SHOUZAB KHAN

SKHAN6

"By submitting this homework, I attest that the homework is my own work and I have not copied any text verbatim from any online or offline source, or from other students (past or present). I also attest that I have not used any paraphrasing tool or any homework solution websites. In addition, I attest that any information taken from course slides and handouts or any websites is properly attributed and referenced. I understand that any violation of the UAB Academic Integrity Code for any portion of the homework will result in a zero score for the entire homework and will be reported to the academic integrity coordinator per university policy."

**QUESTION NO 1.**

Tom called Jerry and asked where he was. Jerry claimed that he was at the University hall right now. Tom wants to verify that Jerry is actually at that location.

Name 4 different ways (as discussed in the class and the lecture) using which Tom can verify Jerry's location.  For each of them, state the issues and disadvantages of the technique. (4x1.5=6)

**ANSWER:**

**Look up that person:** Tom will use the number's directory to find the person. Jerry may be in another location and pretending to be in Birmingham, even though his phone number is registered here. This is a false claim that will damage people's trust. One cannot confirm the location. Companies usually use this situation to search for their information on Google.

**Trust Jerry:** Tom may ask Jerry about the location and trust on him. This may be wrong. Jerry is always willing to tell an inaccurate location by lying. It will be quite simple for Jerry to create a story regarding where he is if nothing is provided.

**Request for location:** Tom requests that Jerry send him his GPS coordinates. Jerry is using his phone, which he controls, to share the location. We are unsure about the authenticity of the place that Jerry provided us. Since Jerry controls the phone, it's simple for him to fake the coordinates. Jerry can act as though the location is part of Google Maps, but we can't be sure if it's real or fake.

**Third-party trail Jerry:** Tom can contact Apple or Google to help him find Jerry. Alternatively, a third party has the ability to track Jerry at all times and request his location at any time. Privacy is the issue with this solution. Nobody enjoys being constantly followed by someone. This is a private issue. A good example might be how they market information when you are in nearby areas of a brand and begin to see advertisements for it the following day.

**Have a connection to the place:** Requesting that Jerry should send something related to the place. Jerry can alter and fake the evidence. For example, you may ask Jerry to send you a false selfie with the background set to seem like you're standing in the university hall. Tom would have a difficult time verifying the authenticity of the selfie.

**QUESTION NO 2.**

Woody woodpecker is running his web-based service on a cloud. Buzz Buzzard wants to bring down Woody's service by launching a Denial of Service (DoS) attack. He is comparing two options:

(i) launch the DoS attack from outside the cloud.

(ii) launch the DoS attack from inside the cloud.

Describe the pros and cons of each of these two techniques. Which one do you think would be more successful in bringing down Woody's server and why? (1.5+1,5+1=4)

**ANSWER:**

**1) DoS attack from outside the cloud:**

**a. Pros:**

Botnets are made to launch this kind of attack. In this situation, it is possible to spoof the attacker's IP addresses or use a very powerful reflection attack.

b. Since the attacker is not within the cloud, they cannot terminate their service even if they get caught by the cloud.

**Cons:**

Modern cloud providers are equipped with powerful firewalls that can identify and stop the traffic coming from these kinds of attacks.

**a.** The attempt might be in vain, and it costs money to undertake this kind of attack.

**2) DoS attack from inside the cloud:**

**Pros:**

**A.** An attacker may block the internal network, which is very efficient because it is harder to stop an attack coming from within the network than one coming from the outside, which a firewall can identify.

**b.** Should the attacker manage to get access to the network, all of the servers in the racks will suffer as a result of the several routers that are part of the cloud-connected network.

**Cons:**

**a.** Because you are inside the cloud, you are subject to detection by cloud providers, who may remove you and take severe action against you.

**3)** There will be a greater chance of success if Woody's server is taken down from within the cloud. It is commonly known that cloud service providers are equipped with advanced firewalls that are capable of blocking external DoS attacks. They made it much more difficult for the attacker to launch an attack from outside the network. In the event that the attacker gains access to the network, the cloud's internal network may experience slowdowns. To the best of our knowledge, there are many routers and hops in the cloud network. It would be difficult for cloud providers to identify the attack and remove it from the network. Within the cloud, the routers are in charge of connecting and controlling the flow of communication between the servers. If Woody's server is on the rack where the router/network is compromised, it will be down.