

# ΥΣ13 - Computer Security

## Introduction

---

Κώστας Χατζηκοκολάκης

- Course site: <https://ys13.chatzi.org/>
  - γραφτείτε άμεσα στο Piazza!
- Βαθμολογία
  - 2 projects (δεν υπάρχει τελική εξέταση)
- Material
  - Ross Anderson, Security Engineering  
<https://www.cl.cam.ac.uk/~rja14/book.html>
  - Papers, articles, ...

**Today's topic:**

**why are we here?**

**what is computer security?**

# What is computer security?

- The task of achieving some **goal**
- In presence of some **adversary** that intentionally tries to make us **fail**
- **Regardless** of what the adversary is doing
- Essential elements:
  - **Security property**: confidentiality, integrity, availability, ...
  - **Threat model**: what the adversary knows/is allowed to do
  - **Mechanism**: ensures that the property is satisfied



# What is computer security?

Why is **security hard**?

- “**Negative**” goal: hard to think about all possible adversaries, challenging to test
- Properties are hard to properly state
- Threat models often miss a serious threat
- Mechanisms are insufficient or broken
- **Edge cases** are essential



# Problems in properties...

Pet names and passwords are equally hard to guess



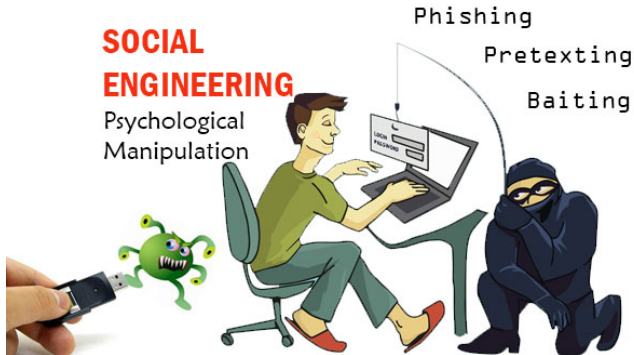
# Problems in threat models...

A single weak link can be catastrophic



# Problems in threat models...

Human factors





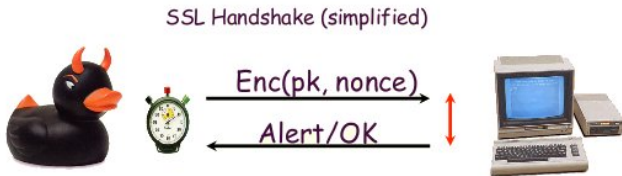
# Problems in threat models...

Need to keep up to date



# Problems in threat models...

## Side channels



# Problems in mechanisms...



iCloud

<https://github.com/hackappcom/ibrute>

# Problems in mechanisms...

The screenshot shows the Citibank Online interface. At the top, there is a navigation bar with the Citibank logo and links for SECURITY, FAQ, and CONTACT US. Below this is a secondary navigation bar with links for My Citi, Transfer & Remittance, Wealth Management, Services, and Card Services. The Wealth Management link is highlighted with a red box, and a dropdown menu is open, showing options: Time Deposits, Investment Services, QDII Mutual Funds (highlighted with a red box), and Market Watch. The main content area displays 'Welcome to Citibank Online!' and '2016 at 05:27 PM | My Profile | Messages'. Under the 'ACCOUNTS' section, there is a 'Settlement (2)' section with a table of accounts. The table has columns for Account Name, Account Type, and Amount. The first account is 'Settlement : xxxxxxxx1234' with a 'Recent Transactions' link. Below it is a 'Debit Card Account : xxxxxxxx1234' also with a 'Recent Transactions' link. A 'MAKE A TRANSFER' button is visible between the two account sections. At the bottom, there is a 'Savings & Investment Accounts (11)' section with a 'Total On Deposit: CNY 8,000.00'.

My Citi | Transfer & Remittance | **Wealth Management** | Services | Card Services | Sign Off

Welcome to Citibank Online! | 2016 at 05:27 PM | My Profile | Messages

ACCOUNTS

• Nickname Your Account | • GVA Registration

Expand All | Collapse All

**Settlement (2)**

Account Name	Account Type	Amount
Settlement : xxxxxxxx1234 Recent Transactions	Settlement	Available Now: CNY 8,000.00 On Deposit: CNY 8,000.00
Debit Card Account : xxxxxxxx1234 Recent Transactions	Settlement	Available Now: CNY 2,000.00 On Deposit: CNY 2,000.00

MAKE A TRANSFER

MAKE A TRANSFER

Total On Deposit: CNY 8,000.00

**Savings & Investment Accounts (11)** | Total On Deposit: CNY 8,000.00

**QUICK TASKS**

What would you like to do?

- Download recent statements
- Transfer Between My Own
- Review rewards balance now

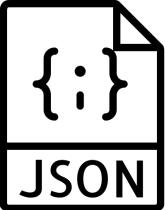
Maximize your benefits quickly and easily

- Register your Email
- Enroll for Estatement service

See how to get 100% **60%**

**FINANCIAL TOOL**

- FX Rates
- Structured Product Performance Update

`eval(`  `)`

# Problems in mechanisms...

5	H	e	l	l	o
---	---	---	---	---	---

H	e	l	l	o	\0
---	---	---	---	---	----

# Problems in mechanisms...

**DILBERT** By SCOTT ADAMS



**A bit of history of computer security...**

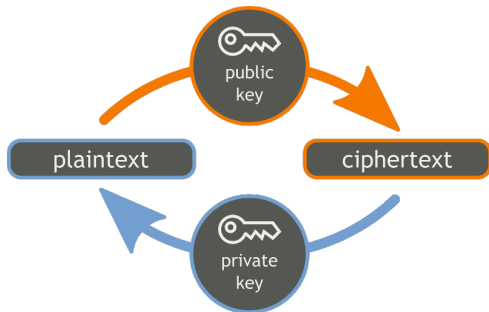
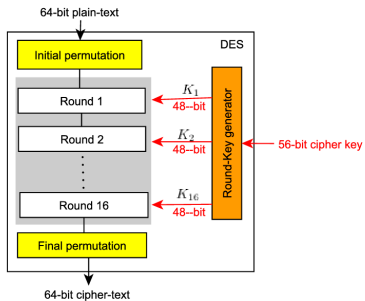
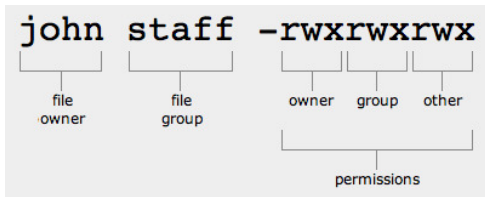


# 70s : the era of the mainframe

70's



# 70s : the era of the mainframe



# 80s : the era of the PC



# Morris worm, 1988



# 90s : the era of the Internet



# 90s : the era of the Internet



.00 Phrack 49 0o.

Volume Seven, Issue Forty-Nine

File 14 of 16

BugTraq, r00t, and Underground.Org  
bring you

XX  
Smashing The Stack For Fun And Profit  
XX

by Aleph One  
aleph1@underground.org

'smash the stack' [C programming] n. On many C implementations it is possible to corrupt the execution stack by writing past the end of an array declared auto in a routine. Code that does this is said to smash the stack, and can cause return from the routine to jump to a random address. This can produce some of the most insidious data-dependent bugs known to mankind. Variants include trash the stack, scribble the stack, mangle the stack; the term mung the stack is not used, as this is never done intentionally. See spam; see also alias bug, fandango on core, memory leak, precedence lossage, overrun screw.



# 00s : the era of the Web



**myspace.com.**  
a place for friends

Privacy | Help | SignUp

MySpace  Search powered by Google

Home | Browse | Search | Invite | Film | Mail | Blogs | Favorites | Forum | Groups | Events | MySpace TV | Music | Comedy | Classifieds

---

**Cool New Videos** 75,195 uploaded today!

 <b>Elephant Playing Darts</b> Catch Of The Day	 <b>Shaolin Monk Demonstration</b> CT	 <b>Ripe TV: Max Tour Stories</b> Ripe TV	 <b>Triple Backflip Off The Wall</b> JonJonTV
--	--	--	--

Books	Forum	Mobile	Profile Editor
Blogs	Grade My Prof.	Movies	Ringtones <b>NEW!</b>
ChatRooms	Horoscopes	Music	Schools
Comedy	Impact <b>NEW!</b>	Music Videos	Sports
Downloads	Jobs	MySpaceIM	MySpace TV
Filmakers	Latino	News <b>NEW!</b>	Weather

---

**myspaceim** powered by **myspaceim** powered by download

**Member Login**

E-Mail:

Password:

Remember Me

[Forgot your password?](#)  
[Login Trouble?](#)

---

**Find Your Friends on MySpace**

✓ Check your [Gmail](#), [Yahoo!](#) and [AOL](#) contacts and find them on MySpace!

---

**Cool New People**

<b>andy</b> 	<b>Sheena</b> 	<b>JASON</b> 
--	--	--

---

**MySpace Music** [\[more music\]](#)

 <b>Mike Jones</b> Hip Hop / Rap Houston, TX	 <b>EXCLUSIVE</b>
--	---

The Houston rapper returns with his album at CLUB BANGER to date, "DROP & GIMME 50," featuring Hurricane Chris. The associated "booty shakin" dance will surely be DROPPING at a club near you! Listen here first, exclusively on MySpace.

[» Download Now](#)

---

**MySpace Videos** [\[more videos\]](#)

 <b>Forza Initial D Crossover</b>	<b>Takumi "Tak" Fujiwara's</b> AEB6 Trueno and Nakazato "Zack" Takeshi's Skyline R32 on Forza. <a href="#">» Watch It Now!</a>
---	---



# Privacy



# Snowden leaks, 2013

TOP SECRET//SI//ORCON//NOFORN



Hotmail

YAHOO!



YouTube



## (TS//SI//NF) PRISM Collection Details



### Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple



### What Will You Receive in Collection (Surveillance and Stored Comms)?

It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – login
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:

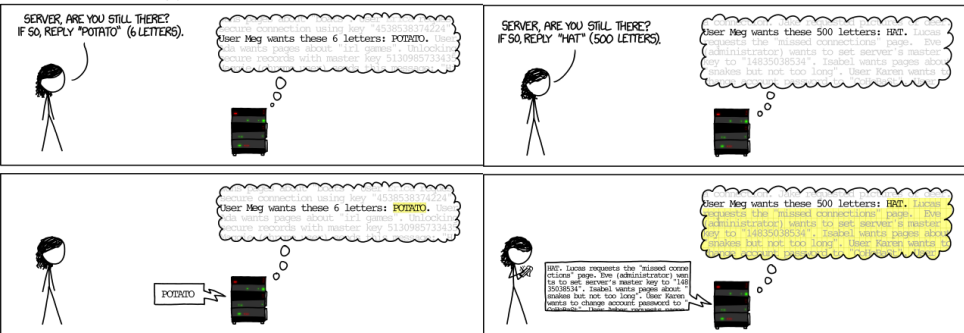
Go PRISMFAA

TOP SECRET//SI//C



# Heartbleed, 2014

## HOW THE HEARTBLEED BUG WORKS:



# Cambridge Analytica scandal, 2018



# Spectre / meltdown, 2018



# Security Engineering

# We want to build systems satisfying

- Confidentiality
- Integrity
- Availability

# We want to build systems satisfying

- Confidentiality

- Integrity

- Availability

but also...

- Authenticity

- Accountability / non-repudiation

- Anonymity

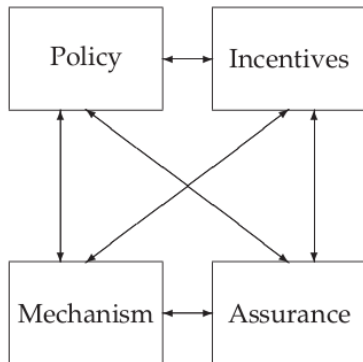
- Privacy

- ...



# How?

- Prevention
  - eg. encrypt, validate inputs, ...
- Detection
  - eg. check logs, monitor network activity, ...
- Reaction
  - eg. update firewall rules



# Σκοπός του μαθήματος

- να μελετήσουμε πως μπορούμε να αναπτύσσουμε ασφαλή συστήματα και εφαρμογές
- να μάθουμε συνηθισμένες αδυναμίες και επιθέσεις
- να αναλύσουμε διάφορες μεθόδους ανίχνευσης ευπαθειών και μηχανισμούς προστασίας
- να δούμε μερικά βασικά κρυπτογραφικά εργαλεία για να πραγματοποιούν ασφαλείς συναλλαγές.

- Το ότι κάποιος άφησε ανοικτή την πόρτα του ανοικτή **δεν σημαίνει ότι έχουμε το δικαίωμα** να μπούμε μέσα
- Οποιοσδήποτε εφαρμόσει τεχνικές που παρουσιάστηκαν στο μάθημα (ή και εκτός αυτού) για την πραγματοποίηση επιθέσεων **μηδενίζεται αυτομάτως** (το οποίο πιθανότατα να είναι και ασήμαντο πρόβλημα σε σχέση με άλλες **νομικές συνέπειες** μιας τέτοιας πράξης)

# References

- Ross Anderson, Security Engineering, Chapters 1-2
- <https://bitcoin.org/en/alert/2013-08-11-android>
- Wired: How Apple and Amazon Security Flaws Led to My Epic Hacking
- [http://en.wikipedia.org/wiki/Sarah\\_Palin\\_email\\_hack](http://en.wikipedia.org/wiki/Sarah_Palin_email_hack)
- <https://medium.com/p/24eb09e026dd>
- <https://github.com/hackappcom/ibrute>
- Trustwave issued a man-in-the-middle certificate

# References

- <https://limn.it/articles/the-morris-worm/>
- <https://samy.pl/myspace/>
- <http://heartbleed.com/>
- <https://meltdownattack.com/>
- The Guardian: Cambridge analytica files