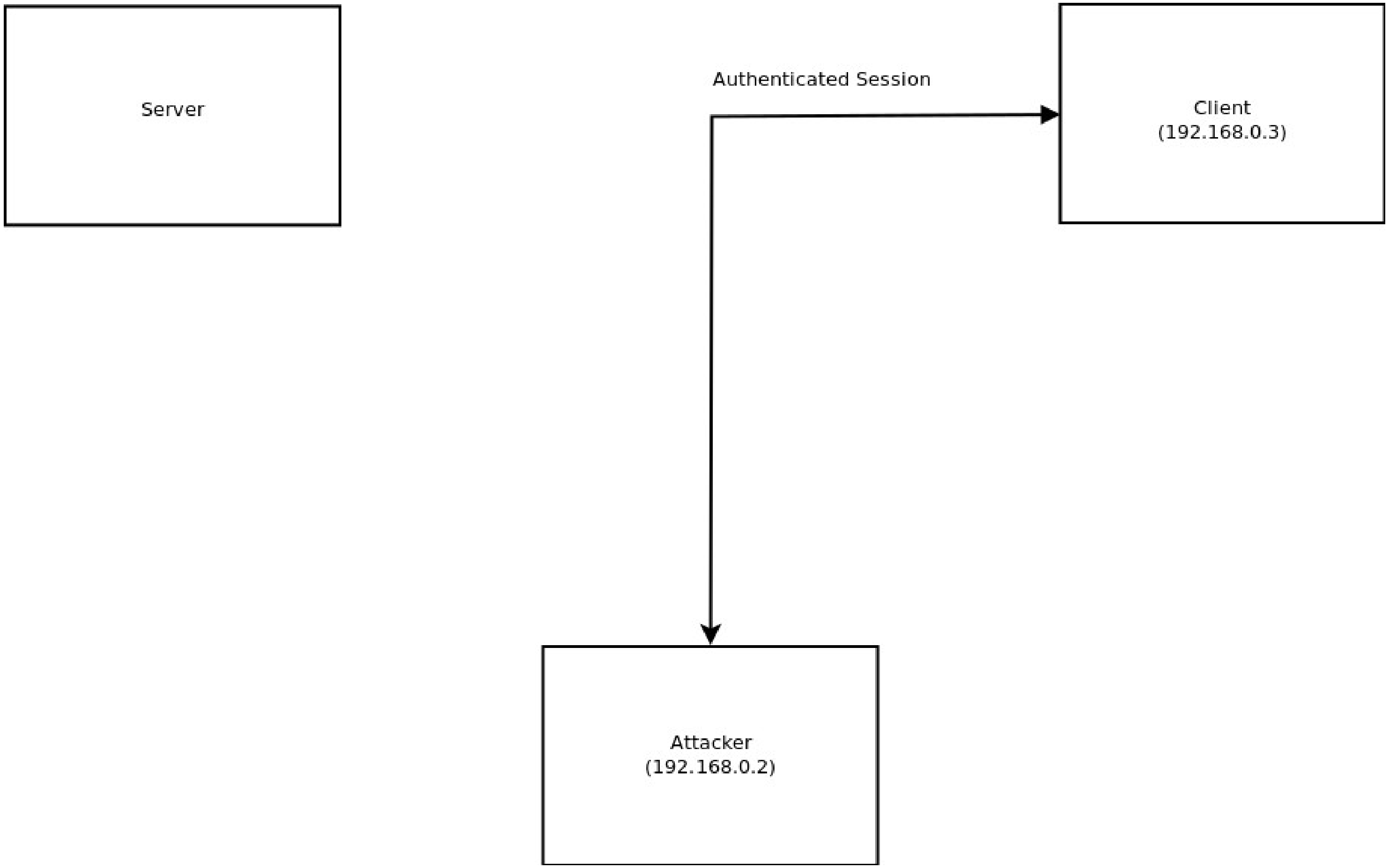
Attacker performs ARP poisoning



Note: technically every connected machine sees the ARP broadcast, including the victim

ARP Poisoning MitM Diagram

Attacker now has full access to the channel



ARP Poisoning Defenses

- Manually map the ports on switches to particular MAC/IP pairs
  - Hardcoding like this forces the network to be static
  - Laptops become impossible to use
- Protecting the data at a higher level of the networking stack
  - Strong authentication and maintaining an authentic secure channel defends against session hijacking
  - Providing a confidential secure channel prevents an attacker from sniffing traffic
  - Technically these do not prevent APRP poisoning, they just mitigate the effects
- Monitoring for ARP Poisoning (i.e. an IDS)

Summary

- ARP poisoning allows an attacker to steal IP addresses from other machines
- It can allow session hijacking and MitM attacks to take place
- Preventing it is all but impossible
- Defend against it with good encryption schemes

References

- Counterhack Reloaded by Ed Skoudis
- http://technet.microsoft.com/en-us/library/cc940021.aspx
  - Description of ARP
- http://tools.ietf.org/html/rfc826 - Definition of ARP
- http://www.rootsecure.net/content/downloads/pdf/arp_spoofing_intro.pdf
  - Description of ARP poisoning

License