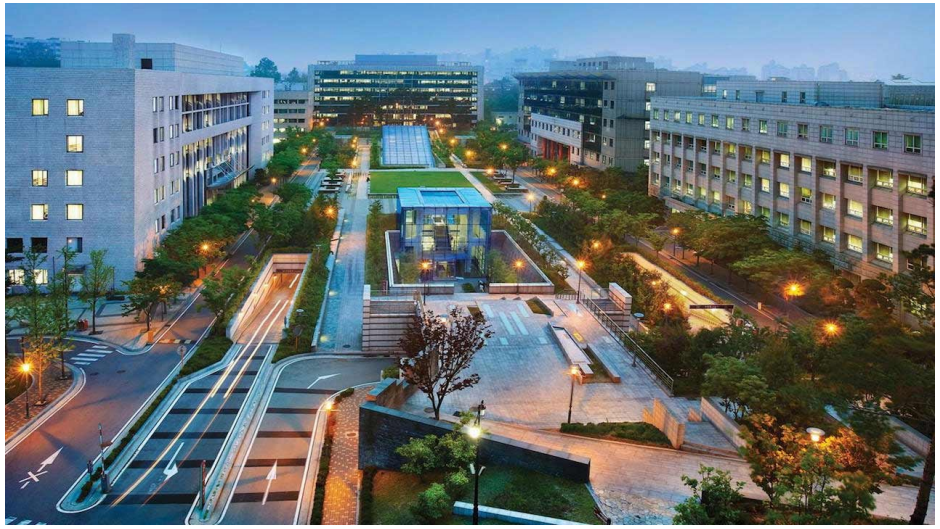
COSC 362

- Sungdeok (Steve) Cha
  - **Erskine Visiting Fellow, 2018**
  - Professor, Korea University, Seoul, Korea, 2008~
  - Professor, KAIST (Korea Advanced Institute of Science and Technology), Daejeon, Korea, 1994~2008
  - MTS, The Aerospace Corporation, El Segundo, CA, 1991~1994
  - Ph.D., Information and Computer Science, Univ of California, Irvine, 1991
  - Research area: Software engineering, Software safety, Security, …

Korea University



KAIST (1971~)

KAIST

QS World University Rankings(2013~)

Ranking Division	2013	2014	2015	2016	2017
World Ranking (Overall)	60	51	43	46	41
Engineering and Technology	24	36	17	13	14
Natural Sciences	48	47	54	28	32
Top 50 Under 50 Ranking	4	3	3	3	3

KOREA UNIVERSITY 1905

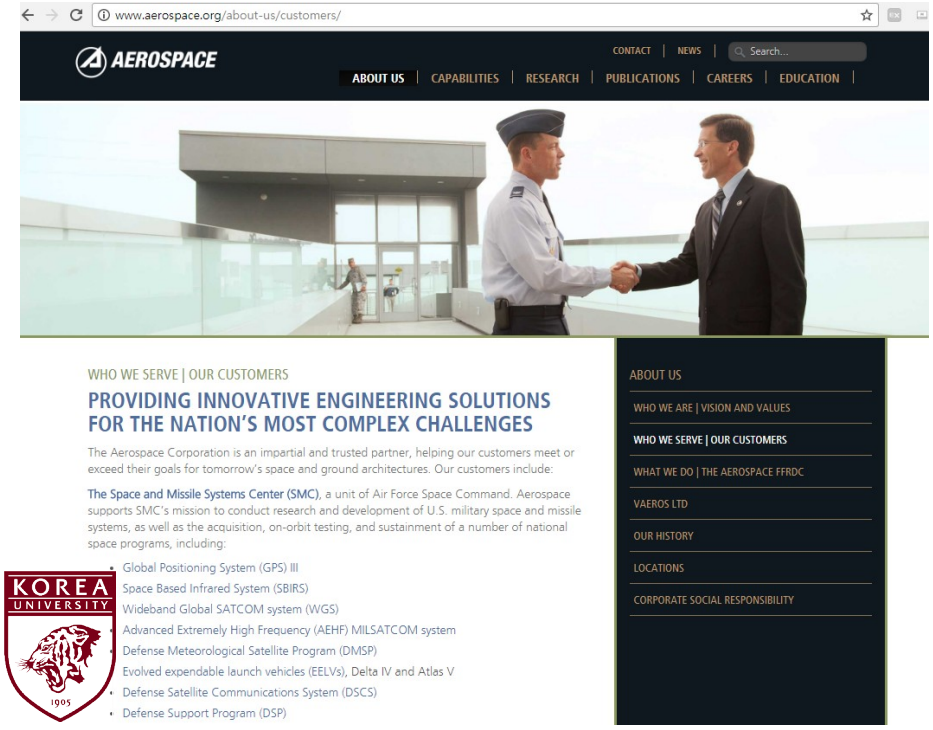
UC Irvine and Anteaters

- Donald Bren School of Information and Computer Science

Security Experience (Industry)

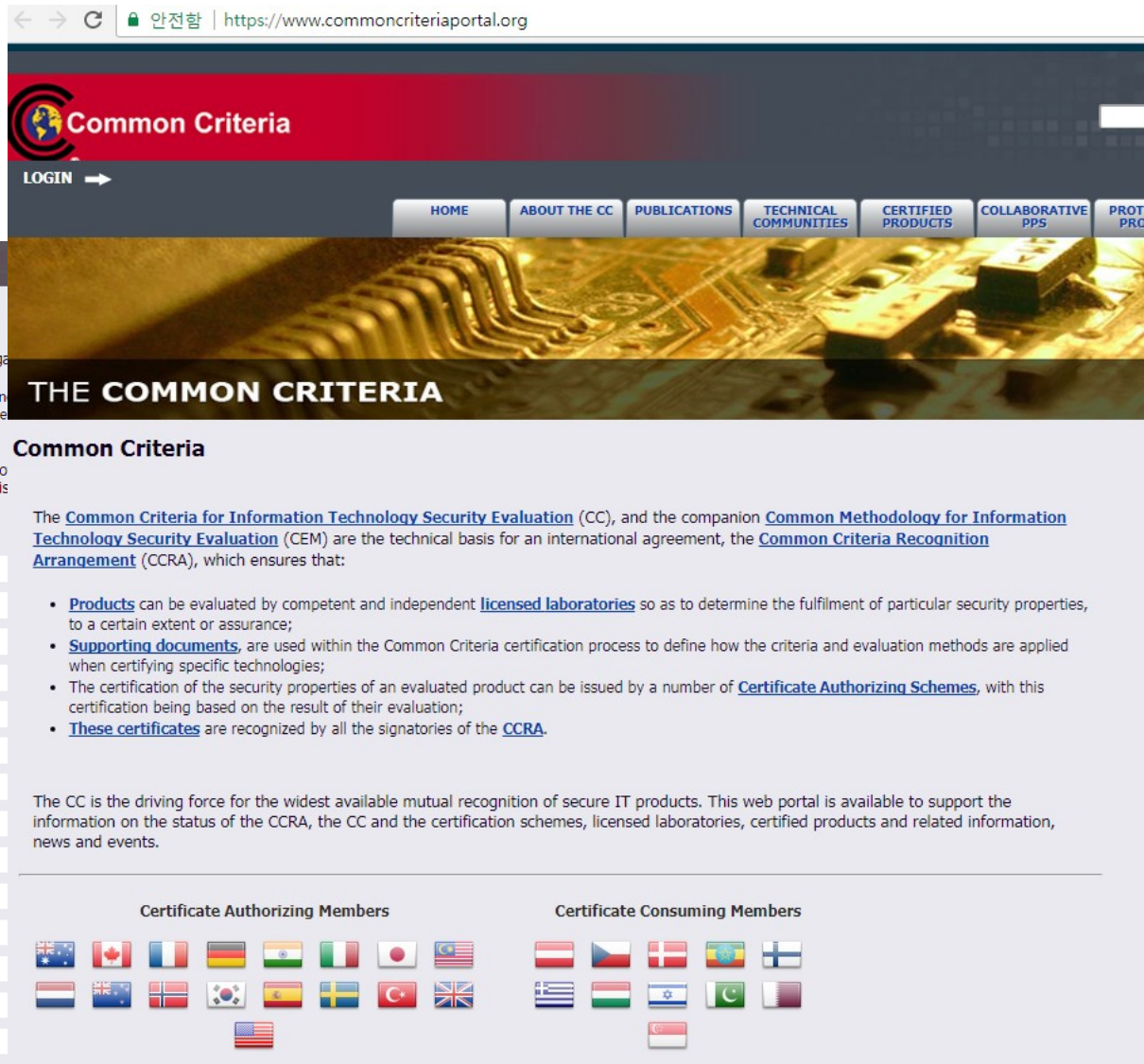
- Trusted Product Evaluation Program, Aerospace Corp / NSA, 1991~1994

Hewlett Packard Corporation	HP-UX BLS release 8.04	B1	09/21/93	TCSEC
Hewlett Packard Corporation	HP-UX BLS release 9.0.9+	B1	12/01/94	TCSEC
Tandem Computers Inc.	Guardian-90 w/Safeguard S00.01	C2	06/14/93	TCSEC



TCSEC and Common Criteria

- More later



Academic Research

- Supervised several Ph.D. students on security research (4 at KAIST, 1 at KU)
- Published some papers in peer-reviewed journals
  - Shinil Kwon and Sungdeok Cha*, “Paradigm Shift on CAPTCHA Race: Adding Uncertainty into the Rules”, IEEE Software, Vol. 33, Issue 6, pp.80-85, Dec. 2016
  - Jeongseok Seo, Sungdeok Cha, Bin Zhu, Doo-Hwan Bae, “PC Worm Detection System Based on the Correlation between User Interactions and Comprehensive Network Behaviors”, IEICE Transactions on Information and Systems, vol. E96-D, no. 8, September. 2013
  - Su Yong Kim, Sungdeok Cha, Doo-Hwan Bae, “Automatic and lightweight grammar generation for fuzz testing”, Computer and Security (ISSN: 0167-4048, IF(2013): 1.172), vol. 36, July. 2013, pp. 1-1
  - Han-Sung Kim and Sungdeok Cha, “Empirical evaluation of SVM-based masquerade detection using UNIX commands”, Computers & Security, vol. 24, no. 2, 2005, pp.160-168
  - Sanghyun Cho, Sungdeok Cha, “SAD: Web Session Anomaly detection based on parameter estimation”, Computer & Security, vol. 23, no. 4,

WANT TO BE PAID FOR YOUR NOTES?

The Disability Resource Service (DRS) is looking to buy high quality lecture notes from students enrolled at UC.

These notes will be used by students who experience difficulties taking notes for themselves for disability-related reasons, and DRS will pay $8 per lecture for them.

For most arts courses the notes need to be taken in MS Word. However, notes in science subjects where many formulas and mathematical symbols are used can be handwritten and scanned.

OF COURSE YOU DO!

STEP ONE:

Email drsnotes@canterbury.ac.nz as soon as possible with two samples of lecture notes you've taken.

STEP TWO:

Complete the application form we'll email back to you.

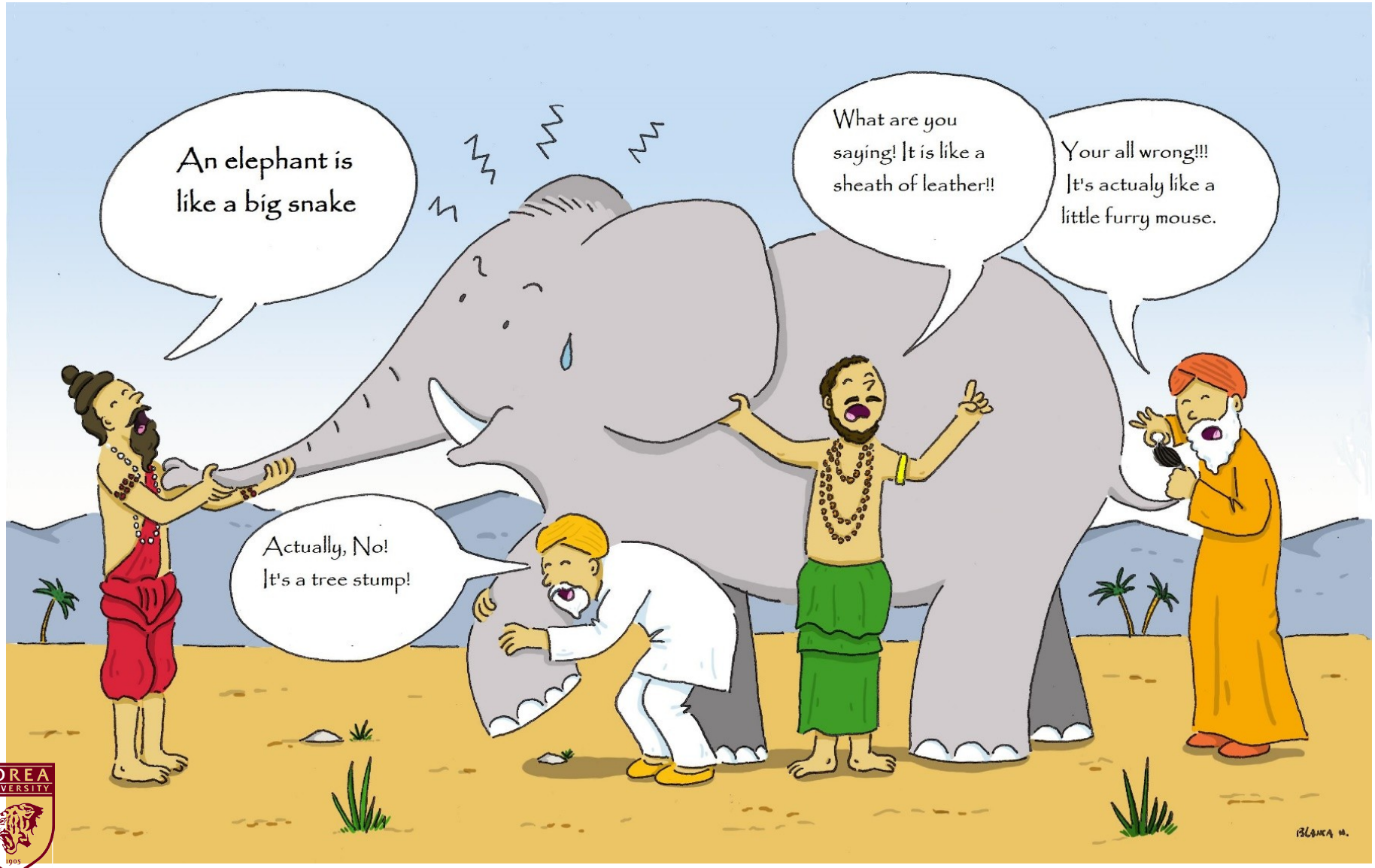
STEP THREE:

Keep an eye on your UC email. If we like what we see and you're selected, we'll be in touch!

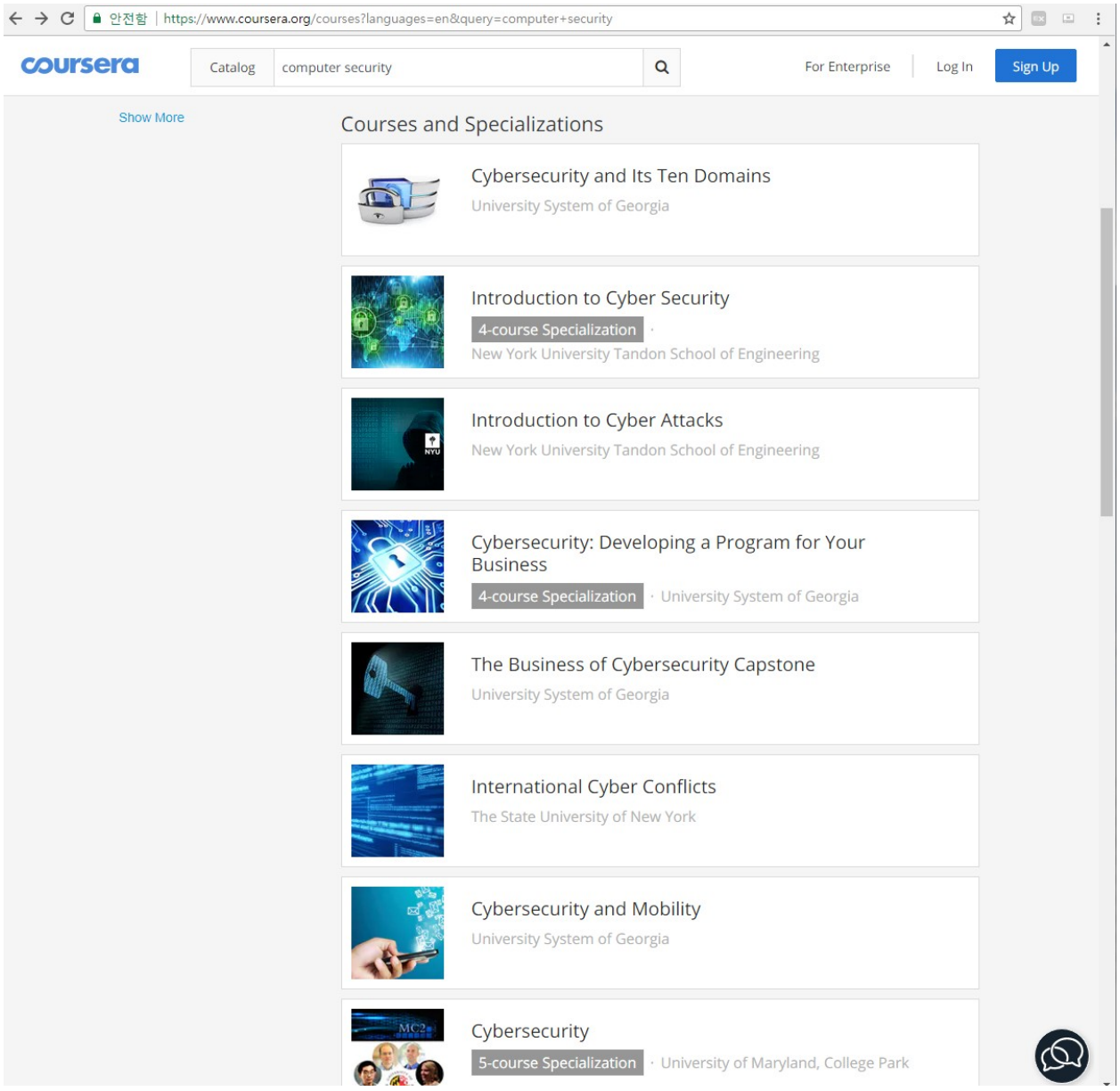
Lecture Slides and Sources

- Either
  - My own ;)
  - Or, “borrowed with permission” from Prof. Dan Dong-Seong Kim
  - Or, from security lecture slides available in Internet
  - Or, Wikipedia or Web page captures
- References are clearly marked

Before we begin...



Lots of resources



Learning objectives

- At the end of this lecture, you will be able to Understand/explain
  - Computer Security Concepts
  - Threats, Attacks, and Assets
  - why cyber security is so important (and challenging)
  - Computer Security Strategy
  - Security Functional Requirements
  - Fundamental Security Design Principles
  - Attack Surfaces and Attack Trees

Recommended Approach to Security Study

- Learn more than “abstract” security concepts or horror stories
  - Study concrete examples whenever practical
- Students are strongly encouraged to study online material (e.g., reports, wiki, blog, …)
- Read on demand.

Brefore we begin…

- Computer security is truly interdisciplinary in nature and requires in-depth and detailed knowledge on several domains
  - Mastery of programming skills including C and assembly
  - Operating systems (e.g., UNIX, Linux, …)
  - Computer networks and protocols (e.g., TCP/IP, …)
  - Databases (e.g., SQL, …)
  - “Computational thinking”, creativity, …
- Security will become more important in the future (e.g., autonomous cars, IoT, Cyber Physical Systems, …)

Subtle but Significant Difference

```
#include <stdio.h>

void func(int i, int *b) {
  int a = i + b[++i];
  printf("%d, %d", a, i);
}
```

vs

```
#include <stdio.h>

void func(int i, int *b) {
  int a;
  ++i;
  a = i + b[i];
  printf("%d, %d", a, i);
}
```

Subtle but Significant Difference

4 Expressions (EXP)

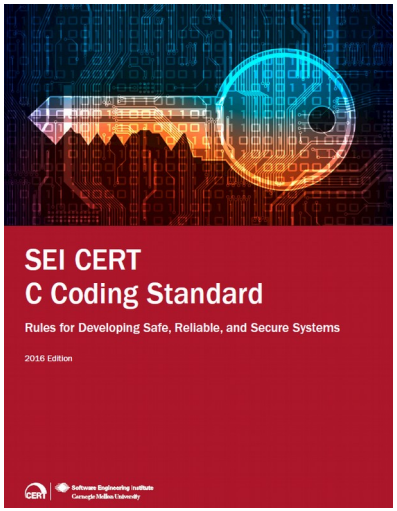
4.1 EXP30-C. Do not depend on the order of evaluation for side effects

Evaluation of an expression may produce side effects. At specific points during execution, known as sequence points, all side effects of previous evaluations are complete, and no side effects of subsequent evaluations have yet taken place. Do not depend on the order of evaluation for side effects unless there is an intervening sequence point.

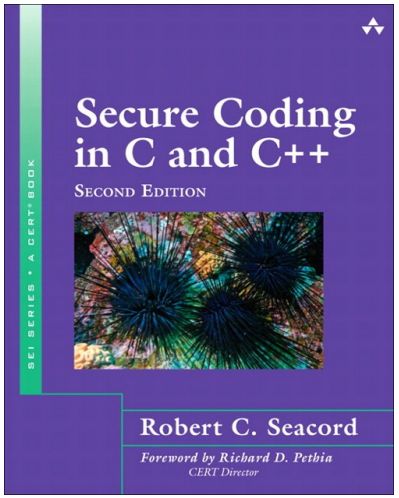
The C Standard, 6.5, paragraph 2 [ISO/IEC 9899:2011], states

> If a side effect on a scalar object is unsequenced relative to either a different side effect on the same scalar object or a value computation using the value of the same scalar object, the behavior is undefined. If there are multiple allowable orderings of the subexpressions of an expression, the behavior is undefined if such an unsequenced side effect occurs in any of the orderings.

This requirement must be met for each allowable ordering of the subexpressions of a full expression; otherwise, the behavior is undefined. (See undefined behavior 35.)

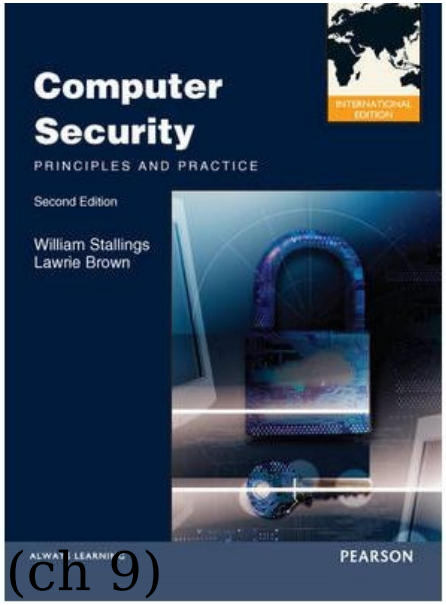


pdf (534 pages)



book

Primary Textbook & Subjects to Cover



- Introduction (ch 1)
- Overview on cryptography (ch 2)
- User Authentication (ch 3)
- Access control (ch 4)
- Malicious software (ch 6)
- Denial-of-service attacks (ch 7)
- Intrusion Detection (ch 8)
- Firewall and Intrusion Prevention Systems (ch 9)
- Buffer Overflow (ch 10)
- Software Security (ch 11)
- Operating system security (ch 12)
- Trusted computing and multilevel security (ch 13)

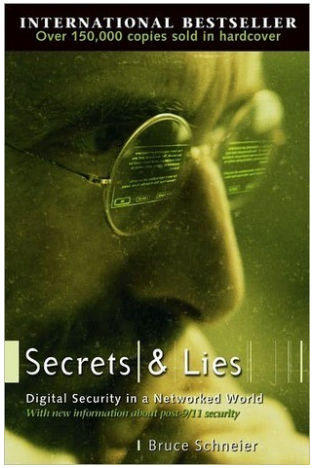
- sometimes in different order (e.g., ch 6, 10, 11 as a group)
- various depth in coverage

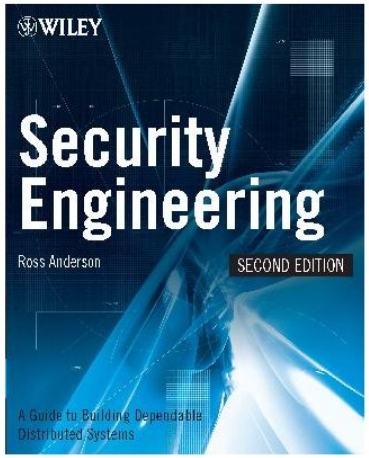
Topics to skip (or cover briefly)

- Database security (ch 5)
- Management issues
  - IT Security management and Risk Assessment (ch 14)
  - IT Security control, plans, and procedures (ch 15)
  - Physical security and Infrastructure security (ch 16)
  - Human resources security (ch 17)
  - Legal and ethical issues (ch 19)
- “Heavy-duty” Cryptographic algorithms
  - Symmetric encryption and message confidentiality (ch 20)
  - Public-key cryptography and message authentication (ch 21)
- Network Security
  - Internet security protocols and standards (ch 22)
  - Internet authentication applications (ch 23)
  - Wireless network security (ch 24)

Likely Useful Reference

- Not required textbooks



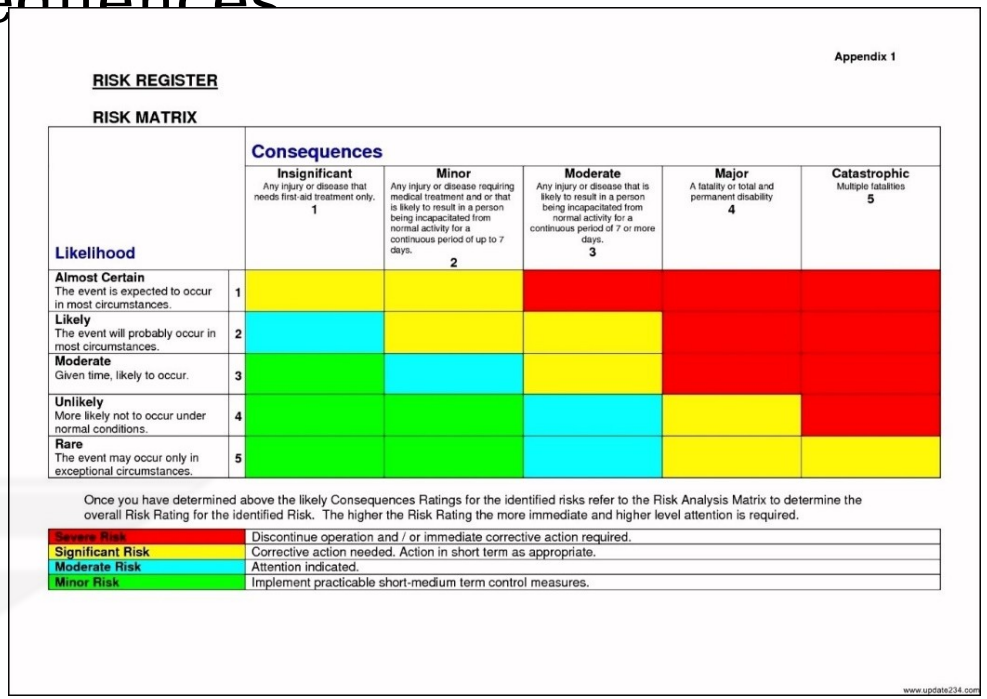


- Students are strongly advised to read recommended online security publications

Perfect Security Possible or Necessary?

- It takes just one “security incident” to be blamed
- Risk management is essential
  - Quantification and prioritization based on likelihood and consequences

		Likelihood		
		High	Medium	Low
Impact	High	Unencrypted laptop ePHI	Lack of auditing on EHR systems	Missing security patches on web server hosting patient information
	Medium	Unsecured wireless network in doctor’s office	Outdated anti-virus software	External hard drives not being backed up
	Low	Sales presentation on USB thumb drive	Web server backup tape not stored in a secured location	Weak password on internal document server



Appendix 1

RISK REGISTER

RISK MATRIX

Likelihood		Consequences: Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain The event is expected to occur in most circumstances.	1					
Likely The event will probably occur in most circumstances.	2					
Moderate Given time, likely to occur.	3					
Unlikely More likely not to occur under normal conditions.	4					
Rare The event may occur only in exceptional circumstances.	5					

Once you have determined above the likely Consequences Ratings for the identified risks refer to the Risk Analysis Matrix to determine the overall Risk Rating for the identified Risk. The higher the Risk Rating the more immediate and higher level attention is required.

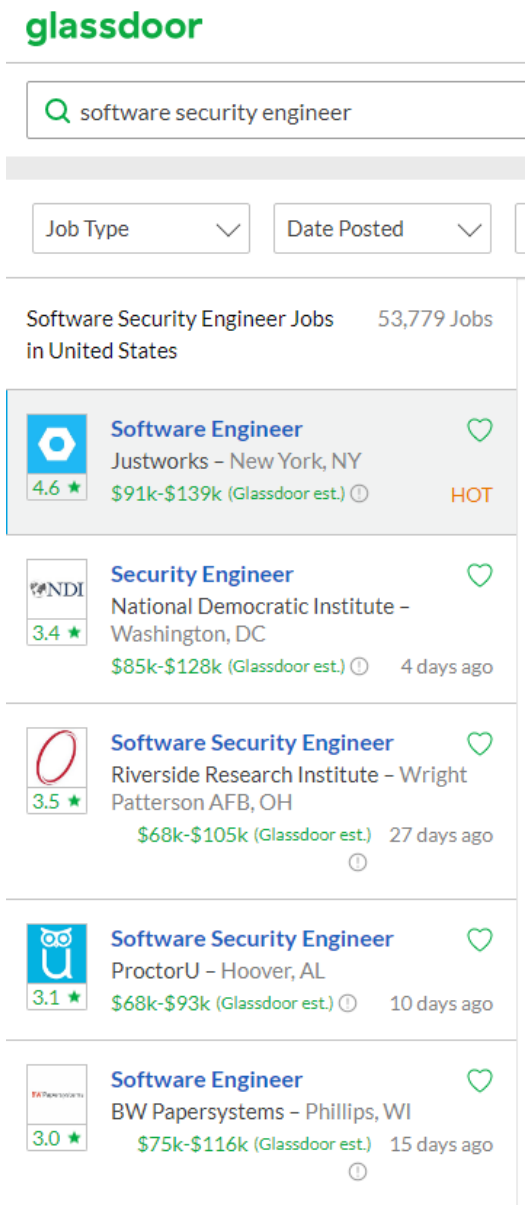
Severe Risk	Discontinue operation and / or immediate corrective action required.
Significant Risk	Corrective action needed. Action in short term as appropriate.
Moderate Risk	Attention indicated.
Minor Risk	Implement practicable short-medium term control measures.

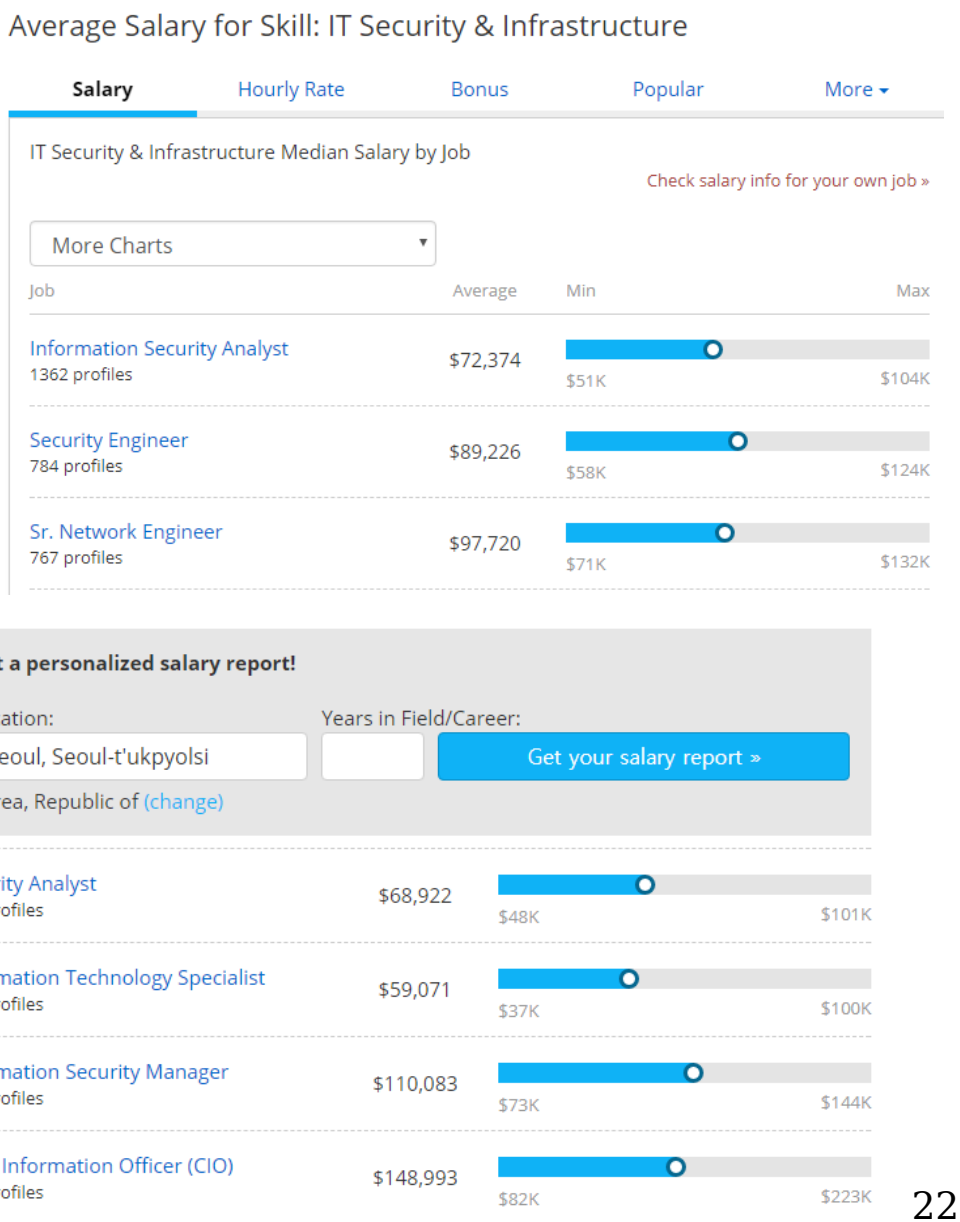
Top IT Security Salaries (in USD)

- Chief information security officer $192,500
- Chief security officer $225,000
- Director of security $178,333
- Lead software security engineer $233,333
- Global information security director $200,000

Source: Paul Curran, Cyber Security Today: Career Paths, Salaries and In-Demand Job Titles, available at: https://www.checkmarx.com/2016/08/30/cyber-security-career-paths-salaries-and-the-most-in-demand-job-titles/

Lots of Opportunities





Computer Security definition?

- The NIST* Computer Security Handbook defines the term Computer Security as:
  - "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources" (includes hardware, software, firmware, information/data, and telecommunications).

*National Institute of Standards and Technology

Three key objectives (the CIA triad)

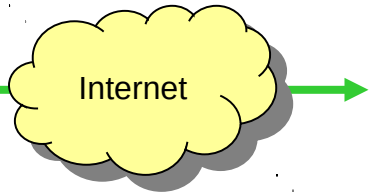
- **Confidentiality**
  - **Data confidentiality**: Assures that confidential information is not disclosed to unauthorized individuals
  - **Privacy**: Assures that individual control or influence what information may be collected and stored
- **Integrity**
  - **Data integrity**: assures that information and programs are changed only in a specified and authorized manner
  - **System integrity**: Assures that a system performs its operations in unimpaired manner
- **Availability**:
  - assure that systems works promptly and service is not denied to authorized users

University example? UCANask

- Confidentiality
  - Student login password should not be improperly disclosed by others
  - e.g., ID: abc123 password: p@ssw0rd!
- Integrity
  - Student name should not be modified improperly
  - e.g., John -> Jonathan
- Availability
  - **Learn** system should be available when a student wants to download lecture slides.

Security objectives : summary

Alice in South Island



Bob in North island

The data has not been viewed by a 3rd party → ***C**onfidentiality* ← Encryption

The data has not been modified in transit → ***I**ntegrity* ← Hash func.

The data must be **available** when it is needed → **A**vailability

Cryptography

Security objectives (cont.)

An example

Internet

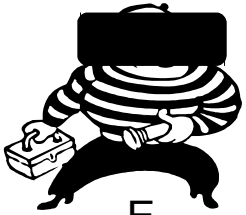
Alice in South Island

UGETG V

Bob in North island

by DES, 3DES, AES, *etc*

by Caesar with *k=2*



E

The data has not been viewed by a 3rd party

***C**onfidentiali ty*

Encryptio n

***C**onfidentiality: the protection of transmitted data from passive attacks (release of message contents and traffic analysis)*

biggest data breaches of all time

All Images News Videos Maps More Settings Tools

About 1,540,000 results (0.75 seconds)

The 17 biggest data breaches of the 21st century | CSO Online

https://www.csoonline.com/.../data-breach/the-biggest-data-breaches-of-the-21st-centu...

Jan 26, 2018 - Details: This is viewed as the worst gaming community **data breach of all-time**. Of more than 77 million accounts affected, 12 million had unencrypted credit card numbers. Hackers gained access to full names, passwords, e-mails, home addresses, purchase history, credit card numbers and PSN/Qriocity ...

5 Biggest Data Breaches of All Time | Fortune

fortune.com › Tech › data breach

Apr 3, 2018

Companies are having a hard time keeping their customers' private information safe. Here are the five worst ...

World's Biggest Data Breaches & Hacks — Information is Beautiful

www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Let us know if we missed **any** big **data breaches**. » Safely check if your details have been compromised in **any** recent **data breaches**: https://haveibeenpwned.com/. » See the **data**: bit.ly/**bigdatabreaches**. This interactive 'Balloon Race' code is powered by **our** forthcoming VizSweet software – a set of high-end dataviz tools ...

The Worst Data Breaches of All Time - Tom's Guide

https://www.tomsguide.com/us/pictures-story/872-worst-data-breaches.html

Oct 3, 2017 - The Yahoo **data breach** may be the **biggest**, but you've probably never heard of other **data breaches** that were smaller, but worse.

11 of the Largest Data Breaches of All Time (Updated) | OPSWAT Blog

https://www.opswat.com/blog/11-largest-data-breaches-all-time-updated

Nov 22, 2017 - The 3 billion Yahoo accounts compromised by a 2013 hack make this easily the **biggest data breach** in the internet era. **All** Yahoo users were affected by the breach – although Yahoo did not determine that this was the case until 2017. Though the U.S. government indicted Russian hackers for a later ...

40 Biggest Data Breaches of All Time | Acuantcorp

https://www.acuantcorp.com/40-biggest-data-breaches-time/

The internet has become a pervasive entity in the lives of businesses everywhere, making communication, marketing, and doing business easier than **ever**. However, the rising number of **data breaches** has begun to paint a darker picture of the internet and what it has in store for companies in the coming years.

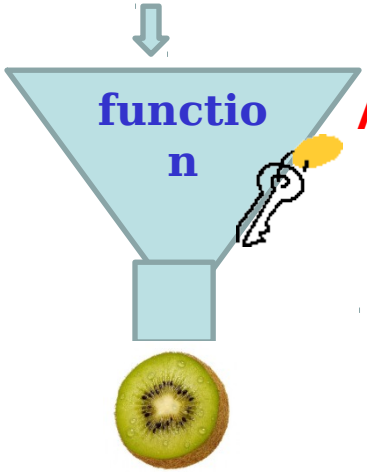
KOREA UNIVERSITY 1905

Security objectives (cont.)

Use HMAC(Hashed message authentication code), such as HMAC-MD5, HMAC-SHA1

Internet

New Zealand fruit?



Kiwi

Alice in South Islaı

Bob in North island

Class 362
- I hate you!

E

New Zealand sport?

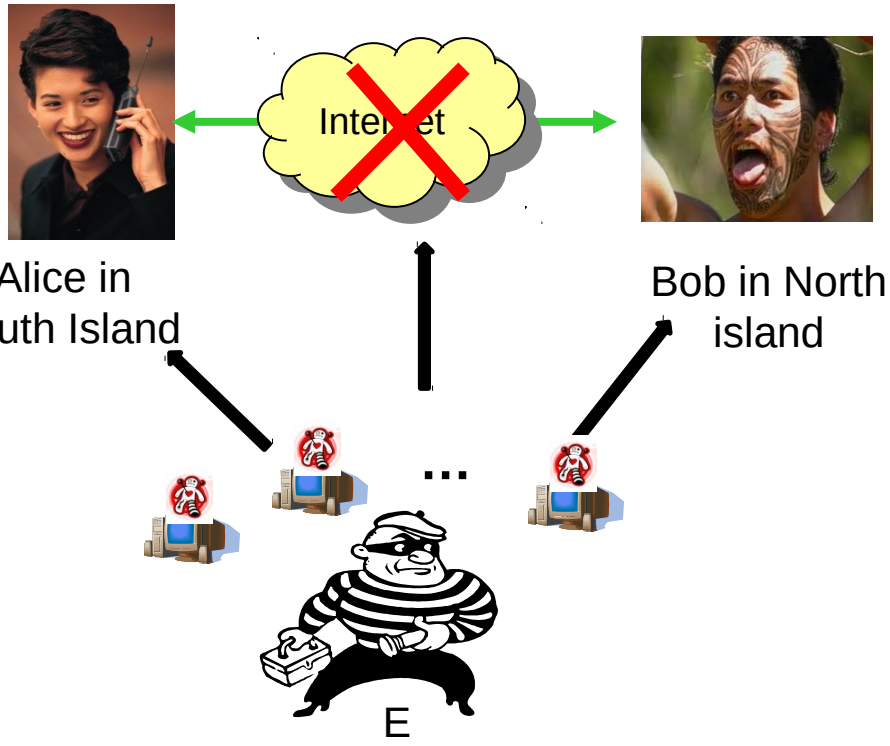
All blacks

The data has not been modified in transit

→ *Integrity* ← Crytographic Hash func.

***Integrity**: the assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay)*

Security objectives (cont.)



Distributed Denial of Service (DDoS) attacks

For any information system to serve its purpose, the information must be **available** when it is needed

→ **A**vailability

Source: http://memeburn.com

Military Example

- Confidentiality
  - The target coordinates of a missile should not be improperly disclosed
- Integrity
  - The target coordinates of a missile should not be improperly modified
- Availability
  - When the proper command is issued the missile should fire

Source: Peng Ning's lecture notes

On military applications…

- Security is a paramount concern, and security requirements are more complex
  - Multi-Level Security (e.g., Bell-LaPadula model)

Not logged in Talk Contributions Create account Log in

WIKIPEDIA
The Free Encyclopedia

Article Talk Read Edit View history Search Wikipedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes

Bell–LaPadula model

From Wikipedia, the free encyclopedia

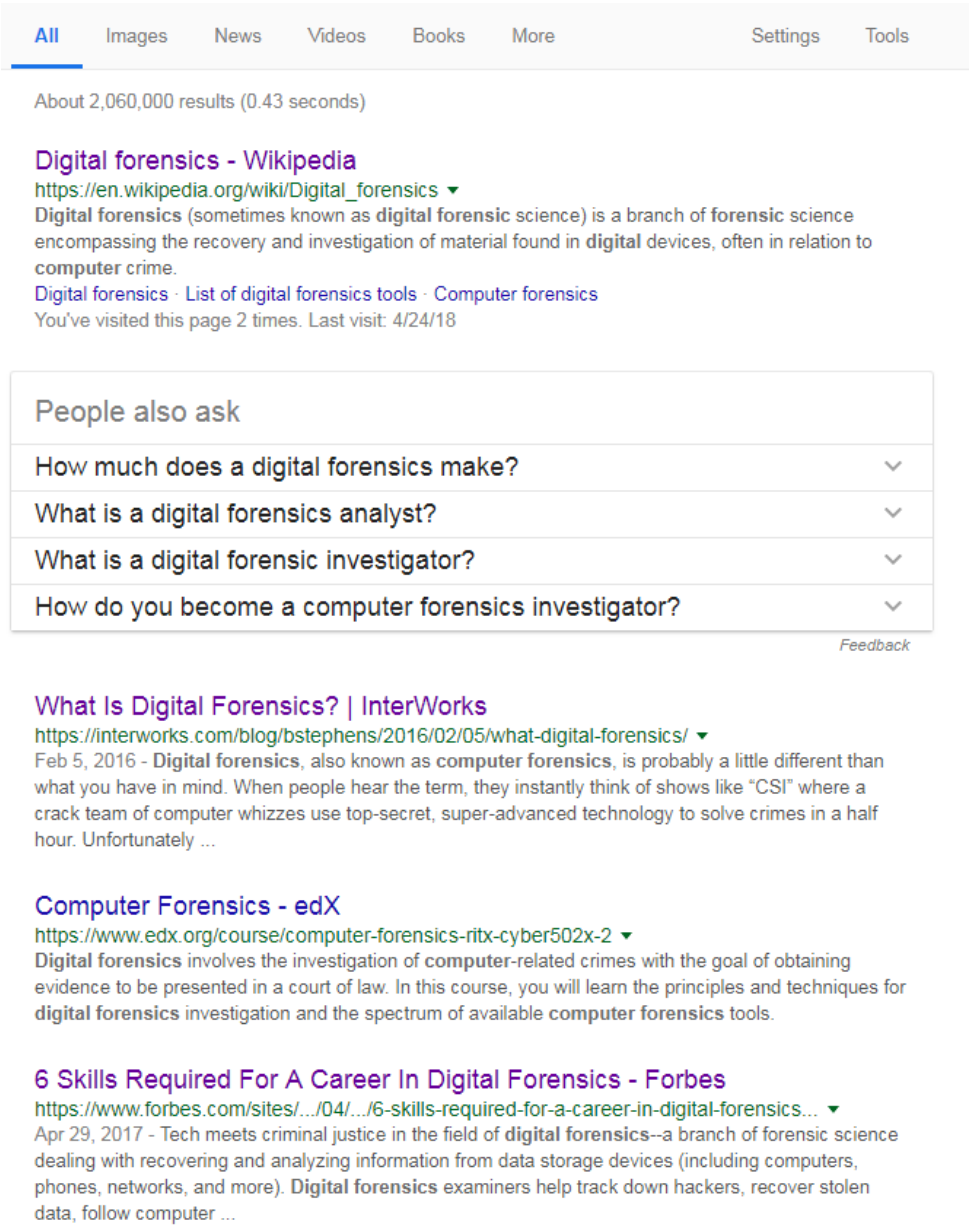
The **Bell–LaPadula Model** (**BLP**) is a state machine model used for enforcing access control in government and military applications.[1] It was developed by David Elliott Bell [2] and Leonard J. LaPadula, subsequent to strong guidance from Roger R. Schell, to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy.[3][4][5] The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").

The Bell–LaPadula model is an example of a model where there is no clear distinction between protection and security.[6]

Additional Security Goals

- Authenticity:
  - The property of being genuine and being able to be verified and trusted
  - This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
  - FIPS PUB 199 includes authenticity under integrity.
- Accountability:
  - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
  - truly secure systems aren't yet an achievable goal, we must be able to trace a security breach to a responsible party.

Digital Forensics



All Images News Videos Books More Settings Tools

About 2,060,000 results (0.43 seconds)

Digital forensics - Wikipedia
https://en.wikipedia.org/wiki/Digital_forensics
Digital forensics (sometimes known as **digital forensic** science) is a branch of **forensic** science encompassing the recovery and investigation of material found in **digital** devices, often in relation to **computer** crime.
Digital forensics · List of digital forensics tools · Computer forensics
You've visited this page 2 times. Last visit: 4/24/18

People also ask
How much does a digital forensics make?
What is a digital forensics analyst?
What is a digital forensic investigator?
How do you become a computer forensics investigator?
Feedback

What Is Digital Forensics? | InterWorks
https://interworks.com/blog/bstephens/2016/02/05/what-digital-forensics/
Feb 5, 2016 - **Digital forensics**, also known as **computer forensics**, is probably a little different than what you have in mind. When people hear the term, they instantly think of shows like "CSI" where a crack team of computer whizzes use top-secret, super-advanced technology to solve crimes in a half hour. Unfortunately ...

Computer Forensics - edX
https://www.edx.org/course/computer-forensics-ritx-cyber502x-2
Digital forensics involves the investigation of **computer**-related crimes with the goal of obtaining evidence to be presented in a court of law. In this course, you will learn the principles and techniques for **digital forensics** investigation and the spectrum of available **computer forensics** tools.

6 Skills Required For A Career In Digital Forensics - Forbes
https://www.forbes.com/sites/.../04/.../6-skills-required-for-a-career-in-digital-forensics...
Apr 29, 2017 - Tech meets criminal justice in the field of **digital forensics**--a branch of forensic science dealing with recovering and analyzing information from data storage devices (including computers, phones, networks, and more). **Digital forensics** examiners help track down hackers, recover stolen data, follow computer ...

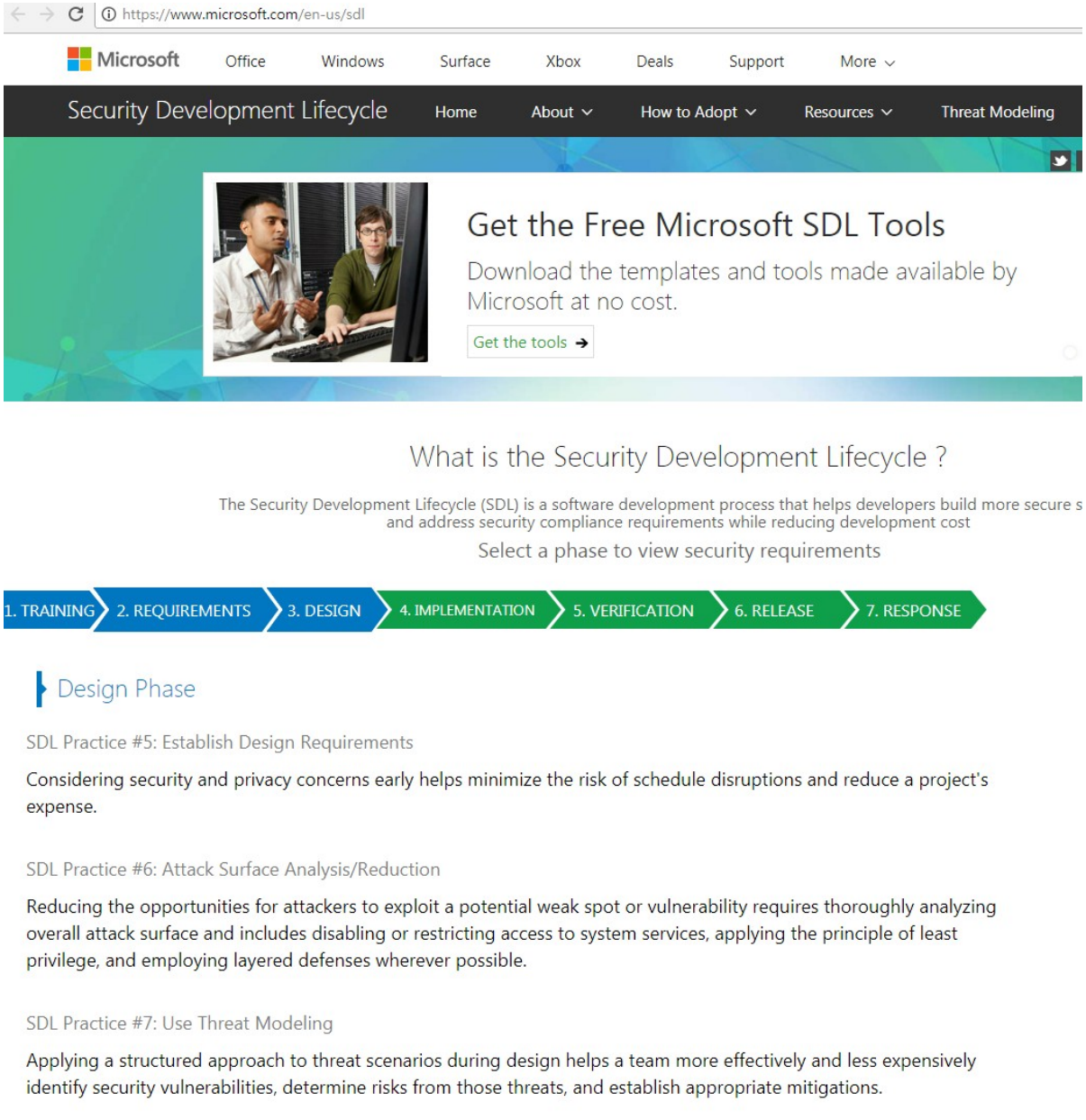
Computer Security Challenges

- Security concepts are simple and straightforward, but mechanisms are NOT
- Developers are often naive about potential vulnerabilities and security threats
  - Security features themselves might contain vulnerabilities
- Real attacks are rarely as simple as they might first appear
  - Attackers are often smarter, more dedicated, better equipped, and highly motivated
    - Sometimes even state-sponsored (e.g., Cyber Command)

Computer Security Challenges

- Easy to defend “known attacks”, but
  - there are always new attack scenarios, powerful attack tools (e.g., script kiddies), new evasion tools (e.g., Tor), unknown vulnerabilities, …
- Security design often involve trade-offs between security assurance and ease of use
- Security is still often an afterthought
  - Must be an integral part of the design process from the beginning

Security Development Lifecycle



Not a Microsoft Informercial

Microsoft Security Development Lifecycle (SDL) Evolution

TwC Next: Marking a Milestone. Continuing Our Commitment.

The Microsoft SDL is the industry-leading software security assurance process. A Microsoft wide initiative and mandatory policy since 2004, the Microsoft Security Development Lifecycle (SDL) has played a critical role in improving the security and privacy of Microsoft software and services with the goal of reducing customer risk. Combining a holistic and practical approach, the Microsoft SDL embeds security and privacy throughout the development process. We believe that by freely sharing the SDL resources, tools, and collaborating with the industry on secure application development, together we can help build safer more trusted computing experiences for everyone.

2000 2001 — The "Perfect Storm"

- Growth of Home PCs
- Rise of Malicious Software
- Increasing Privacy Concerns
- Internet Use Expansion

2002 2003 2004 — SDL Ramp Up

- Bill Gates' TwC Memo
- Microsoft Security Push
- Microsoft SDL Launched
- SDL Becomes Mandatory Policy at Microsoft
- Windows XP SP2 and Windows Server 2003 Launched with Security Emphasis

2005 2006 2007 — Setting a New Bar

- Windows Vista and Office 2007 Fully Integrate the SDL
- SDL Released to Public
- Data Execution Prevention (DEP) & Address Space Layout Randomization (ASLR) Introduced as Features
- Threat Modeling Tool Launches

2008 2009 2010 2011 — Collaboration

- Microsoft joins SAFECode
- Microsoft Establishes SDL Pro Network
- Defense Information Systems Agency (DISA) & National Institution Standards and Technology (NIST) Specify Practices Featured in the SDL
- Microsoft Collaborates with Adobe and Cisco on SDL Practices
- MidAmerican Energy Adopts SDL Practices
- SDL Released Under the Creative Commons License

2012~ — TwC Next

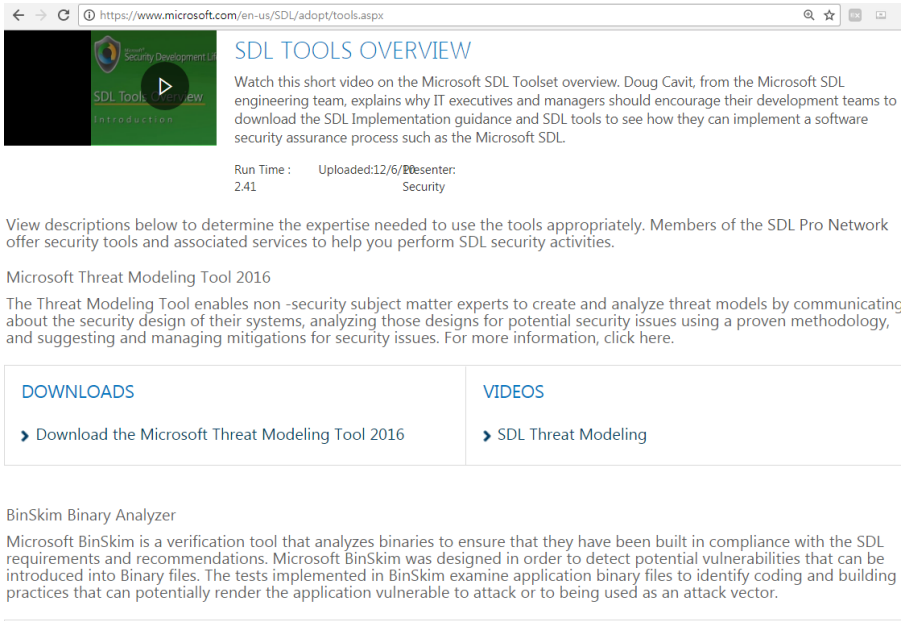
- Additional resources dedicated to address projected growth in Mobile app downloads*
- Industrywide Acceptance of Practices Aligned with SDL
- Adaptation of SDL to New Technologies and Changes in the Threat Landscape
- Increased Industry Resources to Enable Global Secure Development Adoption

Microsoft | Trustworthy Computing www.microsoft.com/sdl

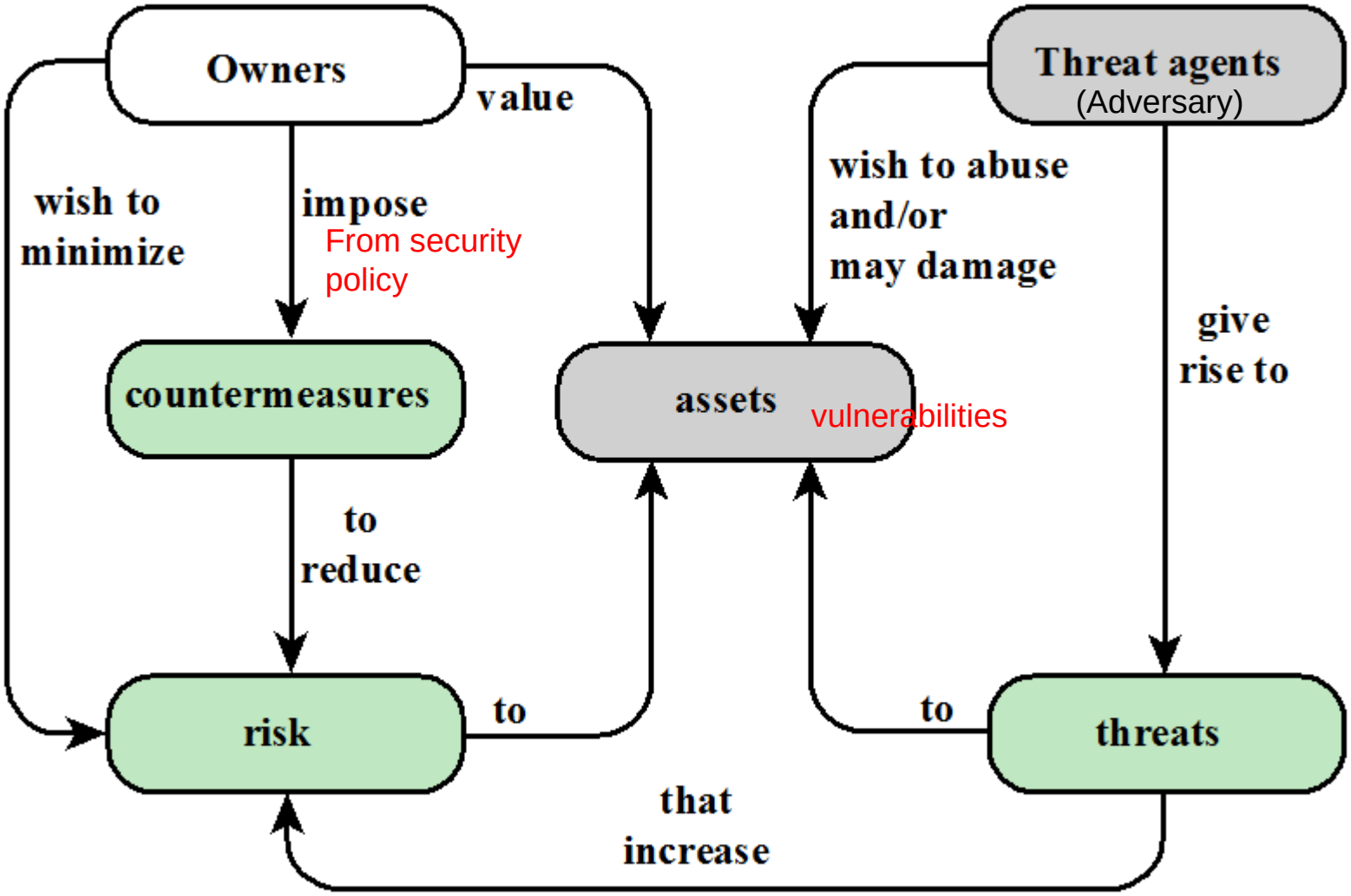
Source: *Gartner Research Press Release, January 26, 2011, Gartner Says Worldwide Mobile Application Store Revenue Forecast to Surpass $15 Billion in 2011 http://www.gartner.com/it/page.jsp?id=1529214

Lots of SDL Tools… Free and Useful

- Threat Modeling Tool 2016
- BinSkim Binary Analyzer
- FxCop
- Attack Surface Analyzer
- Code Analysis for C/C++
- Application Verifier
- …

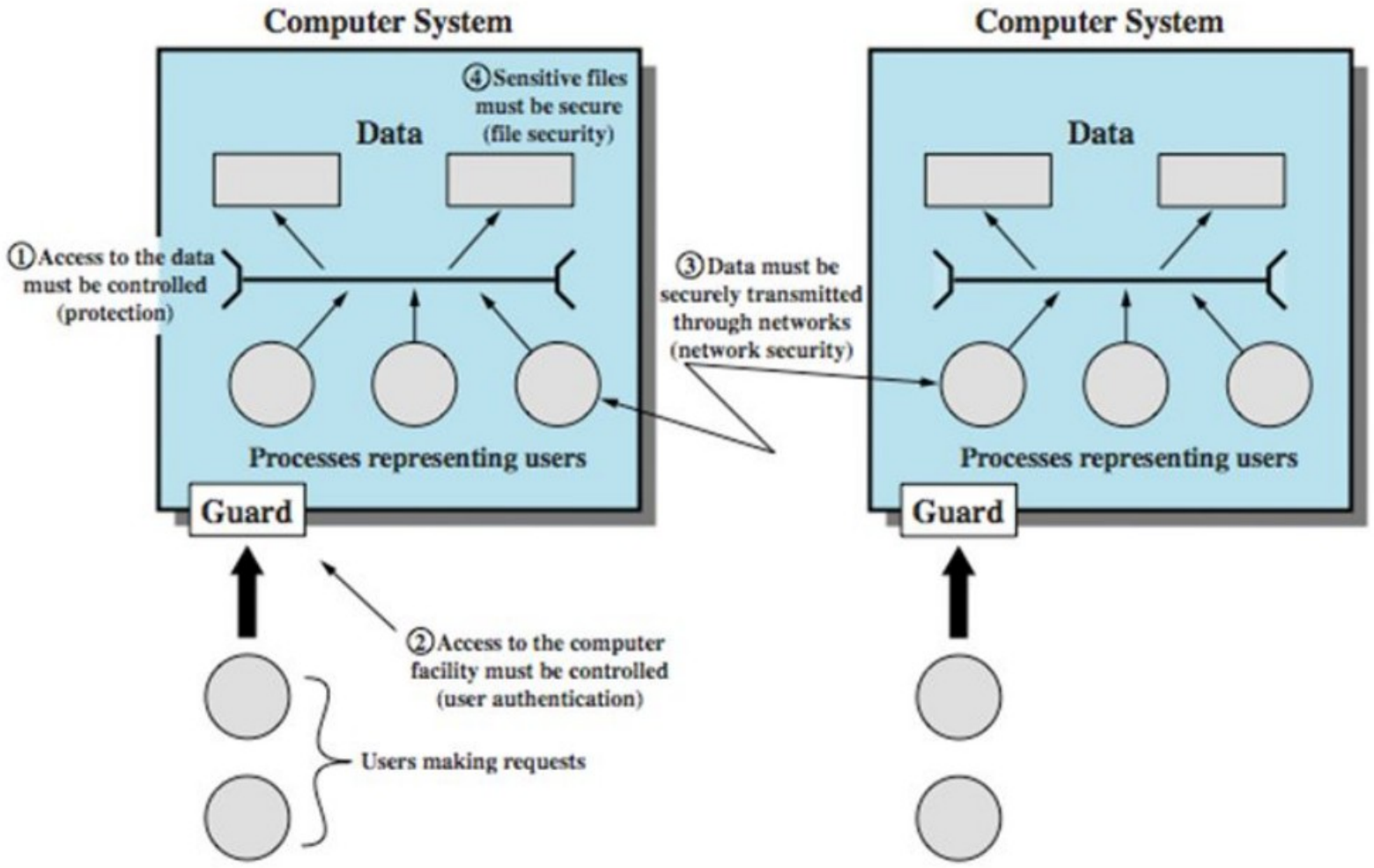


Security concepts and Relationships



Explain this!

Scope of Computer Security



* Stallings and Brown, Ch 1, Figure 1.3

Examples of Threats

	Availability	Confidential-ity	Integrity
Hardware			
Software			
Data			
Communication Lines			

* Computer and Network Assets, Stallings and Brown, Ch 1, Table 1.3

Attacks and their classifications

Alter ?

- Passive:
  - attempt to learn or make use of information from the system that does not affect system resources; eavesdropping on, or monitoring of, transmissions;
  - Two types: release of message contents; traffic analysis
- Active
  - attempt to alter system resources or affect their operation
  - Four categories: Replay, Masquerade, Modification of messages, Denial of service

Origin ?

- Inside
  - initiated by an entity inside the security perimeter
- Outside
  - initiated from outside the perimeter

Security Requirements
(FIPS PUB 200)

- Minimum Security Requirements for Federal Information Processing Standards Publications (17 security-related areas w.r.t. protecting C.I.A.)

- Technical measures
  - Access control; identification & authentication; system & communication protection; system & information integrity
- Management controls and procedures
  - Awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- Overlapping technical and management
  - Configuration management; incident response; media protection (both digital & paper)

Fundamental Security Design Principles

to guide the development of protection mechanisms

Not possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions.

Economy of mechanism	Fail-safe defaults	Complete mediation	Open design
Separation of privilege	Least privilege	Least common mechanism	Psychological acceptability
Isolation	Encapsulation	Modularity	Layering
Least astonishment			

Fundamental Security Design Principles

- Economy of Mechanism
  - Security mechanism should be as simple as possible (KISS?!)
    - A simple design is easier to test and validate. (kids can play with smartphone)
    - Fewer vulnerabilities
- Fail-Safe Defaults
  - Unless a subject is given explicit access to an object, it should be denied access to the object.
    - In computing systems, the save default is generally “no access” so that the system must specifically grant access to resources.
  - Most file access permissions work this way;
    - Windows access control list (ACL), Linux/Unix permissions
    - Firewalls (in the FW figure later)

Fundamental Security Design Principles

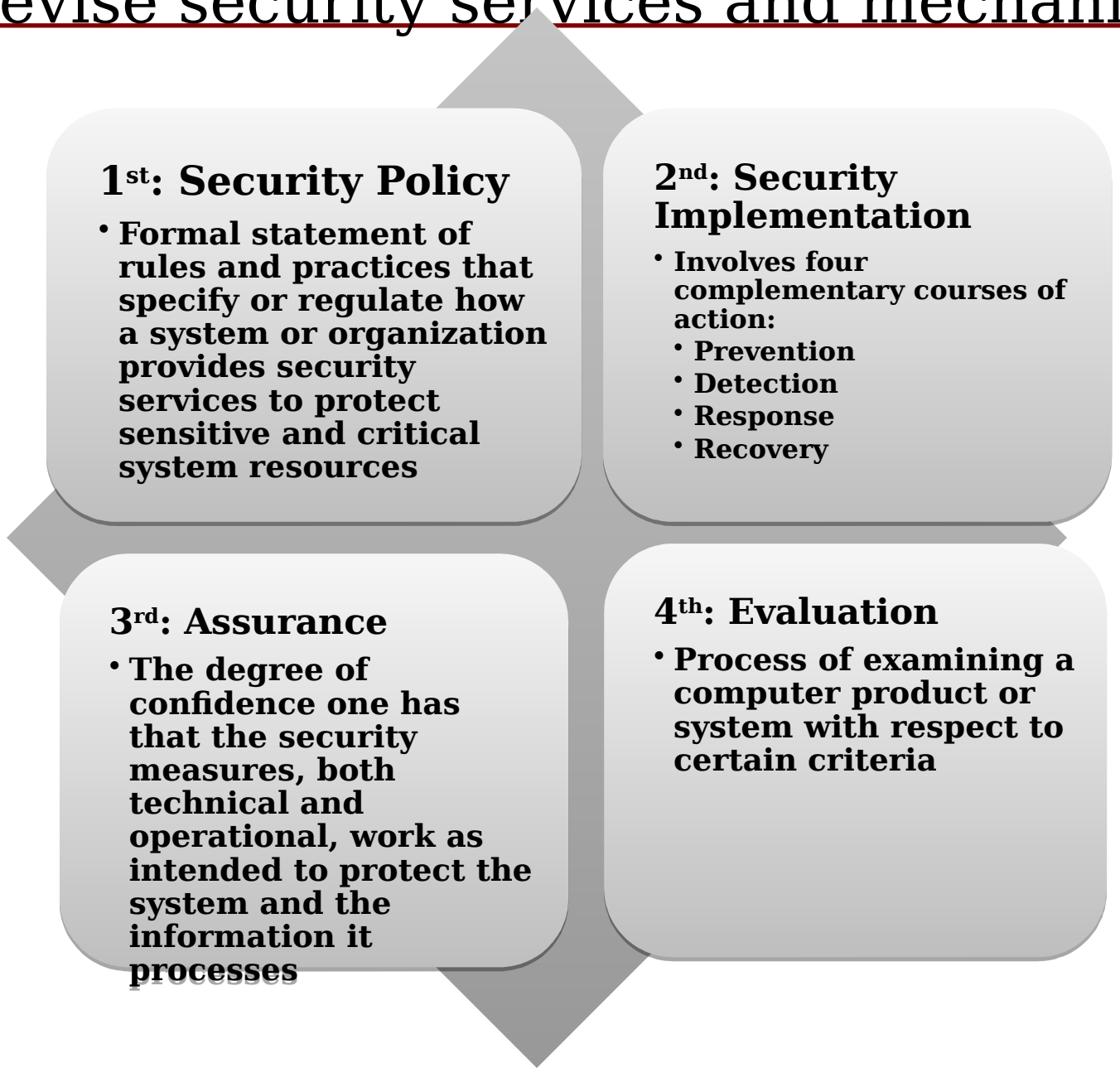
- Complete mediation
  - All accesses to objects should be checked to ensure they are allowed.
    - Access rights are completely validated every time an access occurs
    - the operating system checks the user requesting access against the file's ACL.
- Open design
  - Security of a mechanism should not depend upon secrecy of its design or implementation
  - Should be open for scrutiny (critical observation or examination) by the community
  - e.g., Cryptography and openness
    - secure systems, including cryptographic systems, should have unclassified designs; e.g. AES

- Separation of privilege
  - System should not grant permission based on single condition
    - Access to objects should depend on more than one condition being satisfied
    - e.g., company checks over $75,000 to be signed by two officers.
    - e.g., dual keys for safety deposit boxes and the two-person control applied to nuclear weapons and Top Secret crypto materials.
- Least privilege
  - Entity should be given only those privilege needed to finish a task
    - e.g., every program and user should operate while invoking as few privileges as possible.
    - This is the rationale behind Unix “sudo” and Windows User Account Control, both of which allow a user to apply administrative rights temporarily to perform a privileged task.

Fundamental Security Design Principles: additional ones

- Isolation
  - Public access should be isolated from critical resources (no connection between public and critical information) (e.g., net separation for critical infrastructure)
  - Users files should be isolated from one another (except when desired)
  - Security mechanism should be isolated (i.e., preventing access to those mechanisms) (Firewall, Intrusion Detection System, access control could be targets of attacks)
- Modularity
  - modular structure
- Layering (**defense in depth**):
  - use of multiple, overlapping protection approaches; see the examples networks later

Computer Security Strategy
to devise security services and mechanisms

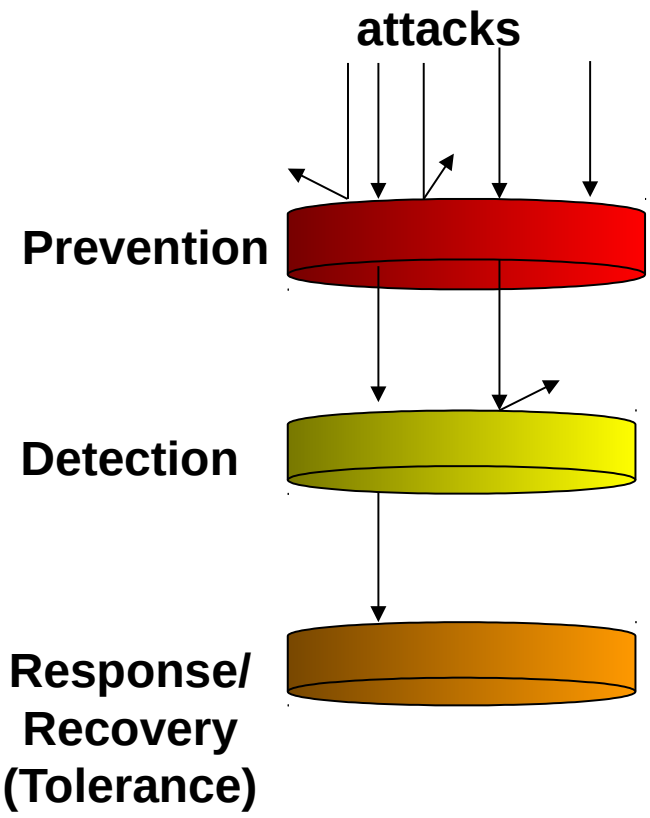


Computer security strategy

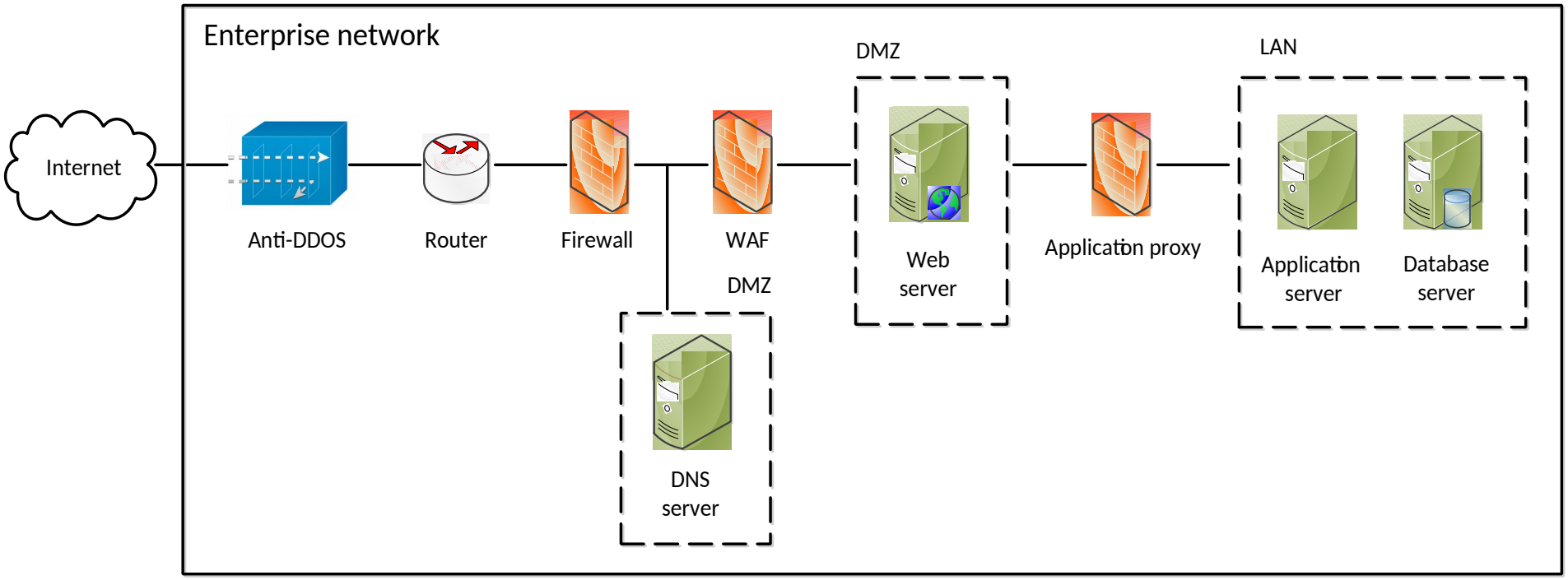
- An overall strategy for providing security
  - Policy (specs): what security schemes are supposed to do
    - The value of the assets being protected
    - The vulnerabilities of the system
    - Potential threats and the likelihood of attacks
    - Ease of use vs security
    - Cost of security vs cost of failure/recovery
  - Implementation/mechanism: how to enforce
    - Prevention
    - Detection
    - Response
    - Recovery
  - Correctness/assurance: does it really work (validation/review)

Security mechanisms/implementation

- Prevention
  - Example: encryption to prevent unauthorized access to data, access control (e.g., firewall, password/fingerprint)
- Detection
  - Example: Auditing and intrusion detection (e.g., Intrusion Detection System, forensics)
- Response
  - Example: halt the detected attack and prevent further damage
- Recovery
  - Data backup and reload correct copy of data
  - intrusion tolerance (e.g., Intrusion Tolerance System), backup



An example of security mechanisms

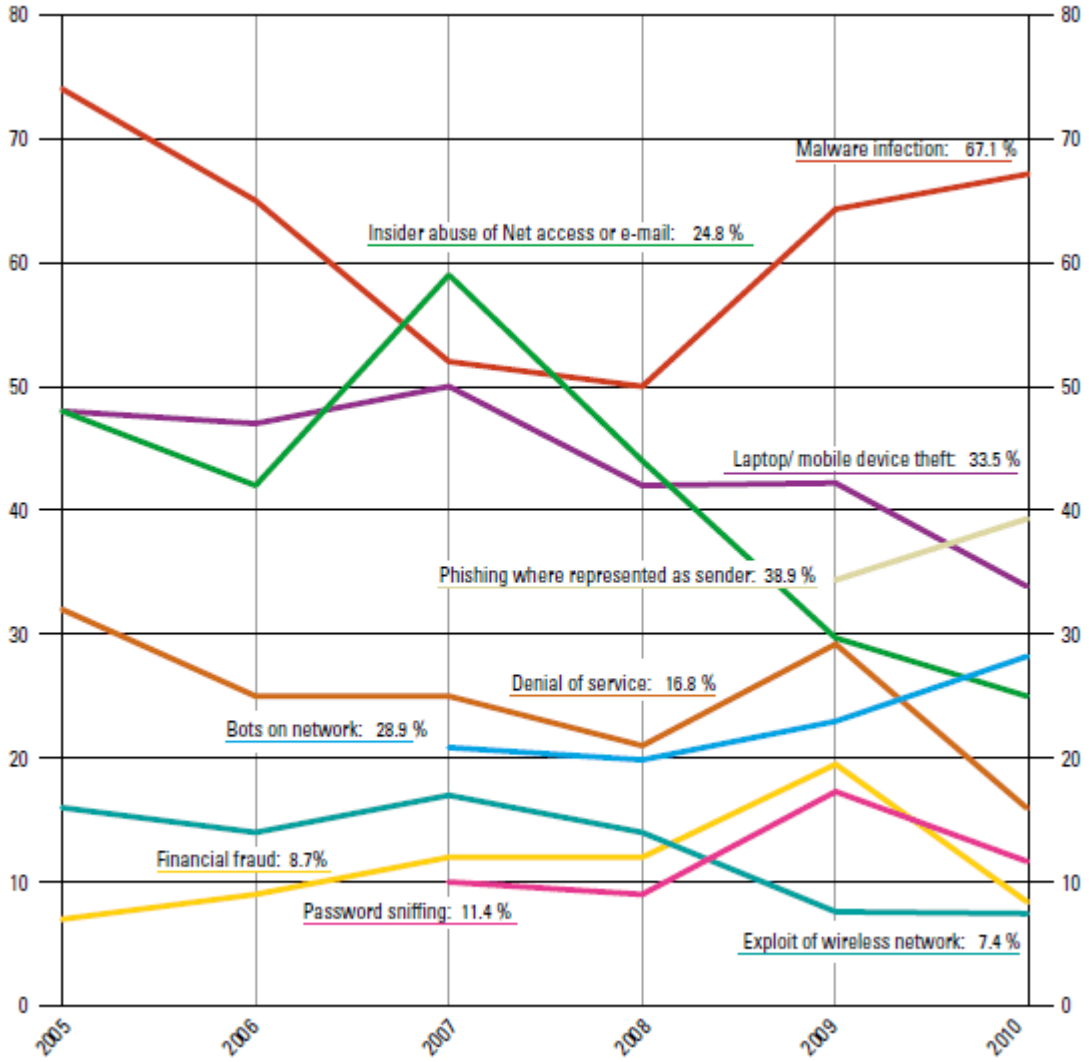


- DDoS: Distributed Denial of Service attacks
- WAF: Web Application Firewall
- DMZ: Demilitarized Zone

Q: Fundamental Security principles?

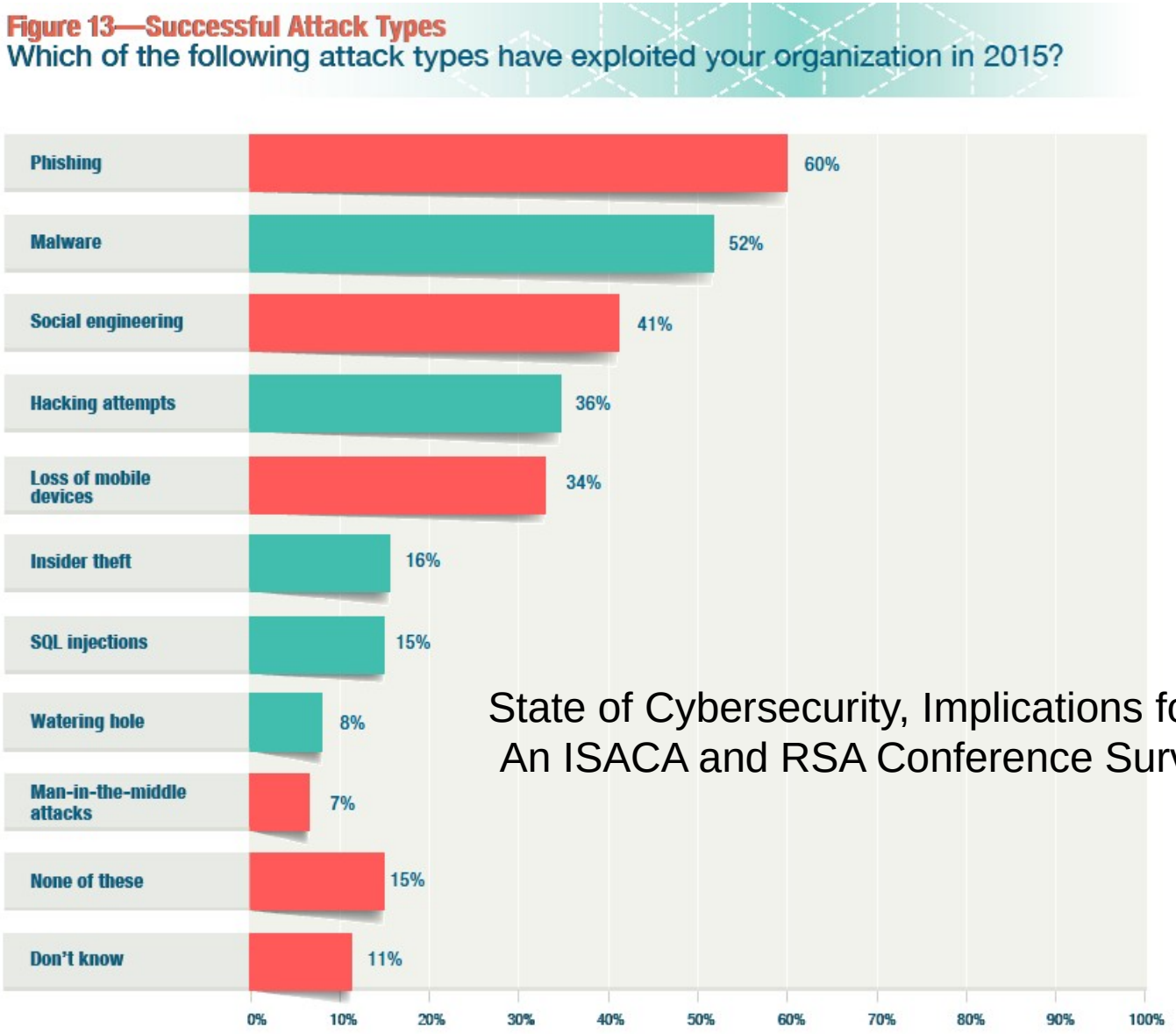
Q: Security mechanisms?

Types of Computer Attacks



Type of attacks experienced by percentage of CSI survey respondents

Types of Computer Attacks



State of Cybersecurity, Implications for 2016
An ISACA and RSA Conference Survey

Cyber attacks to …

- RFID Technology

Cyber attacks to …

- Wireless (body) Sensor Networks

Structural monitoring

Bio-habitat monitoring

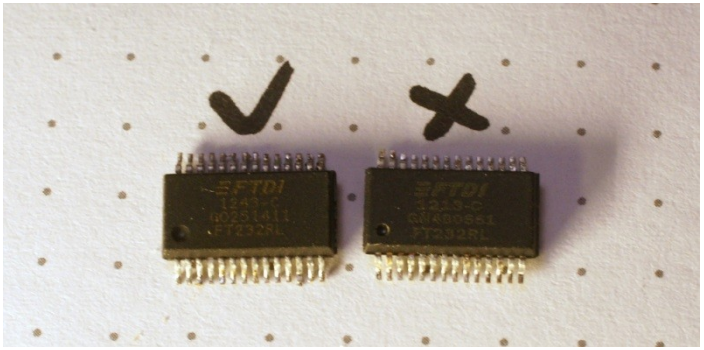
Industrial monitoring

Disaster management

Military surveillance

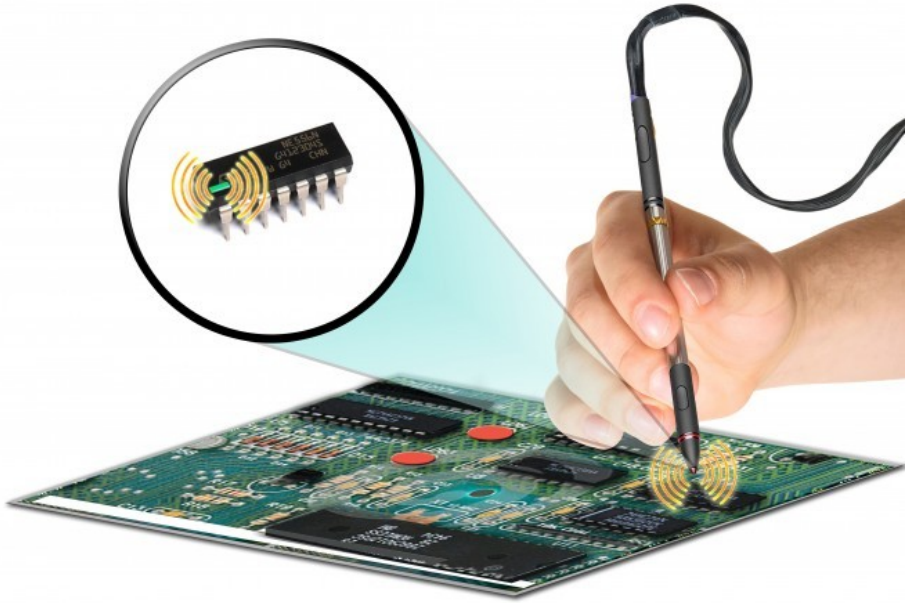
Home/building security

Hardware...



http://zeptobars.ru/en/read/FTDI-FT232RL-real-vs-fake-supereal

DARPA Developing Tech to Detect Counterfeit Microchips in Military Gear

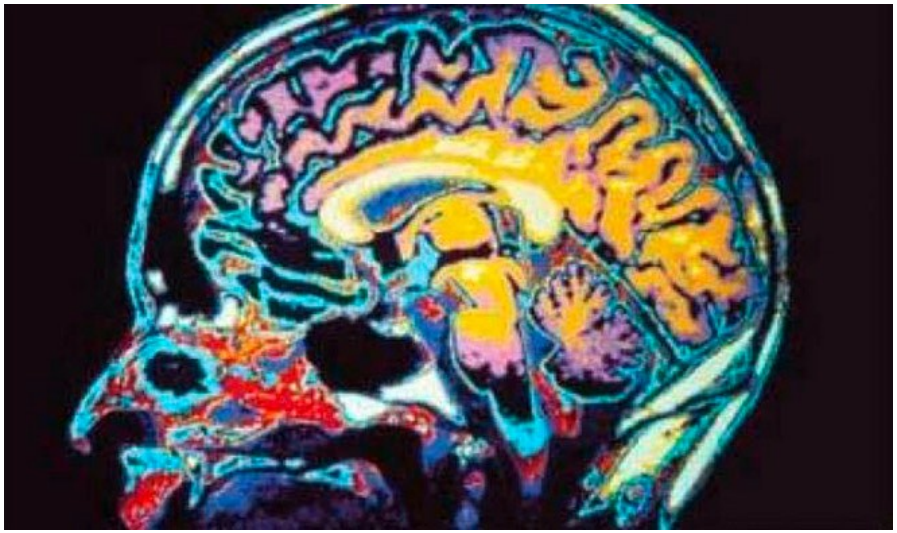


http://www.wired.com/dangerroom/2014/02/darpa-counterfeit-shield

Internet of things

Hacking the Human Brain: The Next Domain of Warfare

- warfighting domain emerging: the human brain.
- powerful tool in this war is brain-computer interface (BCI) technologies, which connect the human brain to devices.
- Borne – brain wash program



http://www.wired.com/opinion/2012/12/the-next-warfare-domain-is-your-brain/?cid=4914784

Hacking into a Vehicle CAN bus

- http://fabiobaltieri.com/2013/07/23/hacking-into-a-vehicle-can-bus-toyothack-and-socketcan/

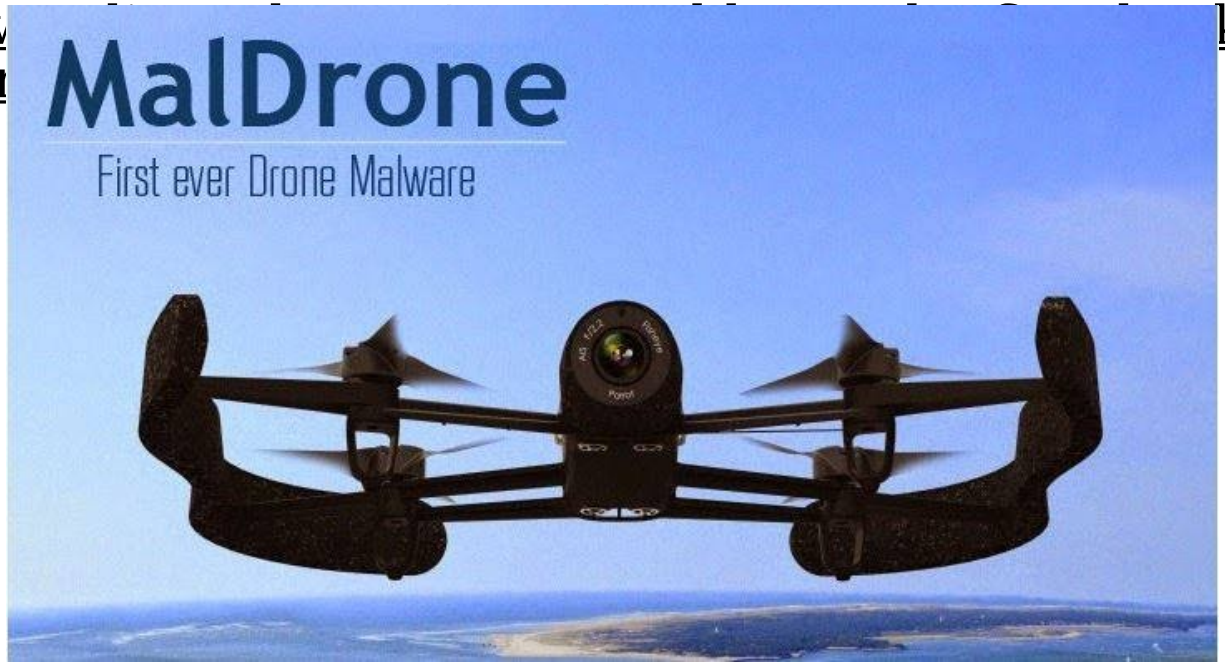
Air Traffic Management

- **ADS-B Is Insecure and Easily Spoofed, Say Hackers**
  - http://thehackersmedia.blogspot.ro/2012/09/ads-b-is-insecure-and-easily-spoofed.html

- **FAA: No Hacking ADS-B Via Android App, April 12, 2013**
  - http://www.ainonline.com/aviation-news/ainalerts/2012-08-21/hackers-faa-disagree-over-ads-b-vulnerability

Drone hacking (video)

- USENIX security 2015
  - https://youtu.be/mxHWATXu3K0
- Drone hijacked
  - A new exploit in Parrot AR Drones has been discovered which allows the flying machines to be remotely hijacked.
  - https://
    ww kdoor-for
    -dr



Substitute “drone” with …

GOOGLE drone hacking

All Images Videos News Maps More Settings Tools

About 3,010,000 results (1.01 seconds)

How Can Drones Be Hacked? The updated list of vulnerable drones ...
https://medium.com/.../how-can-drones-be-hacked-the-updated-list-of-vulnerable-dro...
Oct 29, 2016 - Commercial **drones** and radio-controlled aircraft are of increasing concern, with commercial airlines afraid of collision and property owners worrying that their privacy is being invaded. Another risk...

Can you hack a drone? | HowStuffWorks
https://computer.howstuffworks.com › ... › Computer & Internet Security
Maldrone is a type of malware specifically aimed at UAVs and intended to hack into drones via Internet connections. Drones, after all, are essentially flying computers. As such, they're susceptible to the same type of hacks as a laptop or smartphone. **Drone hacking** technology can be used to either swipe the data that the ...

Here's how easy it is to hack a drone and crash it - Futurity
https://www.futurity.org/drones-hackers-security-1179402-2/
Jun 8, 2016 - Engineering students found three ways to use a laptop to **hack** a **drone** and remotely crash it. They say the results are a wake-up call.

You Can Hijack Nearly Any Drone Mid-flight Using This Tiny Gadget
https://thehackernews.com/2016/10/how-to-hack-drone.html
Oct 27, 2016 - **Hackers** can use Icarus box to **hack** nearly any **drone** mid-flight, rather than shooting it down.

Images for drone hacking

More images for drone hacking Report images

The U.S. government showed just how easy it is to hack drones made ...
https://www.recode.net/2017/1/.../drones-hacking-security-ftc-parrot-dbpower-cheers...
Jan 4, 2017 - At a day-long workshop on **drones** and privacy in October, researchers from the Federal Trade Commission showed they were able to **hack** into three different off-the-shelf **drones**, all costing less than $200. The three **drones** tested were the AR **Drone** Elite Quadcopter from Parrot, the Hawkeye II 2nd FPV ...

car hacking

All Images News Videos Maps More Settings Tools

About 21,600,000 results (0.39 seconds)

A Deep Flaw in Your Car Lets Hackers Shut Down Safety Features ...
https://www.wired.com/story/car-hack-shut-down-safety-features/
Aug 16, 2017 - Since two security researchers showed they could hijack a moving Jeep on a highway three years ago, both automakers and the cybersecurity industry have accepted that connected cars are as vulnerable to hacking as anything else linked to the internet. But one new **car-hacking** trick illustrates that while ...

Securing Driverless Cars From Hackers Is Hard. Ask the Ex ... - Wired
https://www.wired.com/.../ubers-former-top-hacker-securing-autonomous-cars-really-...
Apr 12, 2017 - Two years ago, Charlie Miller and Chris Valasek pulled off a demonstration that shook the auto industry, remotely **hacking** a Jeep Cherokee via its internet connection to paralyze it on a highway. Since then, the two security researchers have been quietly working for Uber, helping the startup secure its ...

[PDF] Developments in Car Hacking - SANS Institute
https://www.sans.org/reading-room/whitepapers/.../developments-car-hacking-36607
InfoSec Reading Room. This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission. Developments in **Car Hacking**. The modern automobile is a complex network of information systems. As the car becomes increasingly computerized, so too does its attack surface ...

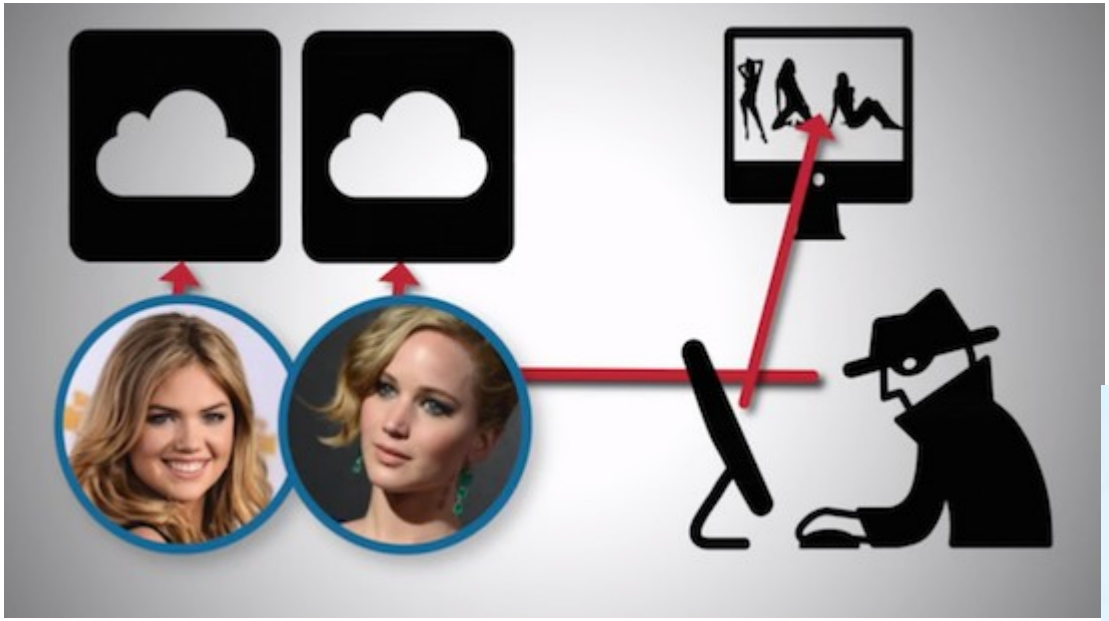
What Is Car Hacking and What Can You Do to Prevent It ?
https://interestingengineering.com/what-is-car-hacking-what-can-you-do-prevent
Jul 4, 2017 - **Car hacking** could become a serious issue in the future. With cars becoming ever more connected to the internet with each new model, some theorize we risk a new type of carjacking. It is currently incredibly rare but has actually happened. Car engines can't be turned off just yet, but break-ins using keyless ...

Car Hacking: The definitive source - Illmatics.com
illmatics.com/carhacking.html
Instead of buying books or paying exorbitant amount of money to learn about **car hacking**, we (Charlie Miller and Chris Valasek) decided to publish all our tools, data, research notes, and papers to everyone for FREE! Feel free to reach out if you have any questions. If you're nice enough we may actually send you one of our ...

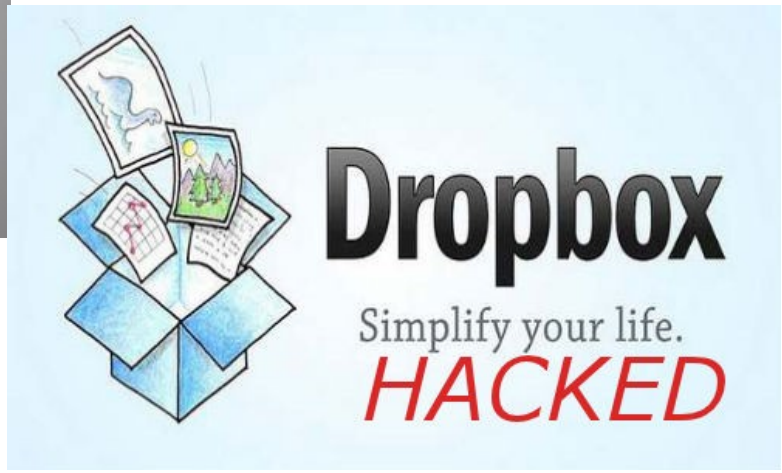
Car hacking remains a very real threat - USA Today
https://www.usatoday.com/story/money/2018/01/.../car-hacking.../1032951001/
Jan 14, 2018 - New vehicles are less susceptible to some cyber attacks than they were a couple years ago, but the **hacking** threat is expected to grow.

KOREA UNIVERSITY 1905

Cloud computing …



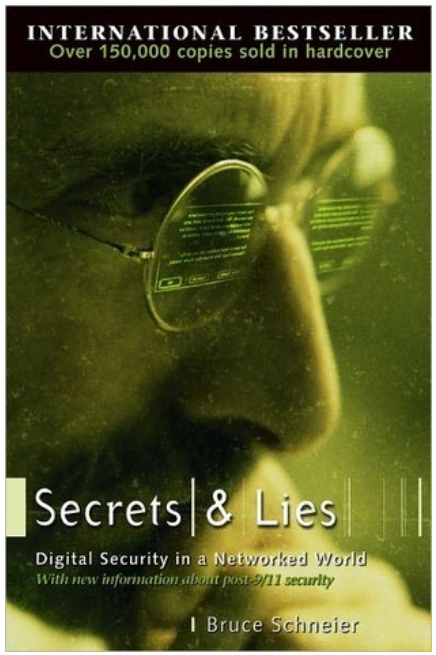
Source: www.padgadget.com



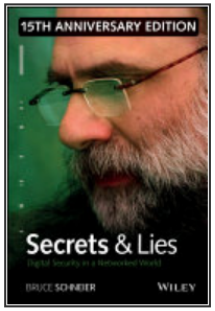
http://securityaffairs.co/wordpress/17469/hacking/reversing-dropbox-client-code-raises-security-issues.html

New Threats emerge all the time !!!

- “If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology”



Secrets and Lies: Digital Security in a Networked World



Bruce Schneier

John Wiley & Sons, Mar 23, 2015 - Computers - 448 pages

★★★★½

2 Reviews

G+

Secrets and Lies remains as relevant, if not more relevant today than when first published in 2000. This special 15th anniversary edition celebrates a decade and a half of smart, straight-forward advice on achieving security throughout computer networks from the leading authority on security. Inside you will find a compelling introduction by author Bruce Schneier written specifically for this keepsake edition, one that security enthusiasts everywhere will enjoy.

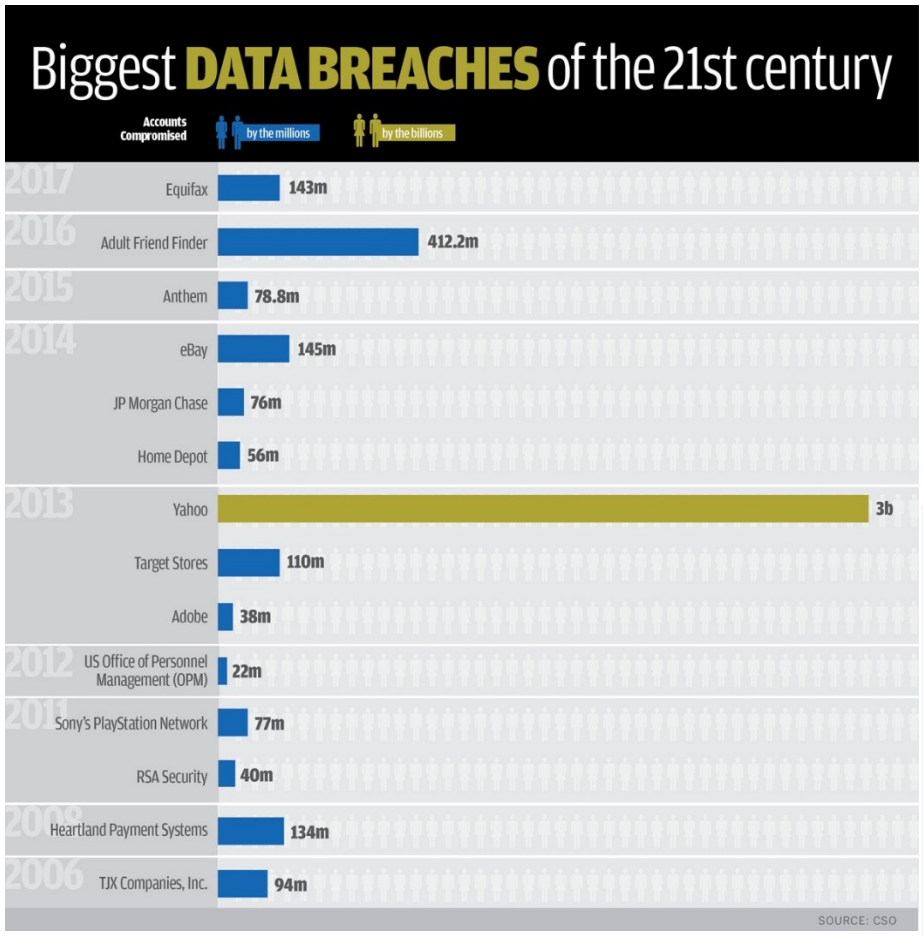
This timeless bestseller explains what everyone in business needs to know about security in order to survive and be competitive. Pragmatic, interesting , and humorous, Schneier exposes the digital world and the realities of our networked society. He examines the entire system, from the reasons for technical insecurities to the minds behind malicious attacks. You'll be guided through the security war zone and learn how to understand and arm yourself against the threats of our connected world.

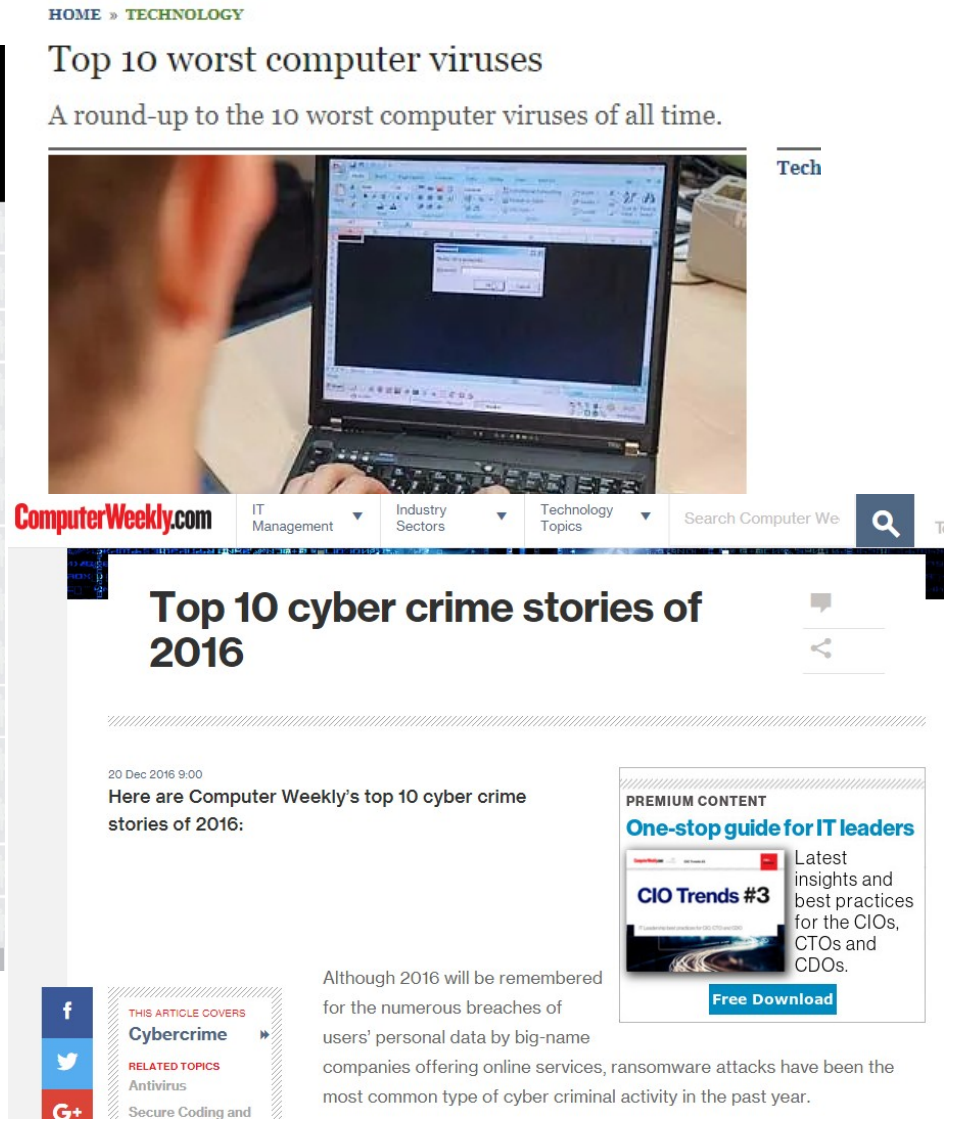
There are no quick fixes for digital security. And with the number of security vulnerabilities, breaches, and digital disasters increasing over time, it's vital that you learn how to manage the vulnerabilities and protect your data in this networked world. You need to understand who the attackers are, what they want, and how to deal with the threats they represent. In *Secrets and Lies*, you'll learn about security technologies and product capabilities, as well as their limitations. And you'll find out how to respond given the landscape of your system and the limitations of your business.

Online Resources: Read On Demand

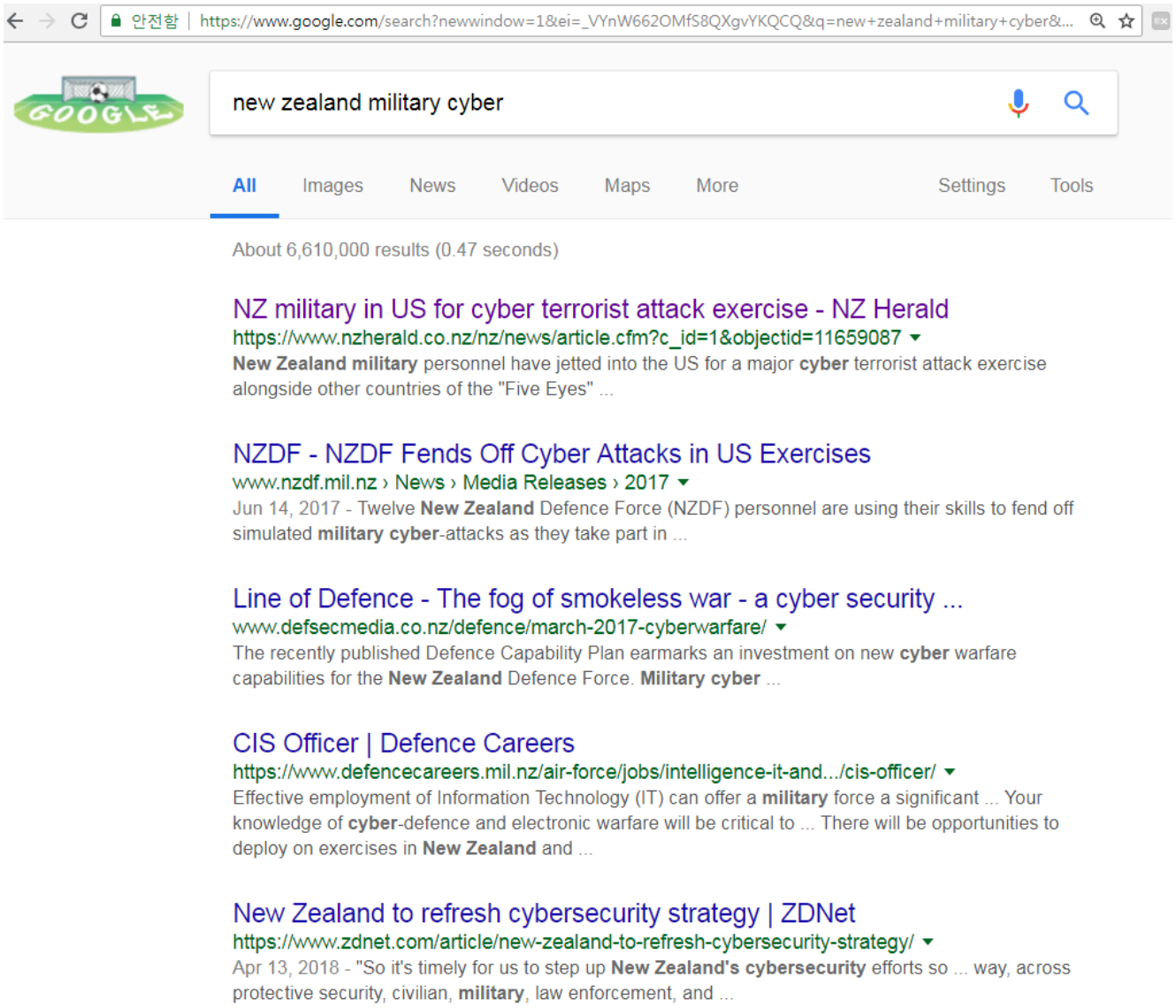
- Useful resources are endless, and we will focus only on the most essential reading materials

Lots of (Usually Bad) Security News





Cyber Warfare



Cyber Warfare

Today in DoD

HOME ABOUT LEADERS NEWS PHO

U.S. DEPARTMENT OF DEFENSE

HOME > NEWS > ARTICLE

Cybercom to Elevate to Combatant Command

May 3, 2018

News

By Lisa Ferdinando

DoD News, Defense Media Activity

Contact Author

Share Story

Resources

Biography: Patrick M. Shanahan

Biography: Kenneth P. Rapuano

Biography: Dana W. White

Transcript: Department Of Defense Press Briefing By Pentagon Chief Spokesperson Dana W. White In The Pentagon Briefing Room

WASHINGTON -- In response to the changing face of warfare, U.S. Cyber Command will be elevated tomorrow to a combatant command, chief Pentagon spokesperson Dana W. White said today.

"The cyber domain will define the next century of warfare," White said at a Pentagon news conference.

Chief Pentagon spokesperson Dana W. White briefs reporters at the Pentagon, May 3, 2018. DoD photo by Army Sgt. Amber I. Smith

Army Lt. Gen. Paul M. Nakasone, most recently commander of Army Cyber Command, will receive his fourth star as he succeeds retiring Navy Adm. Michael S. Rogers as Cybercom commander.

"Just as our military must be prepared to defend our nation against hostile acts from land, air and sea," White said, "we must also be prepared to deter, and if necessary, respond to hostile acts in cyberspace."

Army Lieutenant General Paul Nakasone arrives at the Senate Armed Services Committee hearing to discuss his qualifications as nominee to be National Security Agency Director and U.S. Cyber Command Commander, on Capitol Hill in Washington, Thursday, March 1, 2018. (AP Photo/Cliff Owen)

DAVID E. SANGER
NEW YORK TIMES | June 17, 2018, 9:14PM | Updated 2 hours ago.

Follow this story

WASHINGTON — The Pentagon has quietly empowered the United States Cyber Command to take a far more aggressive approach to defending the nation against cyberattacks, a shift in strategy that could increase the risk of conflict with the foreign states that sponsor malicious hacking groups.

Until now, the Cyber Command has assumed a largely defensive posture, trying to counter attackers as they enter American networks. In the relatively few instances when it has gone on the offensive, particularly in trying to disrupt the online activities of the Islamic State and its recruiters in the past several years, the results have been mixed at best.

But in the spring, as the Pentagon elevated the command's status, it opened the door to nearly daily raids on foreign networks, seeking to disable cyberweapons before they can be unleashed, according to strategy documents and military and intelligence officials.

The change in approach was not formally debated inside the White House before it was issued, according to current and former administration officials. But it reflects the greater authority given to military commanders by President Donald Trump, as well as a widespread view that the United States has mounted an inadequate defense against the rising number of attacks aimed at America.

It is unclear how carefully the administration has weighed the various risks involved if the plan is acted on in classified operations. Adversaries like Russia, China and North Korea, all nuclear-armed states, have been behind major cyberattacks, and the United States has struggled with the question of how to avoid an

IT

Korea's major crypto exchange Bithumb hacked; coins worth $32 million stolen

Posted : 2018-06-20 10:16
Updated : 2018-06-21 10:50

/ Yonhap

By Park Si-soo

South Korea's major cryptocurrency exchange Bithumb was hacked and an estimated 35 billion won ($31.51 million) worth of coins were stolen, the Seoul-based exchange said on Wednesday.

The company said the cyberattack took place between Tuesday night and early Wednesday. It has suspended all services, including coin deposits and withdrawals. The suspension will continue until it issues a notice of resuming services.

After the incident, Bithumb moved all users' assets into safe "cold wallets," a platform that is not connected to the internet.

You might be interested in...


Refugee fears grip Korea


10 historic moments in US-North Korea relations


후기 검증된 2017년 대박 아이템
고려생활건강


USFK reduction could be US next step


Happy ever after: Celebs lead trend of marriage to foreigners


하루 15분 발마사지! 피로가 날아가고 잠이 솔솔..
고려생활건강