Security in Computing & Information Technology

Lecture 2

Vulnerabilities, Threats, Attacks

Lecture Schedule

Foundations

1. Introduction
2. Vulnerabilities, Threats, Attacks

Basic mechanisms

3. Security mechanisms, Elementary cryptography
4. Authentication
5. Access control

Major computing security areas

6. Operating systems
7. Databases
8. Networks
9. Web
10. Mobile computing

Applications

11. Privacy
12. Internet banking

Lecture Topics

- Vulnerabilities, threats
- Attack methods, exploits

Know the Enemy

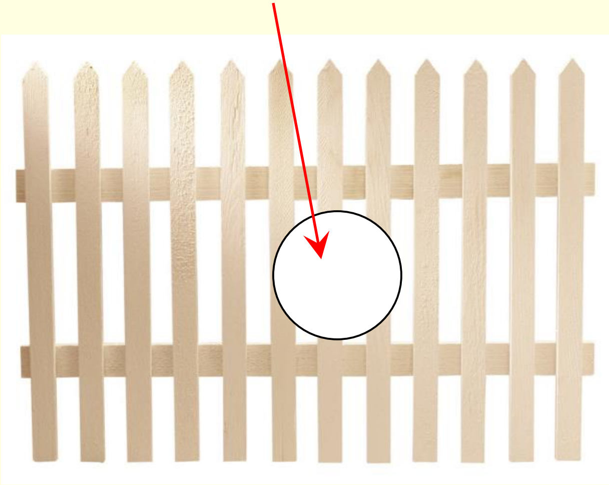
- Terminology
- Attack motives
  - Who are attacking computer systems?
  - What do they want to achieve?
- Attack methods
  - Techniques to compromise computer systems
  - Consequences

Vulnerabilities & Attacks (1)

Terminology

Exploit
Go through hole

Vulnerability
Hole in the fence



Threat agent
Thief

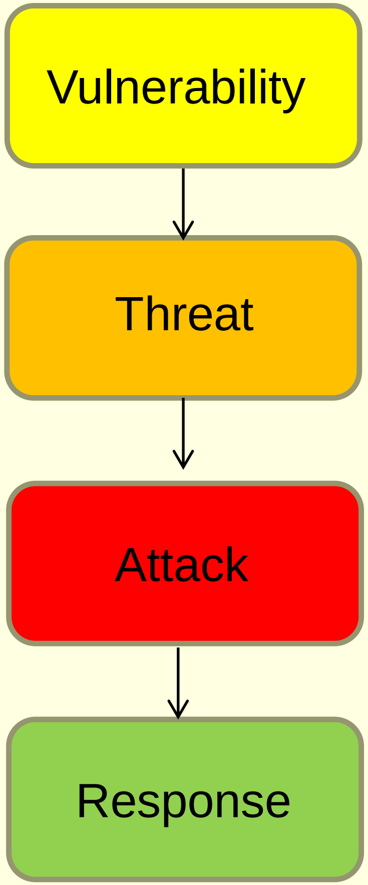
Threat
Loss of stereo

Vulnerabilities & Attacks (2)

- Vulnerability
  - A weakness in the application (design flaw, bug, misconfiguration …)
  - Allows an attacker to cause harm
- Exploit
  - Technique that allows the attacker to take advantage of vulnerabilities
- Attack
  - Use of an exploit
- Threat
  - The potential of a harmful event
- Threat agent

  Threat Agent = Capabilities + Intentions + Past Activities

Vulnerabilities & Attacks (3)



- Current software development methods cannot eliminate all vulnerabilities
- It is possible to exploit these weaknesses
- Someone then exploits a weakness
- After an attack, normal operation has to be restored (and vulnerability fixed)

Common Vulnerability Scoring System

Commonly known as CVSS

- Standardized method to assess security vulnerabilities
- Scoring is based on a number metrics in three main categories
  - Base

    Immutable features of a core vulnerability
  - Temporal

    Evolve during the lifetime of the vulnerability
  - Environmental

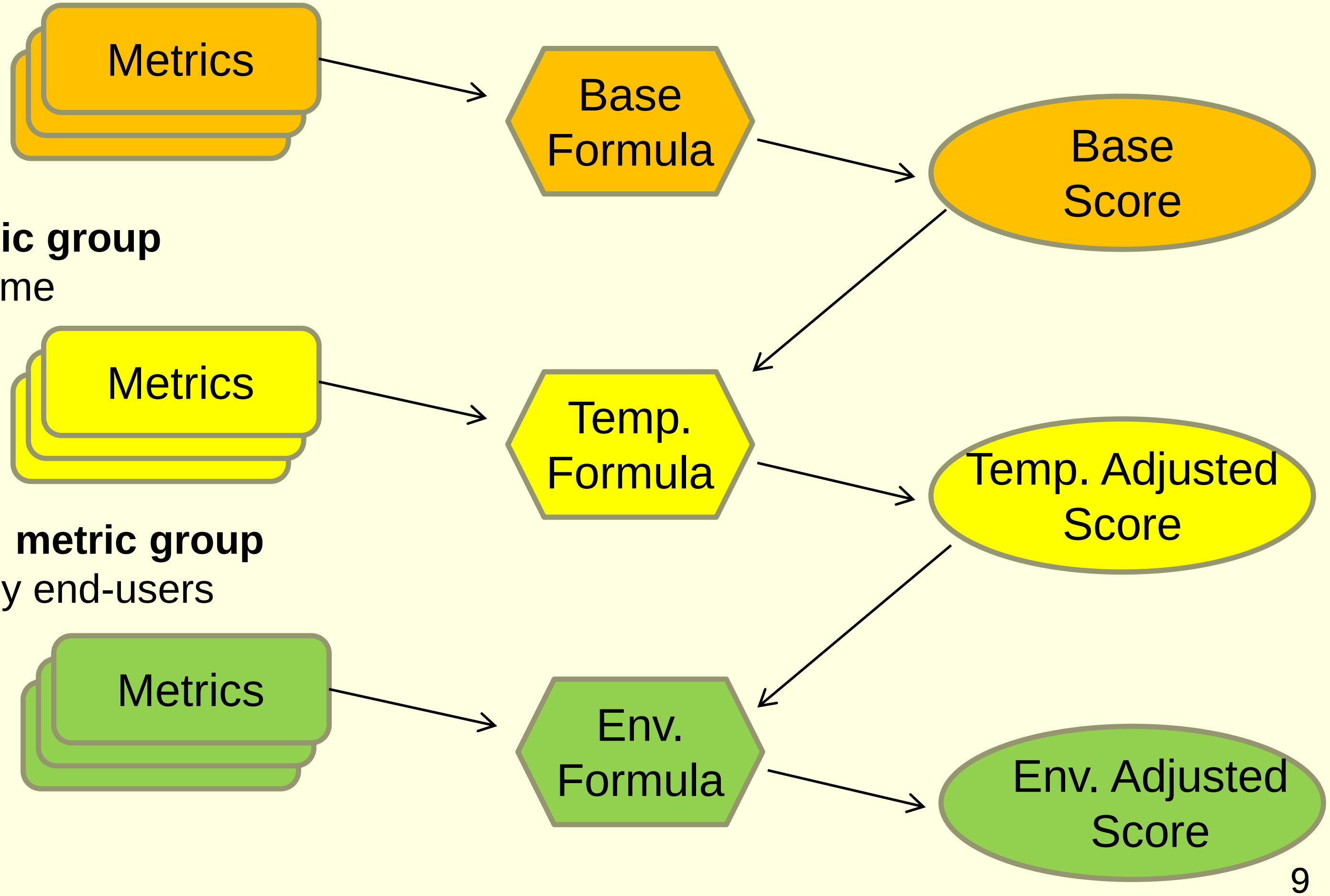
    How the vulnerability affects a particular installation

The CVSS Calculation Process

Base metric group
Once set, it doesn't change

Temporal metric group
Changes with time

Environmental metric group
Optionally set by end-users



CVSS Base Score

- Indicates general severity
- Represents the innate characteristics of the vulnerability, and not expected to change
- Has the strongest influence on the final score
- Main metrics
  - Exploitability
    - Access vector (e.g. local or remote) and access complexity (high – low)
  - Impact
    - None, partial or complete loss of
      - confidentiality, integrity, availability

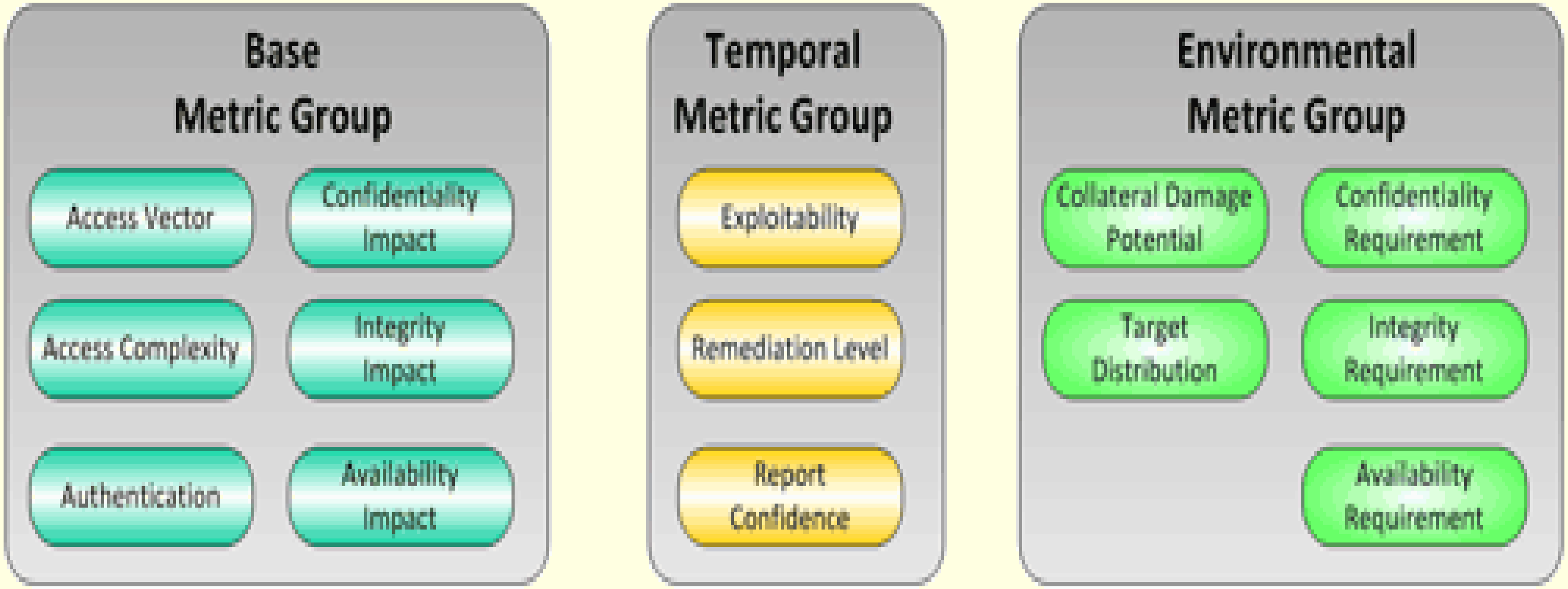
CVSS Temporal Score

- Represents changes over time
- Introduces mitigating factors that usually decrease the final score
- Expected to be re-evaluated periodically
- Indicates urgency
- Main metrics
  - Exploitability
    - Theoretical, proof of concept exists, functional (works for most situations), high (always works)
  - Remediation
    - Official/temporary fix, workaround, not available

CVSS Environmental Score

- Represents vulnerability in an installation
- Addresses deployment and configuration
- Defined by consumer / end-user
- Indicates overall priority
- Main metrics
  - Collateral damage potential
  - Target distribution
    - Number of systems vulnerable in a particular environment

CVS Metrics Groups (Summary)



Set by bulletin analysts, product vendors

Set by end user

Image source: http://www.first.org/cvss/cvss-guide

Threat Assessment

- Aim: identify system vulnerabilities, assess the risk of threats, define an effective mitigation plan
- Complex task, requires expertise
- Tools can help a systematic approach
  - Tool examples
    - Microsoft Threat Analysis and Modeling (TAM)
    - ThreatModeler (http://myappsecurity.com/)
    - Practical Threat Analysis (PTA) Tool (http://www.ptatechnologies.com/)
    - Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM} (OCTAVE) (http://www.cert.org/octave/)

Attack Vectors & Attack Surface

- Attack vector: a way/route/method of triggering or reaching a vulnerability
  - E.g. malicious email, attachments, worms, web pages, downloads, deception (aka social engineering)

    Different from malicious payloads (e.g. viruses, trojans, malicious scripts)
  - Attack vector analysis is useful for
    - understanding the severity of a vulnerability
    - defence (e.g. allows the blocking of certain inputs)
- Attack surface: a sum of different attack vectors threatening a software environment
  - Reducing the attack surface improves security
- Zero-day attack
  - Attack (method) exploiting a vulnerability that has no defence/solution/fix yet

Attack Motives

- Criminal intent

  Financial gain
- Espionage
  - Industrial
  - Military
- Prove a point

  E.g. disclose a vulnerability
- Vendetta, revenge
- Terrorism
- Hate

Common Attack Methods

- Passive attacks

  Obtain information in an unauthorised manner

  - Privacy violation
    - Targeted attack

      E.g. gain information about a specific bank account
    - Data harvesting

      E.g. collect credit card numbers/email addresses
  - Publicity attacks

    Attack for the sake of publicity, e.g. press
- Active attacks

  Interfere with the operation (e.g. manipulate objects)

Criminal Attacks

- Fraud

  Deception for personal gain
- Scam

  Fraud committed after gaining the victim's confidence
- Destructive attacks

  E.g. erase a database or parts of it
- Theft
  - Intellectual property

    Intangible property, e.g. invention, trade mark, original design
  - Identity

    Someone masquerading as another person
  - Brand

    Using the brand-name of someone else, e.g. in a forged web page
- The law changes much slower than life in the digital world

Most Frequent Attacks

- Theft of information
  - Private data (bank account number, password, …)
    - Spyware: collects information without the user's knowledge (e.g. keyloggers)
- Theft of resources
  - Computer hijacking
    - Botnet: network of computers that can be remotely controlled without the lawful owner's knowledge; used e.g. for spamming, DoS attacks
- Interfering with the operation
  - Denial of service (DoS)
    - Overwhelming the target with bogus requests and making it inaccessible for legitimate users

Common Attack Strategies

- Attacker’s aim
  - To “own” the target machine
    - have privileged (root/administrator) access
    - execute programs in privileged (kernel) mode
- Infiltration method
  - Social engineering
  - Exploit root-level flaws
  - Exploit lower-level flaws and escalate privileges via other exploits
- Dissemination of malware
  - Virus (needs a host to spread, e.g. via infected emails, data, …)
  - Worm (spreads on its own)

Other Malware

- Trojan horse
  Code doing what it is supposed to do, plus something else
- Trapdoor
  Access to services by non-standard methods
- Logic bomb
  Dormant malicious code, waiting for a triggering event
- Easter egg
  "Cute" but harmless behaviour triggered by special input

Authentication (Password) Attacks

- Dictionary attack
  - Testing correct words (e.g. from a dictionary)
- Replay attack
  - Using data from an earlier, recorded, valid session
- Password guessing
  - Relies on intuition
- Password sniffing
  - Having access to and monitoring a valid session

Other Prevalent Attacks

- Spoofing
  - Masquerading as someone else by falsifying data
  - Spoofing Attacks
    - Phishing

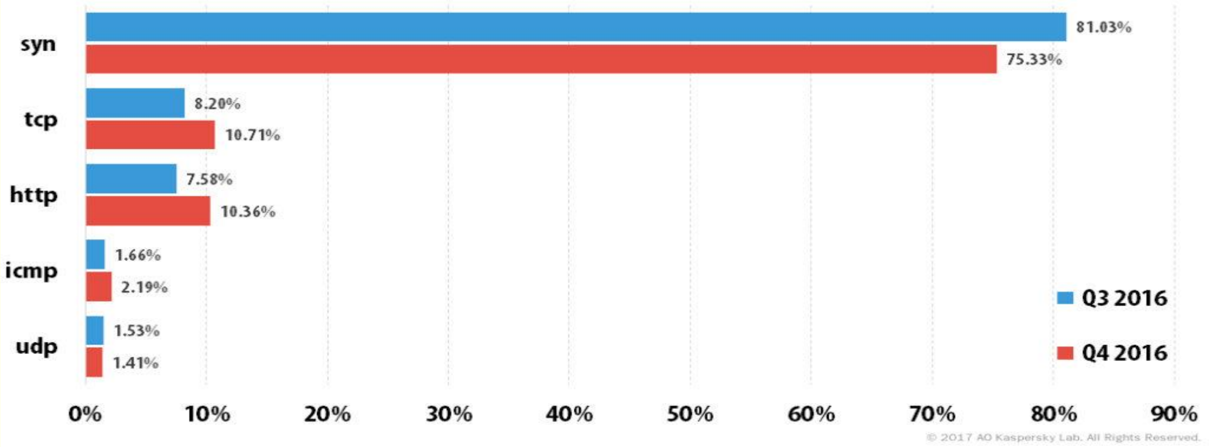
      Tricking the user into volunteering confidential information
- Denial of service (DoS) attacks
  - Direct attacks: overwhelming traffic from attacker to victim
  - Reflected attack: sending a spoofed packet (the victim is shown as the source) to many hosts, the responses overwhelming the victim
  - Distributed DoS (DDoS) attacks
    - Using a network of machines (botnets) for a DoS attack

DDoS Attack Types

- Volume based attacks
  - Method: bandwidth saturation
  - E.g. UDP/ICMP floods (usually spoofed packets)
- Protocol attacks
  - Method: server resource attack
  - E.g. SYN floods, fragmented packets, smurf
- Application layer attacks
  - Method: crash the application
  - E.g. GET/POST floods

DDoS Statistics

- Attack type



- Attack length

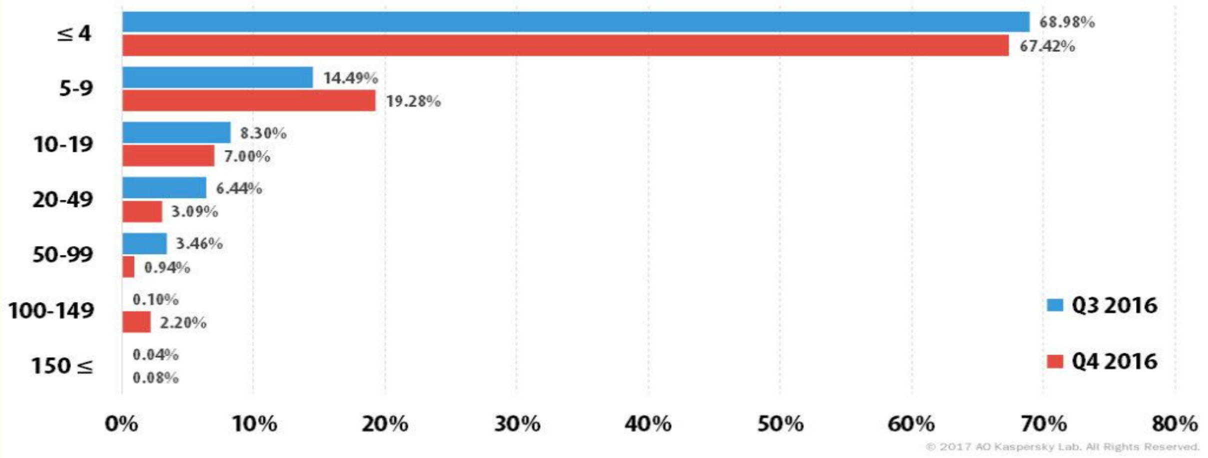


Image source: https://securelist.com/analysis/quarterly-malware-reports/77412/ddos-attacks-in-q4-2016/

Botnets

- Network of compromised computers
- Controlled from a single command point
- Features
  - Well organised hierarchy of computers
  - Workers at the bottom layer
  - Infected computers are zombies – activated by a central command
  - Attack/malicious activity method by the same computer can vary
  - Workers back off randomly, to disguise themselves
- Use
  - Honest use - rare
    - E.g. Distributed computing
  - Malicious use – most often
    - Spam mailer
    - DDoS attack tool

Botnet Platforms

- Internet of Things (IoT) used as bots/zombies
- Most IoT devices use embedded Linux with low security

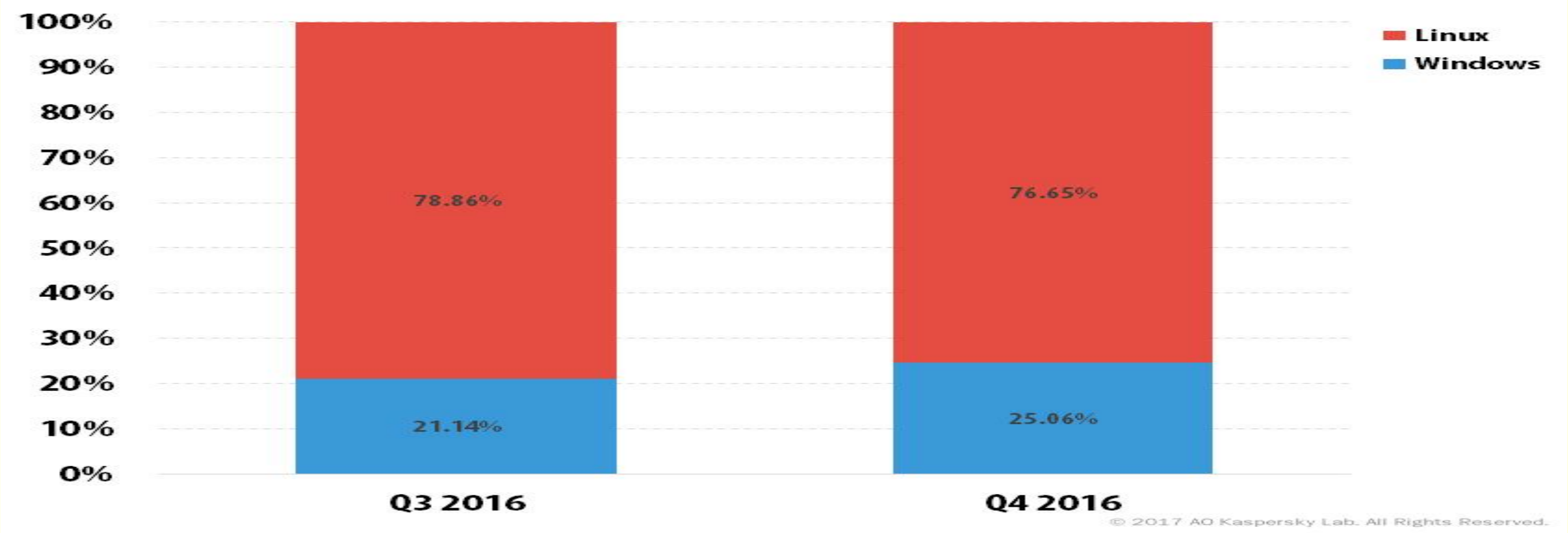


Image source: https://securelist.com/analysis/quarterly-malware-reports/77412/ddos-attacks-in-q4-2016/

Attack Techniques

- Injection attacks
  - Exploiting the input vulnerability of data not being checked or sanitised properly
- Rootkits
  - Malware that hides its presence via modifying system data
- Social engineering
  - Exploiting human gullibility to extract confidential information

Injection Attacks

- Code injection

  Inserting code that is interpreted by the application

  - Command

    Execute system commands by the application and have the application's privileges

  - SQL injection

    Inserting a database query via the input of the application

  - XML injection

    Inserting XML content or structures into a message, e.g. to alter the intended logic of the application

  - Cross-site scripting

    Malicious scripts inserted into benign and trusted web sites

Rootkits

Attempt to hide the presence of malware

- Windows
  - DLL injection (malware loaded into the victim's process), any reference to the malware can be removed before returning control to the real user code
  - Installed as device drivers
- Unix (linux)
  - Simple method: replaces system binaries with the rootkit's version of them
  - Others imitate Windows rootkits

Social Engineering

- Manipulating others into revealing information that can be used to steal data, access to systems, money or even your identity
- Aims at extracting information without raising any suspicion
- Exploits human “vulnerabilities”
  - People are the weakest link in the security chain
- Social engineering is the most effective method for getting around security obstacles
- The hardest form of attack, it cannot be detected by hardware or software alone

Social Engineering Methods

- Human based
  - Methods
    - Phone call
      - to helpdesk by impersonating a legitimate (important) user, or referring to tech support by using names
      - to a user by impersonating tech support
    - In person
      - Shoulder surfing: watching what others are typing
      - Dumpster diving: going through the trash
- Computer based

  Phishing: asking the user to verify account details
  - Methods
    - Popup windows: pretend to have an error
    - Spam, hoaxes
    - Websites offering something free or a chance to win something

Psychology of Social Engineering

- Preys on human nature's qualities
  - desire to be helpful
  - tendency to trust people
  - fear of getting into trouble
- Uses different methods to facilitate conversation
  - Humour, compliments
- Relies on persuasion
  - Directly via systematic, logical arguments
    - To stimulate a favourable response

      E.g. "The head of department has asked me to collect …"
  - Using peripheral cues, misrepresenting objectives
    - To trigger acceptance without thinking

      E.g. Person wearing a shirt with a logo of a relevant company

Social Engineering Exploits

- Contrived situation
  - Inventing several factors to improve plausibility (forgot a password, looming deadlines, …)
- Personal persuasion
  - Employed to overcome initial resistance
  - Seeks voluntary action instead of forcing compliance
  - Target believes they are making the decision
- Request methods
  - Direct request
    - Often challenged and refused, and hence
    - Rarely used
  - Context-aware request
    - The perpetrator sets up a scenario (e.g. cuts a cable) then offers help

Responding to Incidents

- Steps
  1. Detection

     Includes identification of the attack
  2. Containment

     Prevention from causing damage and from spreading (quaranteen)
  3. Eradication

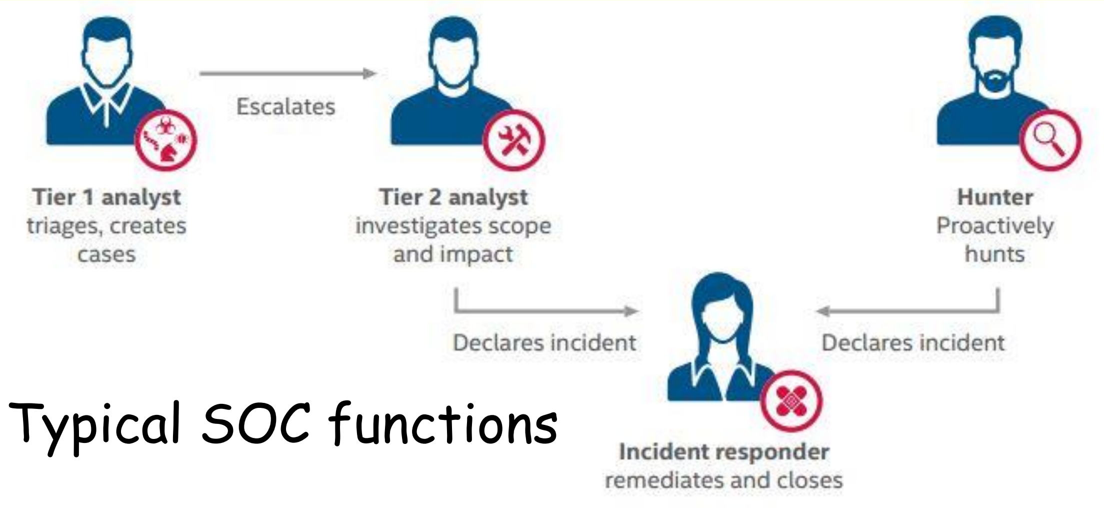
     Remove the agent
  4. Recovery

     Restore the normal operation
- Response tools
  - Assist or automate some of the steps

    E.g. antivirus programs automate steps 1-3

Security Operation Centre (SOC)

- Facility where information systems are monitored, assessed and defended
- Passive defense
  - Monitoring to detect intrusions
- Active defense
  - Testing the system's vulnerability (aka penetration (pen) testing)



Typical SOC functions

Image source: http://www.mcafee.com/au/resources/reports/rp-quarterly-threats-dec-2016.pdf

Incident Response Organizations (1)

Provide general support to local incident response teams

- Computer emergency response team (CERT)
  - Analyses and studies software vulnerabilities
  - Started at Carnegie Mellon University (CMU)

    Now a coordination centre is located at the Software Engineering Institute of CMU
  - Founded after the first Internet worm (1988)
  - Now a world-wide network of national organizations
    - AusCERT
      - Issues security bulletins and advisories
      - Located at The University of Queensland

Incident Response Organizations (2)

- Forum of Incident Response and Security Teams (FIRST)

  289 teams across 64 countries (6 teams in AU)
- Founded in 1990
- Activities
  - Best practices contests
  - Creates ISO standards
  - Has created a common vulnerability scoring system (CVSS)

Summary

- Computers have become part of everyday life, but security awareness is lagging behind
- Computer security is based on protection against specific threats
- Attacks can be based on specifically crafted programs as well as on old deception methods