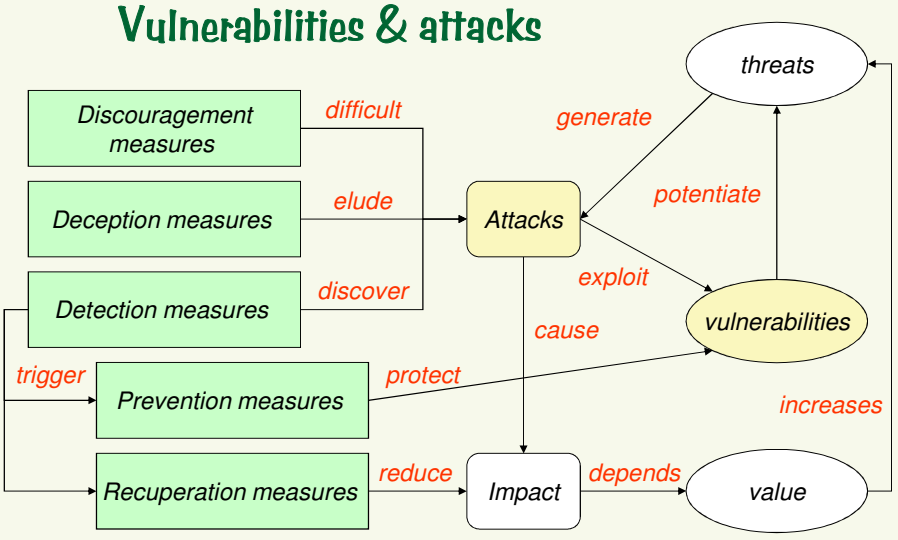
Vulnerabilities

"To know your Enemy,
you must become your Enemy."

Sun Tzu

Information security: Vulnerabilities & attacks



Measures (and some tools)

- Discouragement
  - Punishment
    - Legal restrictions
    - Forensic evidences
  - Security barriers
    - Firewalls
    - Authentication
    - Secure communication
    - Sandboxing
- Detection system
  - Intrusion detection system
    - e.g. Snort
  - Auditing
  - Forensic break-in analysis
- Deception
  - Honeypots / honeynets
  - Forensic follow-up
- Prevention
  - Enforcement of the Principle of Least Privilege
  - Vulnerability scanning
    - e.g. OpenVAS
  - Vulnerability patching
- Recuperation
  - Backups
  - Redundant systems
  - Forensic recuperation

Security readiness (1/3)

- Discouragement, deception and detection measures tackle (mostly) known issues
  - Reconnaissance attempts (e.g. port scanning)
  - Generic attacks (e.g. network eavesdropping)
  - Specific attacks (e.g. buffer overflows)
- Prevention measures tackle well-known and unknown vulnerabilities
  - Generic vulnerabilities
    - e.g. reaction to malformed messages (protocol scrubbers)
    - e.g. stealth attacks (normalization to canonical formats)
  - Specific vulnerabilities
    - e.g. a particular software bug

Security readiness (2/3)

- Measure enforcement requires knowledge about:
  - Known vulnerabilities
    - Problem, exploitation mode, impact, etc.
  - Activity patterns used in attacks
    - *Modus operandi*
    - Attacks' signatures
  - Abnormal activity patterns
    - Abnormal is the opposite of normal ..
    - ...but what's normal?
    - Hard to define in heterogeneous environments

source: flickr

Security readiness (3/3)

- Computer network threats are not like other threats
  - They can be launched anytime, anywhere
  - They can be easily coordinated
    - e.g. Distributed Denial of Service attacks (DDoS)
  - They are cheap to deploy
  - They can be automated
  - They are fast
- Thus, they require a permanent, 24x7 capacity to react to attacks :
  - Teams of security experts
  - Just-in-time attack alerts
  - Security measurement and evaluation
  - Immediate reaction procedures

Zero-day (or zero-hour) attack or threat

- Attack using vulnerabilities which are:
  - Unknown to others
  - Undisclosed to the software vendor
- Occurs at the day zero of the knowledge about those vulnerabilities
  - For which no security fix is available

Vulnerability detection

- Specific tools can detect vulnerabilities
  - Exploiting known vulnerabilities
  - Testing known vulnerability patterns
    - e.g. buffer overflow, SQL injection, XSS, etc.
- Vital to assert the robustness of production systems and applications
  - Service often provided by third-party companies

Vulnerability detection

- Can be applied to:
  - Source code (static analysis)
    - OWASP LAPSE+, RIPS, Veracode, …
  - Running application (dynamic analysis)
    - Valgrind, Rational, AppScan, …
  - Externally as a remote client:
    - OpenVAS, Metasploit, …
- Should not be blindly applied to production systems!
  - Potential data loss/corruption
  - Potential DoS

Survivability

- How can we survive a zero-day attack?
- How can we react to a massive zero-day attack?
- Diversity could be an answer …
  - but software production, distribution and update goes on the opposite direction!
    - And the same happens with hardware architectures
  - Why is MS Windows such an interesting target?
    - And Apple Mac OS not so much?
  - Are you using an Android cell phone?
    - What are the odds of being in the battlefront?

CVE (Common Vulnerabilities and Exposures)

- Dictionary of publicly known information security vulnerabilities and exposures
  - For vulnerability management
  - For patch management
  - For vulnerability alerting
  - For intrusion detection
- CVE's common identifiers
  - Enable data exchange between security products
  - Provide a baseline index point for evaluating coverage of tools and services.

CVE Vulnerability

- A mistake in software
  - that can be directly used by a hacker to gain access to a system or network
- A mistake is a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system
  - This excludes entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system
- A CVE vulnerability is a state in a computing system (or set of systems) that either:
  - Allows an attacker to execute commands as another user
  - Allows an attacker to access data that is contrary to the specified access restrictions for that data
  - Allows an attacker to pose as another entity
  - Allows an attacker to conduct a denial of service

CVE Exposure

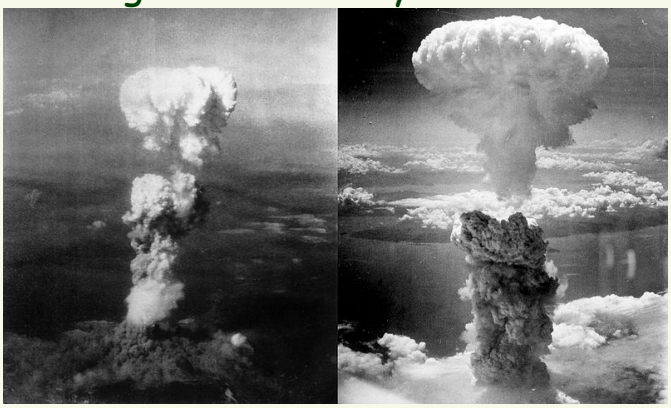
- A system configuration issue or a mistake in software
  - that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network
- A configuration issue or a mistake is an exposure if it does not directly allow compromise
  - But could be an important component of a successful attack, and is a violation of a reasonable security policy
- An exposure describes a state in a computing system (or set of systems) that is not a vulnerability, but either:
  - Allows an attacker to conduct information gathering activities
  - Allows an attacker to hide activities
  - Includes a capability that behaves as expected, but can be easily compromised
  - Is a primary point of entry that an attacker may attempt to use to gain access to the system or data
  - Is considered a problem by some reasonable security policy

CVE benefits

- Provides common language for referring to problems
- Facilitates data sharing among
  - Intrusion detection systems
  - Assessment tools
  - Vulnerability databases
  - Researchers
  - Incident response teams
- Will lead to improved security tools
  - More comprehensive, better comparisons, interoperable
  - Indications and warning systems
- Will spark further innovations
  - Focal point for discussing critical database content issues (e.g. configuration problems)

CVE pitfalls

- Useless against zero-day attacks!



source: wikimedia

CVE identifiers

- Aka CVE names, CVE numbers, CVE-IDs, or CVEs
- Unique, common identifiers for publicly known information security vulnerabilities
  - Have "candidate" or "entry" status
  - **Candidate**: under review for inclusion in the list
  - **Entry**: accepted to the CVE List
- Format
  - CVE identifier number (CVE-Year-Order)
  - Status (Candidate or Entry)
  - Brief description of the vulnerability or exposure
  - References to extra information

Creation of a CVE identifier

1. Discovery of a potential security vulnerability or exposure
   - The information assigned a CVE candidate number by a CVE Candidate Numbering Authority (CNA)
   - CVE identifier is posted on the CVE Web site
     - Which publishes the CVE List
     - This list contains both candidate and entry CVE identifiers
   - CVE Editor proposes the CVE identifier to the Board
     - MITRE Corporation functions as Editor and Primary CAN
2. CVE Editorial Board discusses candidates and votes on whether or not they should become CVE entries
   - If rejected, the reason for rejection is noted in the Editorial Board Archives posted on the CVE Web site
   - If accepted, its status is updated to "entry"

CWE (Common Weakness Enumeration)

- Common language of discourse for discussing, finding and dealing with the causes of software security vulnerabilities
  - Found in code, design, or system architecture
  - Each individual CWE represents a single vulnerability type
  - Currently maintained by the MITRE Corporation
    - A detailed CWE list is currently available at the MITRE website
    - The list provides a detailed definition for each individual CWE
- Individual CWEs are held within a hierarchical structure
  - CWEs located at higher levels provide a broad overview of a vulnerability type
    - Can have many children CWEs associated with them
  - CWEs at deeper levels in the structure provide a finer granularity
    - Usually have fewer or no children CWEs

Seven Pernicious Kingdoms

K. Teipenyuk, B. Chess, & G. McGraw
Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors
IEEE Security & Privacy, 2005

- Input validation and representation
- API abuse
- Security features
- Time and state
- Errors
- Code quality
- Encapsulation
- Environment

Vulnerability databases

- NIST NVD (National Vulnerability Database)
- CERT Vulnerability Card Catalog
- US-CERT Vulnerability Notes Database

CERT (Computer Emergency Readiness Team)

- Organization devoted to ensuring that appropriate technology and systems' management practices are used to
  - Resist attacks on networked systems
  - Limit damage, ensure continuity of critical services
    - In spite of successful attacks, accidents, or failures
- CERT/CC (Coordination Center) @ CMU
  - One component of the larger CERT Program
  - A major center for internet security problems
    - Established in November 1988, after the "Morris Worm"
    - It demonstrated the growing Internet exposure to attacks

CSIRT (Computer Security Incident Response Team)

- A service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity
  - Provides 24x7 Computer Security Incident Response Services to users, companies, government agencies or organizations
  - Provides a reliable and trusted single point of contact for reporting computer security incidents worldwide
  - CSIRT provides the means for reporting incidents and for disseminating important incident-related information
- Portuguese CSIRTs
  - CERT.PT
    - Managed by FCCN
  - CSIRT.FEUP
    - Managed by FEUP
  - CERT-IPN
    - Managed by Lab. de Informática e Sistemas of Inst. Pedro Nunes

Security alerts & activity trends

- Vital to the fast dissemination of knowledge about new vulnerabilities
  - US-CERT Technical Cyber Security Alerts
  - US-CERT (non-technical) Cyber Security Alerts
  - SANS Internet Storm Center
    - Aka DShield (Defense Shield)
  - Microsoft Security Response Center
  - Cisco Security Center

  And many others …