

Network Security
CS261 – 10/5/09

Which issues really are network security?

Just as roads are seen infrastructure connecting resources, the network should be seen as an infrastructure connecting resources. Attacks can generally be split into the following 3 cases. Note that some attacks (case 2) are more truly network security, where as others (case 3) would best be addressed elsewhere.

Case 1: Attacks that are against the network itself

- analogous to taking cobblestones out of the road

Case 2: Attacks interfering with traffic on the network

- analogous to changing a street sign to point somebody the wrong direction

Case 3: Attacks which make use of the network

- analogous to driving a get-away car over the roads

Ethernet 101.

Shared Ethernet: Computers connected in a way that is analogous to a shared bus. The communication medium is time-shared between the parties. All messages sent on the bus are visible to all parties.

Switched Ethernet: Computers each connect to a switch, which in turn relays messages from the sender to the intended recipient only (in theory). Address Resolution Protocol (ARP) is used to associate MAC addresses with IP addresses and the switch routes packets accordingly.

Ethernet Attacks.

Some common attacks executable over Ethernet are:

- Eavesdropping
- Spoofing
- Denial of Service (DoS)
- Man in the Middle

Switched Ethernet tends to make the above attacks more difficult, although it does not eliminate them as a possibility. For example, both the eavesdropping and man in the middle attacks require receiving traffic that was originally destined for another party. While this is trivial in Shared Ethernet, it can also be accomplished over Switched Ethernet through the [ab]use of ARP. ARP spoofing can be used to associate the intended recipient's IP address with the attacker's MAC address.

MIG in the Middle Attack.

In war it is necessary to distinguish the friends from the foes. This is especially important if one is trying to decide if an airplane quickly approaching is a foe (and should be destroyed) or is a friend.

One technique developed to address this involves having a ground unit, perhaps a radar or anti-aircraft missile site, radio a challenge (number) to any incoming air traffic. The traffic would then compute a secret function on the number, and radio it back to the ground site. If the secret function was correct, then the plane could be trusted.

The attack against this system leveraged the fact that an incoming plane does not, strictly speaking, need to *know* the function being computed. The plane must just be able to *apply* the function to the challenge number. This means that an enemy plane could simply repeat the challenge to an allied plane, listen for the answer of the allied plane, and then parrot that answer back to the ground station. In this way, the enemy is able to produce the correct response without any knowledge of the function.

Modeling Threats.

Suppose that Alice and Carol would like to communicate with each other. Bob is mischievous and would like to, eavesdrop on, interfere with, impersonate or otherwise corrupt their communication.

Internet Threat Model

- Assume that if Alice and Carol want to communicate, Bob is not on the path between them
- This model tends to be the more practical of the two, but also makes more assumptions and hence is less thorough

Cryptography Threat Model

- Assume that nothing between Alice and Carol can be trusted
- This model is very thorough and robust, but can be so restrictive and pessimistic in practice that it may reject solutions which tend to work well in practice

Border Gateway Protocol (BGP).

Overview:

BGP is used to route packets through the Internet. For any given packet, it may not be immediately obvious where to pass the packet along to next so that it reaches its destination. BGP allows nodes on the network to broadcast routes they can offer to different IP blocks on the Internet. Adjacent nodes listen, remember, and take advantage of this next time the need to send information to a given IP block.

Attacks:

The most classic attack is to say that you have the shortest path to the whole world, and then drop all packets on the floor. This attack isn't very widely used since it will be easy

to discover and involves higher risk. More advanced and subtle attacks leverage the specifics of the BGP protocol.

For example, the more specific an advertisement for a route is, the faster it will propagate through the routing tables and the more priority it is given. Therefore, if we consider an attack where somebody advertises a fast route to 90% of their target's IP block, this will take precedence over routes advertised over an organization's entire IP block.