Computer Security (COM-301)

Network Security: Spoofing and IP

Thursday live exercises

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

Where did you come from (Cotton-Eye Joe)

The lack of security mechanisms in network protocols enables adversaries to change the origin of packets. This in turn enables :

A) Rerouting packets by changing the cost of routes in the BGP protocol

B) DNS hijacking attacks in which an adversary changes the content of a DNS response

C) Providing fake MAC addresses in response to an ARP request to bootstrap a man in the middle attack

Where did you come from (Cotton-Eye Joe)

The lack of security mechanisms in network protocols enables adversaries to change the origin of packets. This in turn enables :

A) Rerouting packets by changing the cost of routes in the BGP protocol

B) DNS hijacking attacks in which an adversary changes the content of a DNS response

C) Providing fake MAC addresses in response to an ARP request to bootstrap a man in the middle attack

A. No. Changing the cost of routes does not change the origin
B. No. Changing the content of a DNS response does not change the origin (it still comes from the resolver)
C. Yes. When you respond with a fake MAC address, you are changing the origin of the packet you send (from your real MAC address to the fake MAC address)

How far can you defend

Are the following statements TRUE or FALSE

A) Using DNSSEC to resolve example.com guarantees authenticity and integrity on subsequent HTTP connections to example.com, but not confidentiality.

B) Setting paths to be the shortest to a website is the core of a BGP hijacking attacks

C) ARP spoofing can be mitigated using the separation of privilege principle

How far can you defend

Are the following statements TRUE or FALSE

A) Using DNSSEC to resolve example.com guarantees authenticity and integrity on subsequent HTTP connections to example.com, but not confidentiality.

B) Setting paths to be the shortest to a website is the core of a BGP hijacking attacks

C) ARP spoofing can be mitigated using the separation of privilege principle

A. False, DNSSEC provides assurance for the current connection, not subsequent ones (example.com may change IP in the future)
B. False, BGP is not about shortness of route, but about cost. The cheapest route is the one chosen regardless of length
C. True, remember that one solution is to receive information from more than one point so that it is harder to modify (more parties have to be compromised)

Find-a-student

There is a new Internet service `RankAProf` in which students can give ratings to their professors and provide comments on the lectures. To promote honesty, the website publishes the comments anonymously.

To add a rating or a comment, a student needs to visit `www.rankaprof.com`, which is hosted in the US, from her browser and log in. When the user is logged in, the server opens a session and keeps adding ratings and comments to a temporary list. Only when the student clicks “Publish” is the list added to the database and deleted.

A professor with bad ratings wants to identify which students at EPFL are writing negative comments on `RankAProf` . Since the professor is not an EPFL system administrator, he cannot inspect the packets. How can the professor learn who is leaving comments?

a) Attack. Describe an attack the professor can deploy. Concretely identify where in the network the professor must be to deploy this attack and describe how it works (only one attack is needed, select your favourite)

b) Defense. Explain a protocol from the ones seen in class that prevents the attack you propose in **a)** . Explain how it defeats the attack.

Find-a-student

There is a new Internet service `RankAProf` in which students can give ratings to their professors and provide comments on the lectures. To promote honesty, the website publishes the comments anonymously.

To add a rating or a comment, a student needs to visit `www.rankaprof.com`, which is hosted in the US, from her browser and log in. When the user is logged in, the server opens a session and keeps adding ratings and comments to a temporary list. Only when the student clicks "Publish" is the list added to the database and deleted.

A professor with bad ratings wants to identify which students at EPFL are writing negative comments on `RankAProf` . Since the professor is not an EPFL system administrator, he cannot inspect the packets. How can the professor learn who is leaving comments?

a) Attack. Describe an attack the professor can deploy. Concretely identify where in the network the professor must be to deploy this attack and describe how it works (only one attack is needed, select your favourite)

b) Defense. Explain a protocol from the ones seen in class that prevents the attack you propose in **a)** . Explain how it defeats the attack.

Possible answer (there are many!)

A. A possible attack is to use ARP spoofing. The professor would need to be in the same local network as the student. When the student does an ARP request to get the address of the gateway to connect to the internet and learn the IP of the web, the professor can spoof the response and launch a man in the middle attack.

B. Check that there are no anomalous responses (e.g., that not two responses with the same answers are received)

Stop the fake news

WeaselNews is spreading lies about the Coronavirus and the Swiss government has asked you to prevent Swiss citizens from accessing their website. Because WeaselNews is worried about its freedom of speech, the company hosts all their servers on the North pole. Devise a censorship approach to block access to WeaselNews and assess your suggested approach based on its effectiveness in Switzerland and its impact on the rest of the world (will this create a problem for people living in other countries?).

Can users bypass this censorship? If yes, how?

Note: You do not need to come up with a perfect censorship which is uncircumventable. We will grade how well you understand the degree of protection that your proposed censorship approach provides.

Stop the fake news

WeaselNews is spreading lies about the Coronavirus and the Swiss government has asked you to prevent Swiss citizens from accessing their website. Because WeaselNews is worried about its freedom of speech, the company hosts all their servers on the North pole. Devise a censorship approach to block access to WeaselNews and assess your suggested approach based on its effectiveness in Switzerland and its impact on the rest of the world (will this create a problem for people living in other countries?).

Can users bypass this censorship? If yes, how?

Note: You do not need to come up with a perfect censorship which is uncircumventable. We will grade how well you understand the degree of protection that your proposed censorship approach provides.

Two possible answers
1) Announce BGP with smaller prefix for the route from Switzerland to the North pole server. This will attract all Swiss and then you can block them, but it will also attract other users whose routes coincides with the one you are modifying. Users need a VPN outside Switzerland to bypass this.

2) Block/Hijack DNS responses. You can limit this blocking to internal (e.g., only blocking those whose destination is a Swiss IP), so this approach has no international impact. To bypass, users need to know the IP (e.g., get it online) use a VPN