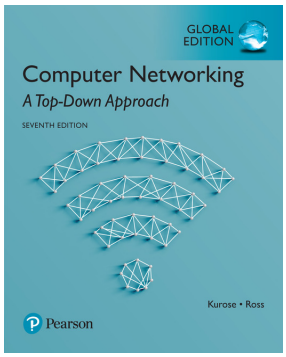
A brief introduction to Network Security Concepts



Prepared by Alvaro Barradas for RC2,
based on Computer Networking by Kurose / Ross

Networks Under Attack

- **The Internet is mission critical,** connecting
  - Large and small companies
  - Universities
  - Government agencies
  - Individuals (professional, social, personal activities)
  - Billions of “things” (wearables, home devices, etc.)

Networks Under Attack

- **The Internet is mission**
  - Large and small compa
  - Universities
  - Government agencie
  - Individuals (profes
  - Billions of "things"

But there is a DARK SIDE

"Bad Guys"

Cyber criminals that have the expertise and tools necessary to take down critical infrastructure and systems

Networks Under Attack

- **Network security breaches,** can
  - Disrupt e-commerce and cause the loss of business data
  - Compromise the integrity of information
  - Threaten people's privacy
  - Result in theft of intellectual property
  - Lawsuits
  - Threaten public safety

Networks Under Attack

Some of today's more prevalent security-related problems

- **Bad Guys can**
  - **Put malware into your host via the Internet**
  - **Attack servers and network infrastructure**
  - **Sniff packets**
  - **Masquerade as someone you trust**

Networks Under Attack

The Bad Guys can

- **Put malware into your host via Internet**
  - We attach devices to send/receive data to/from the Internet
    - Posts
    - Streaming music or movies
    - Vídeo conference calls
    - etc.

Networks Under Attack

The Bad Guys can

- **Put malware into your**
  - We attach devices to s
    - Posts
    - Streaming music o
    - Vídeo conference
    - etc.

But malicious stuff
Malware

can also enter and
infect our devices

Networks Under Attack

Once it infects your device

- **Malware can**
  - Delete your files
  - Install spyware to collect
    - your private information, social security numbers
    - your passwords and keystrokes
    - and send this back to “the bag guys”

Networks Under Attack

Once it infects your device

- **Malware can**
  - Enroll your device in a network of thousand of infected devices collectively known as a **botnet**
  - Participate in spam e-mail distribution
  - Participate in denial-of-service attacks against targeted hosts

Networks Under Attack

Most of the malware today is

- **Self-replicating**
  - Once it infects one host, it seeks entry into other hosts
  - Can spread exponentially fast in the Internet
  - Can spread in a form of **vírus** or a **worm**

Networks Under Attack

- **Viruses**
  - Malware that require some form of user interaction to infect the user's device.
  - Typically: e-mail attachment with malicious executable code.
  - Once executed the vírus will send identical messages.
- **Worms**
  - Malware that can enter a device without explicit user interaction.
  - Example: a vulnerable network application to which an attacker can send malware. The application may accept the malware and run it, creating a worm.
  - It then can scan the internet searching for the same vulnerability to send a copy of itself.

Networks Under Attack

The Bad Guys can

- **Attack Servers and Network Infrastructure**
  - Another broad class of security threats are known as **denial-of-service** (DoS) attacks
  - The network, host, or other piece of infrastructure become unusable by legitimate users
  - Web servers, e-mail servers, DNS servers, and institutional networks can be subject to DoS attacks.

Networks Under Attack

Most Internet DoS attacks fall into one of three categories

Vulnerability attacks

Involves sending a few well-crafted messages to a vulnerable application or operating system. If the right sequence of packets is sent the service can stop or, worst, the target host can crash.

Connection flooding

The attacker establishes a large number of half-open TCP connections at the target host. The host can become so affected with these bogus connections that it stops accepting legitimate connections

Bandwidth flooding

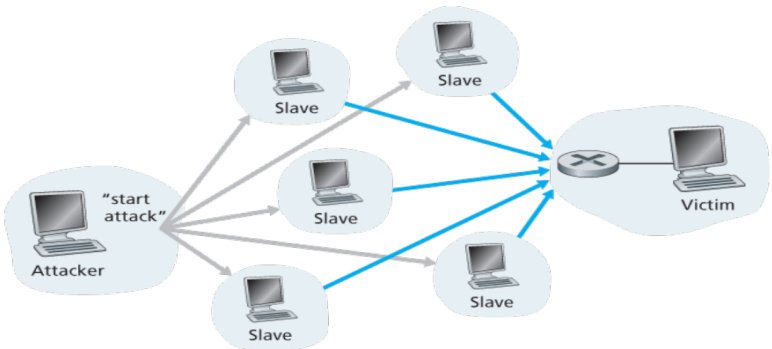
A deluge of packets is sent to the target host. So many packets that the target's access link becomes clogged, preventing legitimate packets to reaching the server.

Networks Under Attack

A distributed denial-of-service attack (DDoS)

To be effective, the deluge of packets must approximate the access rate R of the server. If R is very large a single attack source may not be enough. Also, if all the traffic emanates from a single source, an upstream router may be able to detect the attack and block all traffic from that source.

In a DDoS attack the attacker controls multiple sources and has each source blast traffic at the target. DDoS attacks leveraging botnets with thousand of compromised hosts are common today.



Networks Under Attack

The Bad Guys can

- **Sniff Packets**
  - Many users today access the Internet via wireless devices, which brings a major security vulnerability: a passive receiver near the transmiter can obtain a copy of every packet
  - This passive receiver is called a **packet sniffer** and it makes copies of traffic packets. Sniffed packets can than be analysed offline for sensitive information
  - Sniffers can also be deployed in wired environments

Networks Under Attack

The Bad Guys can use

- **Packet Sniffers**
  - Can also be deployed in wired environments

    A bad guy who gains access to an institution's access router (or link) may be able to plant a sniffer that makes a copy of every packet going to/from the organization
  - Are passive, they do not inject packets into the channel.

    They are dificult to detect

Networks Under Attack

Sniffing a switched LAN

When a host is connected to a switch, it only receives frames that are intended for it. When host A sends a frame to B (and there is an entry for host B in the switch table) the frame will be forwarded only to B. If host C is running a sniffer, C will not be able to sniff this A-to-B frame.

Thus, **in a switched-LAN environment** (in contrast to a broadcast link environment such as hub-based or 802.11 LANs) **it is more difficult** for an attacker **to sniff frames**.

However,
because the switch broadcasts frames that have destination addresses that are not in the switch table, the sniffer at C can still sniff some frames that are not intended for C.

A sniffer will be able to sniff frames with destination address FF-FF-FF-FF-FF-FF.

Networks Under Attack

Sniffing a switched LAN:

Switch Poisoning

This is a well-known attack against a switch. Consists in sending tons of packets to the switch with many different bogus source MAC addresses, thereby filling the switch with many different bogus source addresses and leaving no room for the MAC address of the legitimate hosts.

This causes the switch to broadcast most frames, which can then be picked up by the sniffer

Networks Under Attack

The Bad Guys can

- **Masquerade as Someone You Trust**

  It is easy to create an hand-crafted packet with an arbitrary source address, packet content, and destination address, and then transmit it into the Internet, which will forward the packet to its destination.

  The receiver (say, a router) will take the (false) source address as being truthful, and then performs some command embedded in the packet's contents (say, modify its forwarding table).

The ability to inject packets into the Internet with false source address is known as

IP spoofing

and is one of many ways in which one user can mascarade as another user

Networks Under Attack

- **How the Internet** became such an insecure place?
  - It was originally designed to be that way, based on a model of a *"group of mutually trusting users attached to a transparent network"*
  - The ability for one user to send a packet to any other user (default) reflets this notion of mutual trust.

Networks Under Attack

- **How the Internet** becom
  - It was originally designed t
    "group of mutually trusting
  - The ability for one user t
    reflets this notion of mu

But today's Internet
does
not
involve
"mutually trusting users"

Networks Under Attack

- **Although the Internet** is such an insecure place
  - Users still need to comunicate
  - May wish to communicate anonymously
  - May communicate indirectly through third parties
  - May distrust the hardware, software, and even the air

We have many security-related challenges

We should seek defenses against…

Networks Under Attack

- **Although the Internet i**
  - Users still need to comunic
  - May wish to communicate
  - May communicate indire
  - May distrust the hardw

  We have many secr

  We should seek de

Sniffing
End-point masquerading
Man-in-the-midle attacks
DDoS attacks
Malware

(and more...)