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

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

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 are writing negative comments on `RankAProf` . Since he 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 <u>one</u> 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.

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.