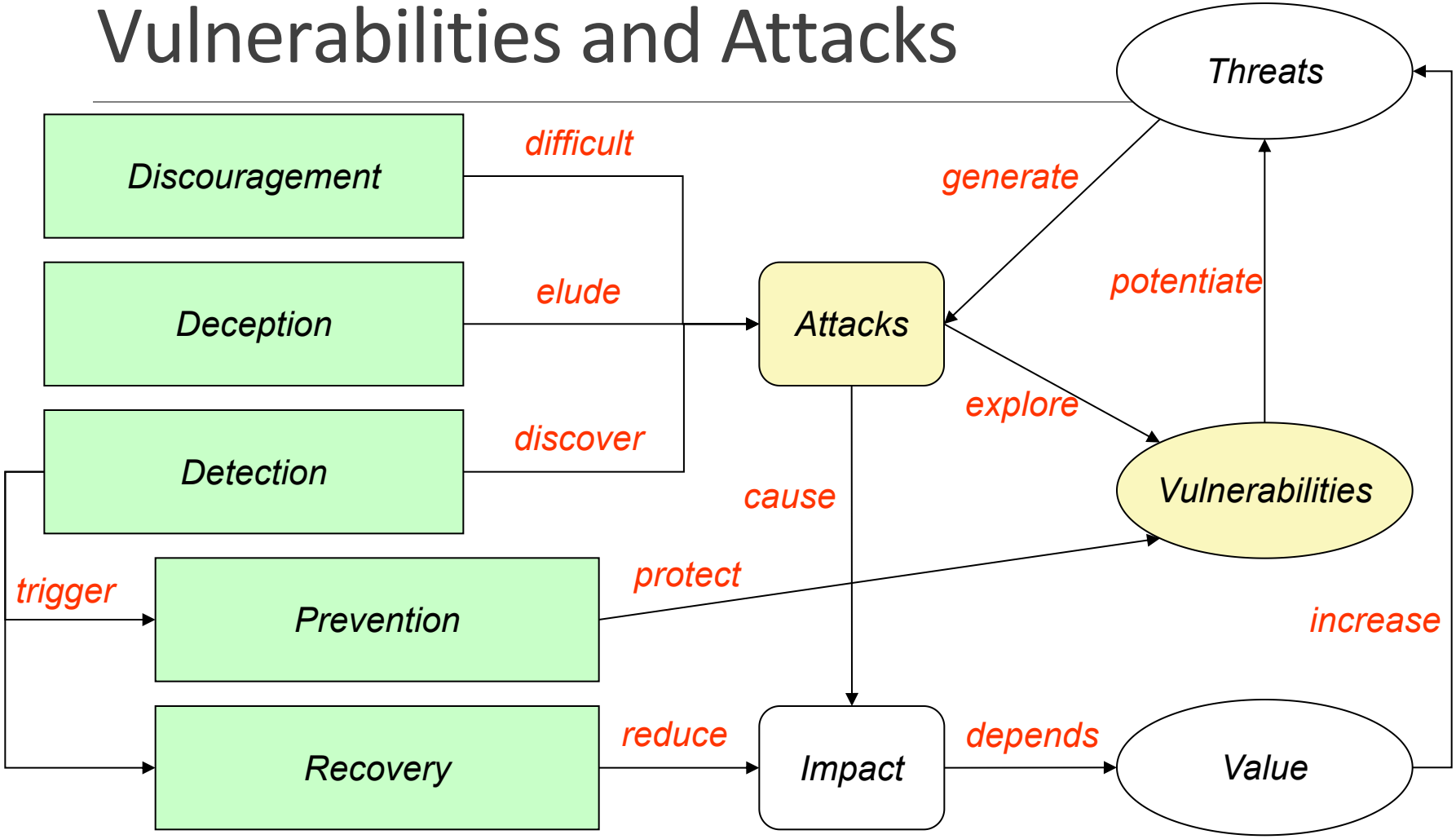
Vulnerabilities

INFORMATION AND ORGANISATIONAL SECURITY

Information Security Vulnerabilities and Attacks



Measures (and some tools)

Discouragement
- Punishment
  - Legal restrictions
  - Forensic evidences
- Security barriers
  - *Firewalls*
  - Autentication
  - Secure communication
  - *Sandboxing*

Detection
- Intrusion detection system
  - e.g. Snort, Bro
- Auditing
- Forensic break-in analysis

Deception
- *Honeypots / honeynets*
- Forensic follow-up

Prevention
- Restrictive policies
  - e.g. least privilege principle
- Vulnerability scanning
  - e.g. OpenVAS, metasploit
- Vulnerability patching
  - e.g. regular updates

Recovery
- Backups
- Redundant systems
- Forensic recovery

Security readiness (1/3)

Discouragement, Deception and Detection measures mainly tackle 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 specific knowledge

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, and chain multiple attacks
  - 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/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

A single "day zero" may exist for months/years

- Known to attackers, unknown to others
- Frequently part of attack arsenal

Case Study: ShadowBrokers

Background: State actors have exploits to publicly unknown vulnerabilities

- For many years, used for state level warfare, and never revealed

August 2016: Shadowbrokers publish large stash of tools from state actors

- Use standard public channels: Twitter, Github, PasteBin, Medium
- Then several other stashes, make an auction, black friday sales, etc...
- Objective: sell tools to highest bidder

March 2017: Microsoft releases patch to most Windows systems

- but not to W7, W8, WXP and Server 2003
- Possibly tipped by state actor

Case Study: ShadowBrokers

April 2017: ETERNALBLUE leaked by ShadowBrokers to the public

- Exploit to MS Windows SMB v1, allowing Remote Code Execution

May 2017: Wannacry Ransonware

- Uses 2 exploits from ShadowBrokers leak (ETERNALBLUE as entry point)
- Asks for $300-600 ransom to obtain the key
- Impact: Files are encrypted in >300.000 devices

May 2017: EternalRocks Ransonware

- Uses 7 exploits from ShadowBrokers leak (ETERNALBLUE as entry point)
- Impact: Panic only. Author disables worm

June 2017: NotPetya Ransonware

- Uses ETERNALBLUE and infects the Master Book Record
- Asks for $300 ransom (that doesn't work!)
- Targets Ukraine companies and utilities
- Impact: Files are lost. >$10B of damage

Vulnerability detection

Specific tools can detect vulnerabilities

- Exploiting known vulnerabilities
- Testing known vulnerability patterns
  - e.g. buffer overflow, SQL injection, XSS, etc.

Specific tools can replicate known attacks

- Use known exploits for known vulnerabilities
  - e.g.: MS Samba v1 exploit used by Wannacry

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

Can be applied with care as a form of vulnerability assessment

- To production systems or replicas

Survivability

How can we survive a zero-day attack?

How can we react to a massive zero-day attack?

Diversity is one answer (as a policy) …

- 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 macOS not so much?
- Are you using an Android cell phone?
  - What are the odds of being in the battlefront? (you are)

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.

Details about a vulnerability can be kept private

- Part of responsible disclosure: Until owner provides a fix

CVE Vulnerability

A mistake in software

- that can be directly used by an attacker 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

- allowing access to information or capabilities used 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

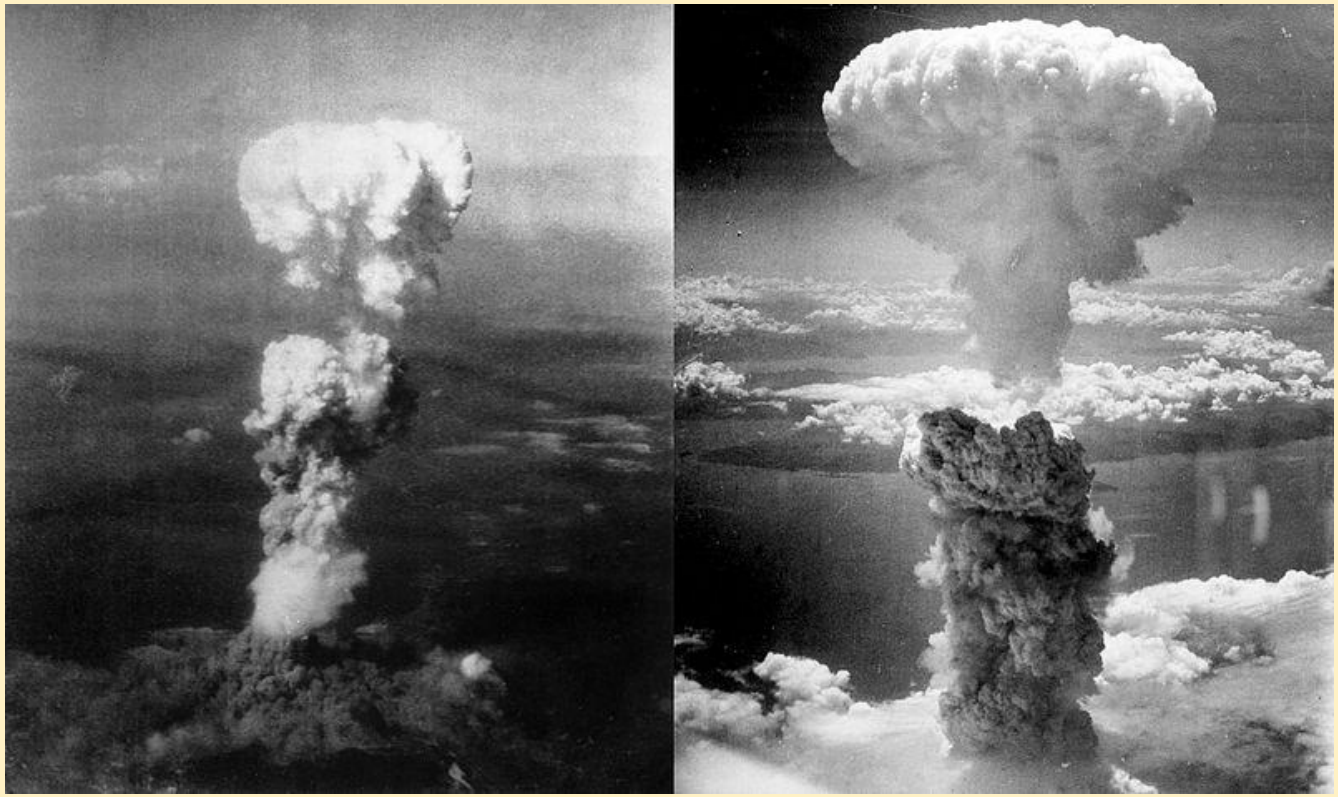
- More comprehensive, better comparisons, interoperable
- Indications and warning systems

Will spark further innovations

- Focal point for discussing critical database content issues

CVE limitations

Worthless Against 0-day attacks



CVE identifiers

Aka CVE names, CVE numbers, CVE-IDs, 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

CVE and Attacks

Attacks can be made possible through multiple vulnerabilities

- One CVE for each vulnerability

Exemple: Stagefright (Android, video in MMS messages)

- CVE-2015-1538, P0006, Google Stagefright ‘stsc’ MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1538, P0004, Google Stagefright ‘ctts’ MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1538, P0004, Google Stagefright ‘stts’ MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1538, P0004, Google Stagefright ‘stss’ MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-1539, P0007, Google Stagefright ‘esds’ MP4 Atom Integer Underflow Remote Code Execution
- CVE-2015-3827, P0008, Google Stagefright ‘covr’ MP4 Atom Integer Underflow Remote Code Execution
- CVE-2015-3826, P0009, Google Stagefright 3GPP Metadata Buffer Overread
- CVE-2015-3828, P0010, Google Stagefright 3GPP Integer Underflow Remote Code Execution
- CVE-2015-3824, P0011, Google Stagefright ‘tx3g’ MP4 Atom Integer Overflow Remote Code Execution
- CVE-2015-3829, P0012, Google Stagefright ‘covr’ MP4 Atom Integer Overflow Remote Code Execution

CVE-ID	
CVE-2015-1538	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Date Entry Created	
20150206	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20150206)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE list, which standardizes names for security problems.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

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

1. **Input validation and representation**
2. **API abuse**
3. **Security features**
4. **Time and state**
5. **Errors**
6. **Code quality**
7. **Encapsulation**

(*) Environment

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

Vulnerability databases

NIST NVD (National Vulnerability Database)

CERT Vulnerability Card Catalog

US-CERT Vulnerability Notes Database

Other

- https://en.0day.today
- https://www.exploit-db.com/
- https://vuldb.com/

CERT
Computer Emergency Readiness Team

Organization 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 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: https://www.facebook.com/CentroNacionalCibersegurancaPT
- 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 …