Security part

13.2. Vulnerabilities and attacks

Vulnerabilities

- Vulnerabilities appear everywhere in the stack
  - Modern systems are very large and complex
  - Impossible to test all possible use cases in advance
- Long history of
  - Network protocol vulnerabilities
  - OS vulnerabilities
  - Application vulnerabilities
    - Browsers, web servers, database mgmt systems, mail programs
    - Web apps (see OWASP Top 10)
    - Mobile apps
- Also non-technical vulnerabilities”
  - Social engineering
  - Illness, loss of personnel
  - Power failure, comms problems, fire, flood, earthquake, …

Human vulnerabilities (Social Engineering)

- Social engineering is the practice of manipulating legitimate users
- Users are tricked into providing passwords or other secrets or allowing the attacker to bypass security
- Can be very effective
  - Typically tried in bulk on a large number of users in the hope that a few users will fall for it
  - Sometimes very subtle

- Best defence is security awareness training
  - See SANS ”Securing the Human” project:
  - http://securingthehuman.sans.org/

Malware: risks from insecure programs

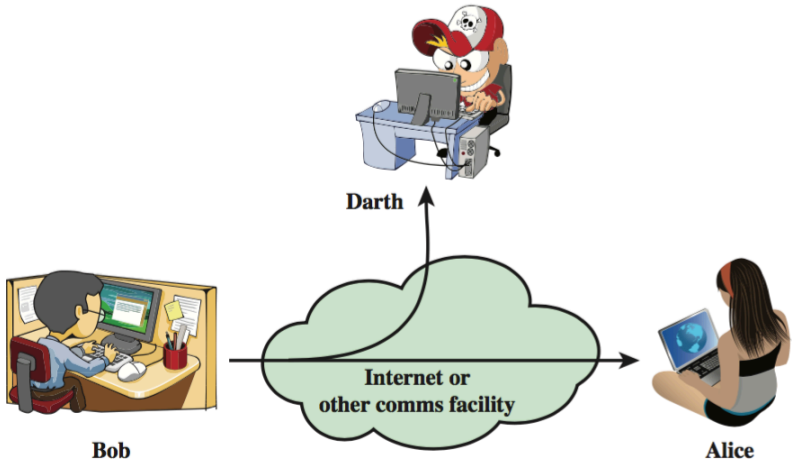
- Anything that can be executed on a machine may have all the rights and privileges of the user who is (directly or indirectly) executing it
- This may include
  - Read/write/modify/create/delete files or data
  - Reading from input devices (e.g. keyboard)
  - Writing to output devices
  - Interacting with the user
  - Administrative tasks like creating user accounts, opening/closing ports, launching other programs
  - Connection to other networked machines, file transfer, send emails, etc

Types of Attackers

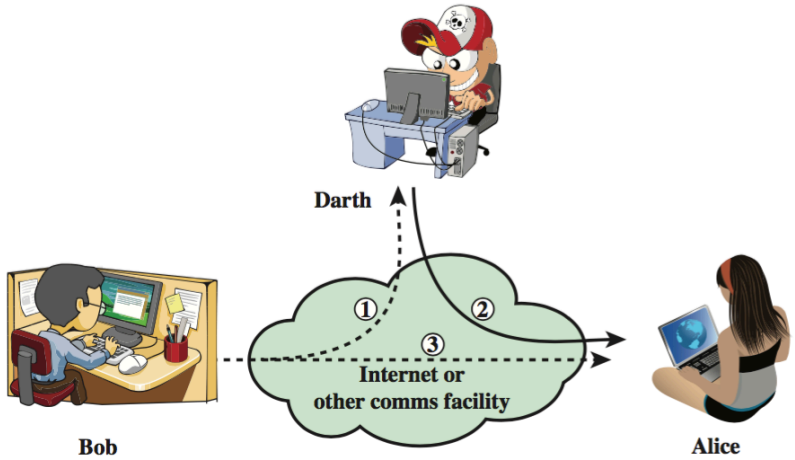
- Opportunists
  - Typically scan wide range of addresses looking for system to exploit
  - For fun; to vandalise; to store pirated movies, music, etc
- Professionals
  - Industrial espionage; Fraud; Spam
- Activists
  - Political or social motivation
- Disgruntled current and former employees and contractors
  - May be able to bypass security measures – via legitimate accounts, accounts left open, back doors, etc
- Worms and automated agents
  - Malicious software

Classification of Attacks

- Passive Attack
  - Eavesdropping or monitoring to:
    - Obtain message contents, or
    - Monitor traffic flows



- Active Attack
  - Modification of data stream to:
    - Masquerade as someone else
    - Replay previous messages
    - Modify messages in transit
    - Denial of service
  - Break into system



Passive attack: Sniffing

- Sniffing on a network
  - Easy to do on broadcast LAN if attacker can get physical access to network point
  - Wireless LANs often have no encryption or broken encryption (e.g. WEP)
  - WAN security varies

- Keystroke logging
  - Keystroke logging software may be installed by virus or directly by attacker.
  - Alternatively, can insert small piece of hardware between keyboard and computer

KeyGhost USB KeyLogger : M

www.keyghost.com/USB-Keylogger.htm

KEY GHOST
THE HARDWARE KEYLOGGER

Interface Security

THAWTE Authentic Site Secured by SSL

Ordering | Customer Support | Products | Company Info | Links | Helpdesk

We welcome

VISA

MasterCard AMERICAN EXPRESS

Home - Site Map

- Home
- Products
- Reviews
- Demonstration
- Testimonials
- Photos
- Specifications
- FAQ
- Press releases
- Download
- Legal Disclaimer
- Affiliates
- Distributors

NEW! QIDO - Qwerty to Dvorak USB Adapter.

QIDO
Qwerty-In > Dvorak-Out

Our latest development in

KeyGhost USB Keylogger

World's first keylogger for Mac and PC USB keyboards.
Simply plug it in and record keystrokes.
Works with 100% of all USB keyboards!

NEW! TimeDate USB/HUB KeyGhost device released.

High-capacity and compact.
NEW! Plug-style USB KeyGhost devices released.

KeyGhost devices are always designed in consultation with leading law enforcement and government officials.

You can be certain that a KeyGhost product will always work as described.

NATO Classification Information
KeyGhost LTD (NATO supplier) NCAGE Code E1969

The plug-style KeyGhost USB devices look similar to USB Thumb Drives and record all keystrokes typed on any USB keyboard (Mac or PC).

KeyGhost Headlines

KeyGhost USB Keylogger
"Customer satisfaction guaranteed" 12-Month Manufacturers Warranty.
Order now

Stages of an active attack – the five Ps

- Probe
- Penetrate
- Persist
- Propagate
- Paralyse

Stages of an attack – Probe

- Reconnaisance
  - Public information – Whois, DNS, target company website, search engines
  - Maltego
  - “Google hacking”
  - Social engineering

- Sniffing & scanning
  - Listen on broadcast (W)LANs; NetStumbler, Wireshark
  - Key logging
  - Network mapping
  - Port scanning; Nmap
  - Software version mapping
  - Vulnerability scanning

Stages of an attack – Penetrate

- Finding secrets
  - Password guessing & grinding (brute force cracking)
  - Malware (virus, Trojan, rootkit, etc)
- Spoofing
  - IP address / MAC address
- Session hijacking
- DNS cache poisoning
- Malformed input
  - Buffer overflows, format string attacks, …
- Web app attacks
  - SQLi, XSS, CSRF, …
- All of the above; Metasploit framework

Stages of an attack – Persist

- Having gone to the trouble of breaking in, the attacker wants to get back in easily
- Back door for remote control
  - Install small service listening on port and providing access (e.g a shell)
  - or else a small client that “dials out”
- Trojan horse
  - Malicious software often disguised as something innocuous
- Rootkit
  - Trojan suite that hides itself by suppressing logging and monitoring tools
- Covert channels
- Steganography

Stages of an attack – Propagate

- Use newly compromised system as the source of further attacks – more sniffing and scanning (see “Probe”)
- Map internal network from compromised machine.
- Often internal resources are configured to trust each other, making it easier to attack.

Stages of an attack – Paralyse

- The attacker does some damage – stealing or destroying data, bringing systems down, etc.
- Access confidential data
  - By sniffing, malformed input, web app attacks, etc (see “Probe”, “Penetrate”)
- Integrity breach
  - Modify/corrupt data
- Denial of Service (DoS)
  - where one user takes up so much of a shared resource that little or none of the resource is left for others.
  - These resources can be CPU time, disk space, OS processes, network bandwidth, or even someone’s time.
  - Examples: Amplifier attacks, Distributed DoS