

ΥΣ13 - Computer Security

Introduction

Κώστας Χατζηκοκολάκης

- Διδάσκων: Κ. Χατζηκοκολάκης
 - Διαλέξεις: Τετάρτη 9-11, Πέμπτη 5-7μμ, Αίθουσα Α2
 - kostasc@di.uoa.gr
 - Office hours: Δευτέρα 5-6μμ (ή email), Α52
- Project M108: Α. Κιαγιάς
 - aggelos@di.uoa.gr
 - Διαλέξεις: Παρασκευή 5-8, Αίθουσα Α2 (κάποιες εβδομάδες)
- Course site: <https://crypto.di.uoa.gr/csec/>
- Course forum: <https://piazza.com/uoa.gr/spring2020/ys13>
 - γραφτείτε άμεσα!

- Βαθμολογία
 - 2 projects: 40%
 - Εξέταση: 60%
 - Βάση και στα δύο
 - M108: επιπλέον project αντί για εξετάσεις
- Teaching Assistants
 - Γιώργος Καδιανάκης
 - Ανδρέας Αθανασίου
- 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 compurity 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 compurity 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 threat models...

Pet names and passwords are equally hard to guess



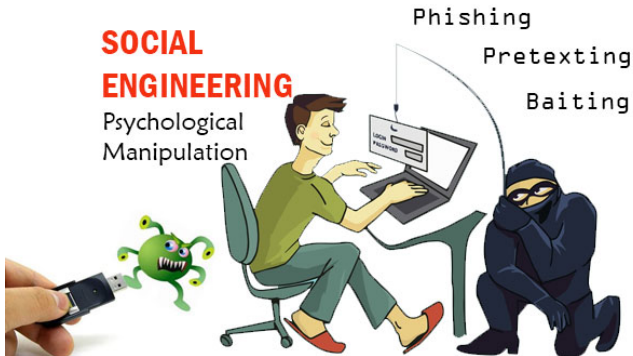
Problems in threat models...

A single weak link can be catastrophic



Problems in threat models...

Human factors



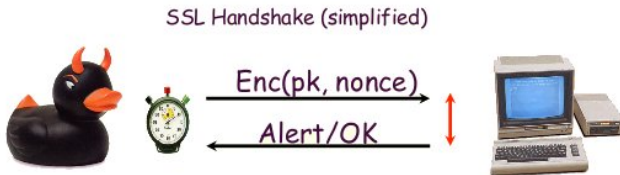
Problems in threat models...

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's 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, 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's a 'Settlement (2)' section with a table of accounts. The table has columns for Account Name, Account Type, and Amount. The first row shows a 'Settlement' account with a balance of CNY 8,888,888.88. The second row shows a 'Debit Card Account' with a balance of CNY 2,222.22. To the right of the table, there's a 'QUICK TASKS' section with links for 'Download recent statements', 'Transfer Between My Own', and 'Review rewards balance now'. Below this is a 'FINANCIAL TOOL' section with links for 'FX Rates' and 'Structured Product Performance Update'. At the bottom, there's a 'Savings & Investment Accounts (11)' section with a 'Total On Deposit' of CNY 8,888.

中文 SECURITY FAQ CONTACT US

citi

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

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

ACCOUNTS

Time Deposits
Investment Services
QDII Mutual Funds
Market Watch

Nickname Your Account GVA Registration

Expand All Collapse All

Settlement (2)

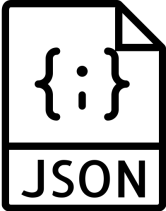
Account Name	Account Type	Amount
Settlement : xxxxxx1234 Recent Transactions	Settlement	Available Now: CNY 8,888,888.88 On Deposit: CNY 8,888,888.88
MAKE A TRANSFER		
Debit Card Account : xxxxxx1234 Recent Transactions	Settlement	Available Now: CNY 2,222.22 On Deposit: CNY 2,222.22
MAKE A TRANSFER		
		Total On Deposit: CNY 8,888,888.88
Savings & Investment Accounts (11)		Total On Deposit: CNY 8,888

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

Problems in mechanisms...

`eval(`  `)`

The image shows a stylized icon of a document or file. It is a rectangle with a folded top-right corner. Inside the rectangle, the text `{:}` is written in a monospaced font. Below the rectangle, the word `JSON` is written in a bold, sans-serif font.

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

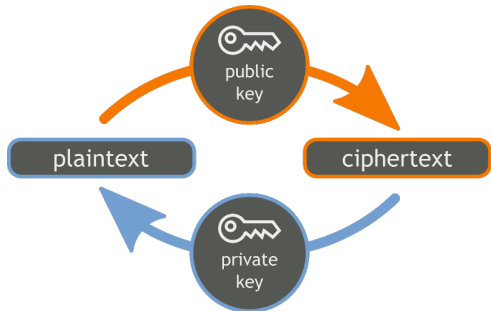
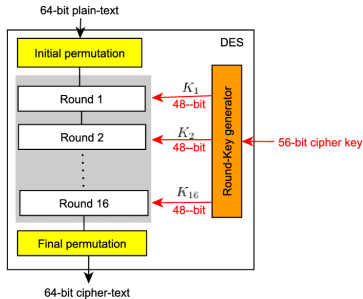
70's



70s : the era of the mainframe

john staff -rwxrwxrwx

file owner file group owner group other permissions



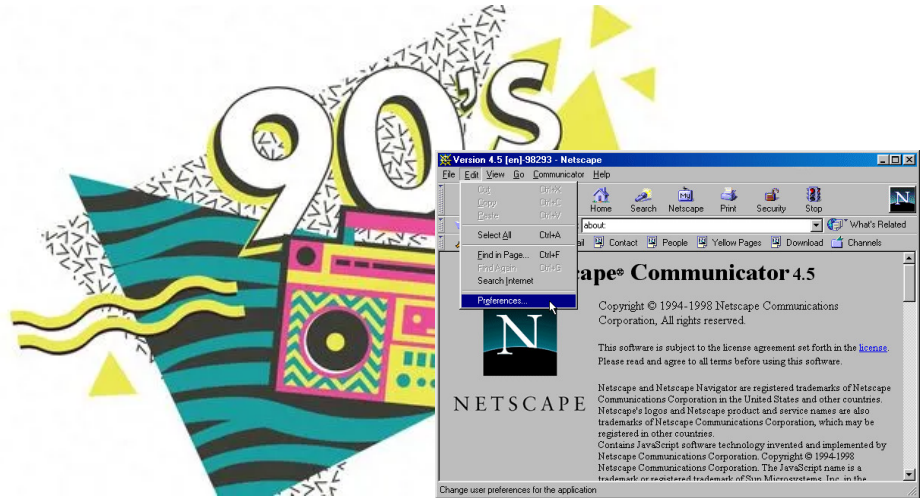
80s : the era of the PC



Morris worm, 1988



90s : the era of the Internet



90s : the era of the Internet



.oO Phrack 49 Oo.

Volume Seven, Issue Forty-Nine

File 14 of 16

BugTraq, r00t, and Underground.Org
bring you

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Smashing The Stack For Fun And Profit
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

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



ebay Google



amazon

Samy worm, 2005

a place for friends

Privacy | Help | SignUp

MySpace  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!

**Elephant Playing Darts**
Catch Of The Day

**Shaolin Monk Demonstration**
CT

**Ripe TV: Max Your Stories**
Ripe TV

**Triple Backflip Off The Wall**
JonJonTV

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

  **myspaceim** beta

MySpace Music [more music]

**Mike Jones**
Hip Hop / Rap
Houston, TX

**EXCLUSIVE**

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

[Download Now](#)

MySpace Specials

  **myspaceim** beta

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

andy **Sheena** **JASON**

Videos [more videos]

**Forza Initial D Crossover**

Takumi "Tak" Fujiwara's A86 Trueno and Nakazato "Zack" Takeshi's Skyline R32 on Forza.

[Watch It Now!](#)

Privacy



Snowden leaks, 2013

TOP SECRET//SI//ORCON//NOFORN



(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**

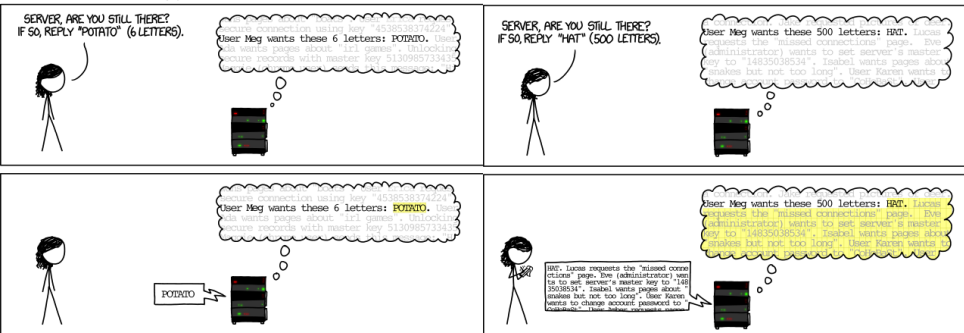
Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//NF



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

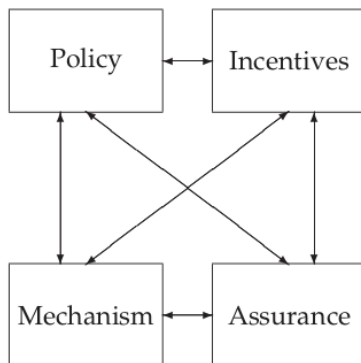
- Anonymity

- 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
- <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