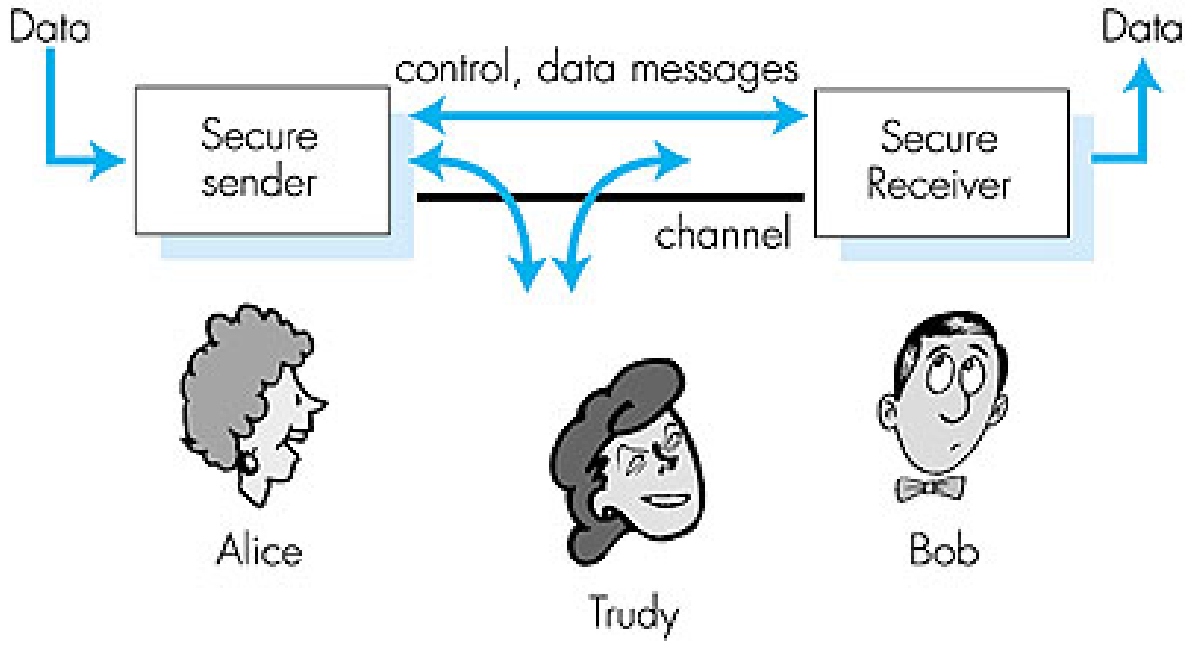
Network security

Terminology

What is security?

- Security is keeping unauthorized entities from doing things you don‘t want them to do...
- This definition is too informal

Scenario



- Well-known in network security world
- Friends and enemies: Alice, Bob, Trudy/Eve
- Bob, Alice want to communicate "securely" (they maybe "lovers")
- Trudy/Eve, the "intruder", the "evil person" may intercept, delete, add messages

What is security (2.)?

- Confidentiality
- Integrity
- Availability

(Definitions from [RFC 2828], Trust in Cyberspace)

Confidentiality

- Confidentiality: „The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]."
- Not the same as *privacy!*
- Privacy: „the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others."
- Privacy is a reason for confidentiality!

Integrity

- Data integrity: „The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.“
- System integrity: „The quality that a system has when it can perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.“

- Often of more commercial interest than confidentiality

Availability

- Availability: „The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.“

- Turning off a computer provides confidentiality and integrity, but hurts availability...
- Denial of service attacks are direct assaults on availability

Additional terms

- Vulnerability: „An error or weakness in the design, implementation, or operation of a system“
- Attack: „A means of exploiting some vulnerability in a system“
- Threat: „An adversary that is motivated and capable of exploiting a vulnerability“

Vulnerabilities vs. Threats

- Vulnerability
  - Technical failure in a system
  - Primary focus of most computer security classes
  - Close all vulnerabilities => threats don‘t matter?
    Or do they?
- Threats
  - Different enemies have different abilities
  - Teenage joy-hackers can‘t crack modern cryptosystems
  - Serious enemies can exploit the „three B‘s“: burglary, bribery, and blackmail (in addition to social engineering)
  - Cannot design a security system
    unless one knows who the enemy is!

Threats: joy hackers

- Who are they
  - Many are „script kiddies“; some are very competent
  - ⇒ The scripts are very sophisticated
  - The hackers share tools more than the good guys do!
- Are they a problem?
  - What would it cost you to rebuild a machine?
  - What would your CEO say if you ended up on the front page of the NYTimes / Welt?
  - What if they’re working for someone else?
  - Their target selection has improved

Threats: hacking for profit

- Hackers have allied themselves with the spammers and the phishers
- Primary motivation for most current attacks: money!
- The market works – the existence of a profit motive has drawn new talent into the field
- We are seeing, in the wild, sophisticated attacks
- We are seeing less pure vandalism
- Most of today's worms and viruses are designed to turn victim computers into „bots"

Threats: organized (disorganized) crime

- Often hacking is just another venue for ordinary criminal activity
- The same people who hack
  - Steal credit card numbers
  - Launder money
  - ...

Threats: industrial espionage

- Less than 5% of attacks are detected

- Professionals who are after you won't use your machine to attack other companies, and that's how successful penetrations are usually found
- Professionals are more likely to use non-technical means, too:
  - social engineering, bribery, etc...
- Professionals tend to know what they want

Threats: inside jobs

- Insiders know what you have
- Insiders often know the weak points
- Insiders are on the inside of your firewall
- ....

⇒ What if your system administrator turns to the „Dark Side“???

Threats: spies

- Governments may want your technology
- Some governments lend tangible support to companies in their own countries
- Spies tend to be sophisticated, well-funded, etc.
- What about cyber warfare?

Threats: why does it matter?

- You have to build your defenses accordingly
- Security is fundamentally a matter of economics
  - How much security can you afford?
  - How much do you need?

Assets: what are you protecting?

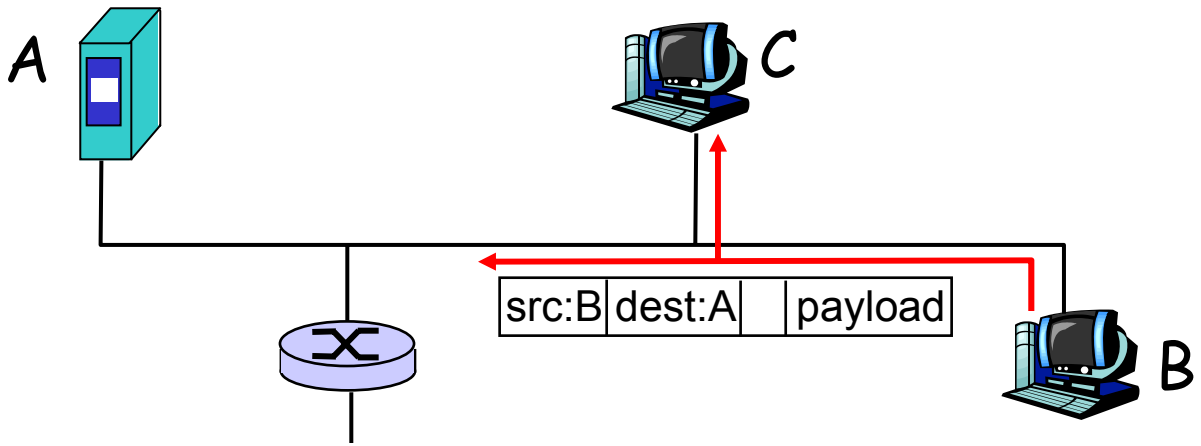
- Host-resident data?
- Bandwidth?
- CPU time?
- Knowledge of what hosts exist?
  - Network scans
  - Why (1)? The # of computers == # of people
    How large is your competitor?
  - Why (2)? Attack power
    MAC addresses can only be determined on-LAN
    Does the attacker have this ability?

Attacks

- Bandwidth attacks
  - Clog your bandwidth via DoS attacks
  - Use your bandwidth to attack someone else, e.g.,
  - Reflector attacks:
    - UDP-based service where response is > than request
    - Forge source address to victims address
  - Network identity attack:
    - Run the server with illegal content on hacked machine
  - Eavesdropping
    - Pick up traffic, e.g., passwords/credit cards via sniffer
    - Done to major backbones in 1993-4
    - e.g., http://monkey.org/~dugsong/dsniff/

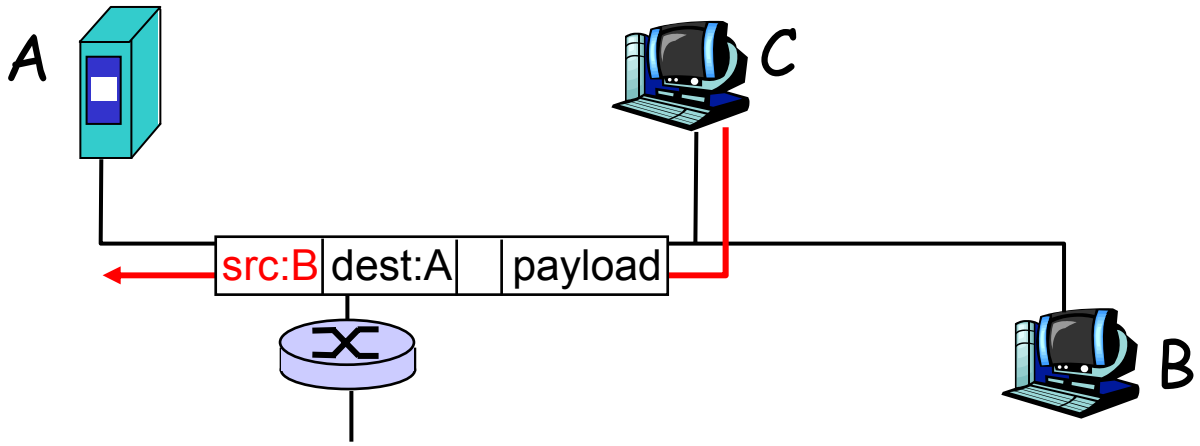
Packet sniffing: how

- Easiest case: broadcast media
- Promiscuous NIC reads all packets passing by. Can read all unencrypted data (e.g., passwords)
- E.g.: C sniffs B's packets



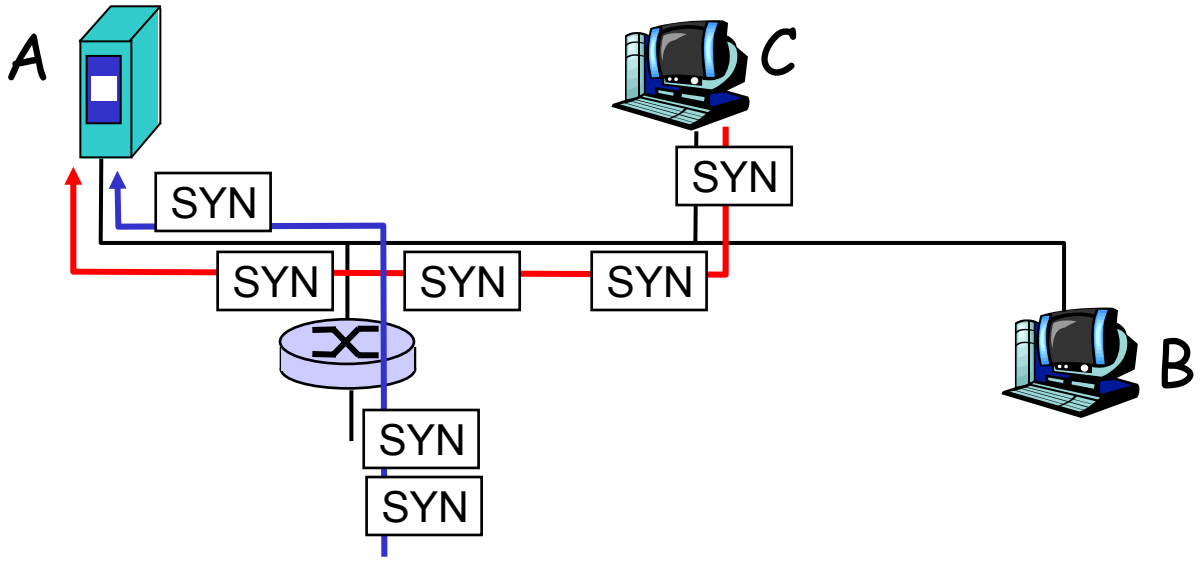
IP Spoofing: how

- Can generate "raw" IP packets directly from application, putting any value into IP source address field
  - Receiver can't tell if source is spoofed
  - E.g.: C pretends to be B



Denial of service attack: how

- Maliciously generated packets "swamp" receiver
- Distributed DoS (DDoS):
  multiple coordinated sources swamp receiver
- E.g., C and remote host SYN-attack A



Vulnerabilities:

- Dichotomy: Host vs. network
- We deal with both!
- We need protect against both
- Techniques differ

Vulnerabilities: hosts

- Goal: keep the bad guy from penetrating the networked host (generally via a buggy application)
- If a penetrated application is used to break host security, it is probably an OS and application security issue
- If the application itself can be tricked into doing nasty things, it is probably a network security problem
- No clean categories

Vulnerabilities: network

- What can the attacker do?
- Where is the attacker located?
- What are you trying to protect?

Vulnerabilites: different network layers

- Examples
  - Link layer: ARP-spoofing
    - ARP: maps IP addresses to Ethernet addresses
    - Another machine can reply: first reply generally wins
  - Transport layer: TCP sequence number guessing
    - Initial sequence number (ISB) used to be incremented by some constant k after each connection and every half-second
    - X opens legitimate connection to S to learn ISB
    - X can now impersonate T
      - Spoofs T's source IP
      - Blocks RST from T

Protecting a network

- Analysis
  - What are you trying to protect?
  - Against whom?
  - Enumerate vulnerabilities
  - Deploy protective measures

Protection mechanisms

- Replace vulnerable mechanisms by strong ones
  Example: address-based authentication with cryptography
- Use filters or firewalls to limit access to important but insecure services
  Example: no not permit outside access to Windows file-sharing ports
- Use procedural mechanism as last resort
  Example: there is no way to block ARP-spoofing
  $\Rightarrow$ have to keep would-be spoofers of your LAN (the attack only works locally)

Human element (important!)

„Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed, but they are sufficiently pervasive that we must design our protocols around their limitations."

Kaufman et al.

Course overview

- Introduction
  - Attacks and threats, cryptography overview
  - Authentication (Kerberos, SSL)
- Applications
  - Web, email, ssh
- Lower layer network security
  - IPsec, firewalls, wireless
- Monitoring / information gathering
  - Intrusion detection, network scans
- Availability
  - Worms, denial of service, network infrastructure