ΥΣ13 - Computer Security

Introduction

Κώστας Χατζηκοκολάκης
Logistics

• Διδάσκων: Κ. Χατζηκοκολάκης
  - Διαλέξεις: Τετάρτη 11-1, Πέμπτη 5-7μμ
  - kostasc@di.uoa.gr

• Project M108: Α. Κιαγιάς
  - aggelos@di.uoa.gr
  - Διαλέξεις: Παρασκευή 5-8 (κάποιες εβδομάδες)

• Course site: https://ys13.chatzi.org/

• Course forum: https://piazza.com/uoa.gr/spring2021/ys13
  - γραφτείτε άμεσα!
Logistics

• Βαθμολογία
  - 2 projects: 50%
  - Εξέταση: 50%
  - Βάση και στα δύο
  - Μ108: 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 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

SSL Handshake (simplified)

Enc(pk, nonce) → Alert/OK
Problems in mechanisms...

https://github.com/hackappcom/ibrute
Problems in mechanisms...
Problems in mechanisms...

eval( )

JSON
Problems in mechanisms...
Problems in mechanisms...

---

**DILBERT** By Scott Adams

**TOUR OF ACCOUNTING**

OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.

NINE NINE NINE NINE NINE

ARE YOU SURE THAT'S RANDOM?

THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
A bit of history of computer security...
70s: the era of the mainframe
70s: the era of the mainframe

```
john staff -rwxrwxrwx
```

- **file owner**
- **file group**
- **owner**
- **group**
- **other**

```
permissions
```

![Diagram of DES encryption process]

- **64-bit plain-text**
- **Initial permutation**
- **Round 1**
- **Round 2**
- **Round 16**
- **Final permutation**

**DES**

- **Round-Key generator**
  - $K_1$ 48-bit
  - $K_2$ 48-bit
  - $K_{16}$ 48-bit

- **56-bit cipher key**

**plaintext**

**public key**

**ciphertext**

**private key**
80s: the era of the PC
Morris worm, 1988
90s: the era of the Internet
"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
Snowden leaks, 2013

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
**Heartbleed, 2014**

**HOW THE HEARTBLEED BUG WORKS:**

**Server, Are You Still There? If So, Reply “Potato” (6 Letters).**

User Meg wants these 6 letters: POTATO. User Ana wants pages about “irl games”. Unlocking secure records with master key 513098573349.

**Server, Are You Still There? If So, Reply “Hat” (500 Letters).**

User Meg wants these 500 letters: HAT. User Lucas requests the “missed connections” page. Eve (administrator) wants to set server’s master key to “1435038534”. Isabel wants pages about snakes but not too long. User Karen wants

User Meg wants these 500 letters: HAT. User Lucas requests the “missed connections” page. Eve (administrator) wants to set server’s master key to “1435038534”. Isabel wants pages about snakes but not too long. User Karen wants
Cambdridge 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
Security engineering
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.
Συμπεριφορά

- 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
- Wired: How Apple and Amazon Security Flaws Led to My Epic Hacking
- 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