EPFL

SPRING
SECURITY AND PRIVACY ENGINEERING LABORATORY

Computer Security (COM-301)

Network Security - Spoofing

Live exercises

Noisy roommate

Alice subscribed to a digital diary site. She is worried that her roommate might try to read her diary. She went through the COM-301 material to learn what attacks her roommate could launch. She made a shortlist of worrisome attacks and asked you to confirm.

Which attack(s) would you remove from the list because they are not applicable in this scenario?

A) BGP hijacking

B) Looking over the shoulder

C) ARP poisoning

D) DNS hijacking

(A) The roommate is on the same LAN, a BGP hijacking makes no sense. Remove from the list
(B) The roommate could indeed spy over Alice's shoulder. Do not remove
(C) The roommate is on the same LAN, so she can launch and ARP poisoning attack to MITM connections to the diary page. Do not remove
(D) The roommate can hijack DNS responses when Alice is looking for the diary web's IP, and then MITM the connection. Do not remove

MCQ

Which of the following statements are true:

a) In ARP, the receiver can check the authenticity of a sender upon receiving a packet.
b) In a DNS hijacking attack a malicious router A in AS1 tells routers in AS2 that it is the fastest route.
c) Unless IPSEC is used, IP headers contain source and destination IP addresses in the clear.
d) ARP associates a MAC address to a given IP address.

a) False, ARP does not provide authenticity.
b) False, this is BGP hijacking
c) True
d) True

Hearing secret whispers

Suppose you are concerned that your browser has malicious code running within it, and sends information about your browsing activity to `www.badsite.com` though you are confident that your operating system has not been compromised. You type `www.twitter.com` into your browser's address bar to take you to the Twitter site.

Are there steps you could take (which could involve additional effort on your part) to check whether your browser sent any information to `www.badsite.com` via cookies as part of that request?

Potential Answer 1: You can run a sniffer (e.g., Wireshark) to observe the network traffic actually sent by your browser, and check whether it contains any cookies. To figure out whether those leak any information about your site visits, you could visit different sites and try to correlate it with the cookies sent.

Potential Answer 2: You could configure your browser to route your all HTTP requests through a web proxy you've written that checks whether the request includes any cookies. As before, you can visit different sites and correlate the information sent.

Stop John!

John Oliver has aired a new show to expose the evil nature of Evil corp, the owners of Evil Service Provider, a famous ISP with millions of users. Since watching this video may lead to loss of customers, Evil corp wants to block access to this content through its provider.

Part I. Describe one method that the Evil Service Provider can use to prevent its customers from watching this content without affecting its other services.

Part II. Can Evil Service Provider's users bypass the censoring which you designed in the previous part? Justify. Assume that Evil Service Provider is the only ISP available to the users.

(other answers than this may be valid)

Part I:
Potential Attack 1: Evil Corp can drop packets to IP Oliver
Potential Attack 2: Evil Corp could launch a DNS Poisoning attack on John Oliver's domain to redirect any user trying to watch the show to another web.

Note: Answers must reflect how Evil Corp can target those customers visiting John Oliver's show. Answers that would affect all customers would receive less points

Note: ARP attacks is not a valid answer: ISPs cannot launch local network attacks.

Note: BGP Hijacking is a valid answer. However, it is not a good idea in terms of economy of the attack.

Part II:

Potential Mitigation for Attack 1 Packet drop: Customers can bypass the censorship by using a VPN to hide their destination IP (The answer must specify how users would hide IP Oliver so that it counts as defense for attacks based on IP)

Potential Mitigation for Attack 2 DNS Poisoning: DNSSEC to protect against DNS poisoning **or** obtain John Oliver's IP from another DNS that is not under control of the adversary or from an out of band channel.