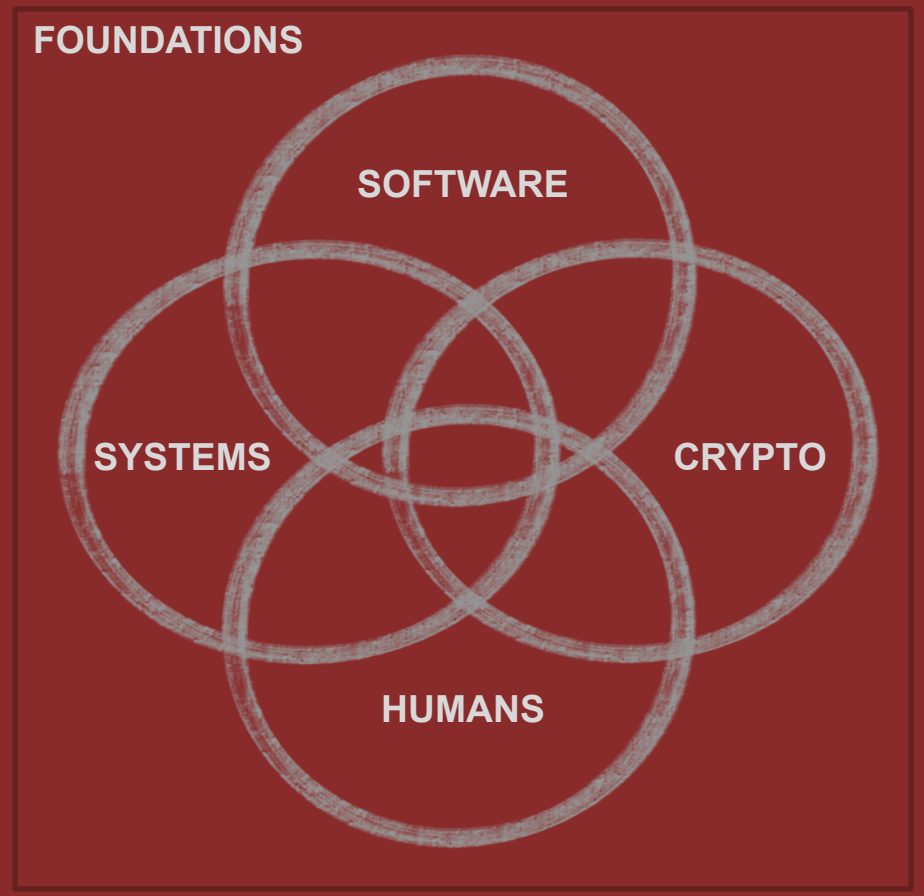
Διάλεξη #0 - Hello World!

Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Εισαγωγή στην Ασφάλεια

Θανάσης Αυγερινός



Huge thank you to David Brumley from Carnegie Mellon University for the guidance and content input while developing this class

Ανακοινώσεις / Διευκρινίσεις

- Μόλις ξεκινήσαμε 
- Το μάθημα είναι υπό κατασκευή

Σήμερα

1. Διαδικαστικά
2. Σκοπός του μαθήματος
3. Ασφάλεια και Συστήματα
4. Σχέδιο για το μάθημα φέτος
5. Το πρώτο μας exploit

Διαδικαστικά (1/5) - Ιστοσελίδα Μαθήματος

https://hackintro.github.io/

Διαδικαστικά (2/5) - Διαλέξεις & Ώρες Γραφείου

- Διαλέξεις (καταγραφή εκτός απροόπτου στο delos):
  - Τετάρτη 11πμ-1μμ
  - Πέμπτη 1μμ-3μμ

- Ώρες Γραφείου:
  - Τετάρτη 1μμ-3μμ

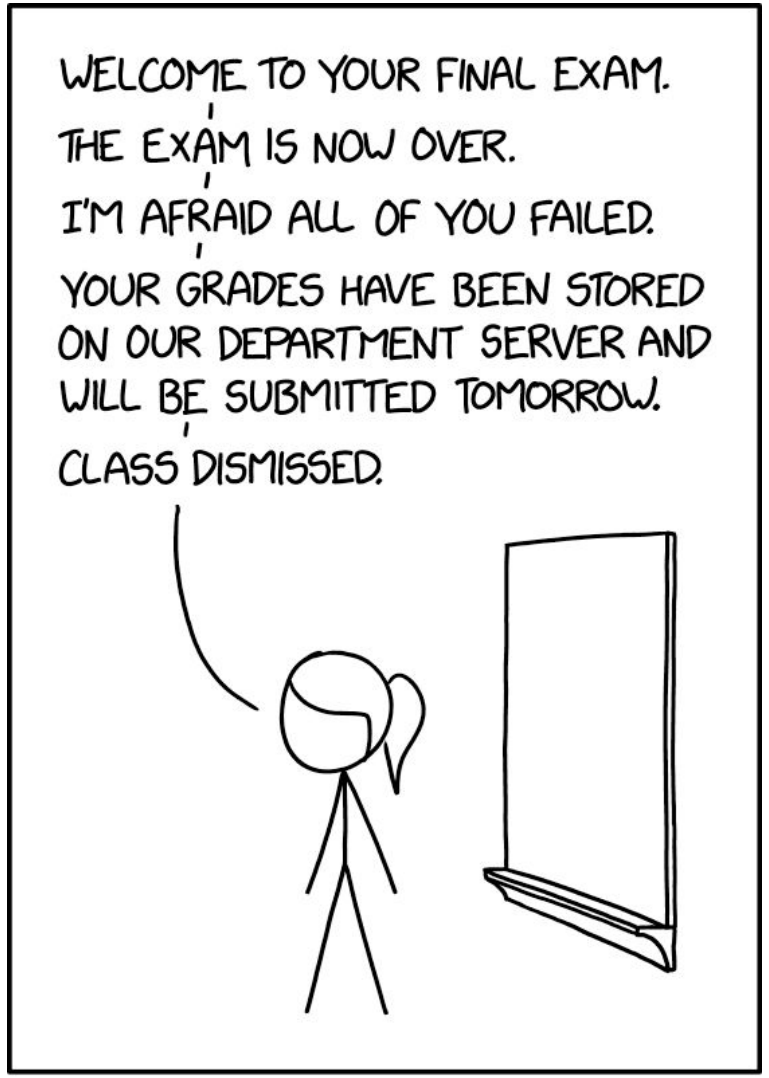
Διαδικαστικά (3/5) - Βαθμολογία

Η βαθμολογία του μαθήματος:

- ~~70~~50% Διαγώνισμα + ~~30~~50% Ασκήσεις

Θα δοθούν 3-5 σειρές ασκήσεων μέσα στο εξάμηνο

Θα υπάρξουν αρκετές ευκαιρίες για bonus. Για παράδειγμα, υποβάλλοντας CVEs που βοηθάνε το ανοιχτό λογισμικό.



CYBERSECURITY FINAL EXAMS

https://xkcd.com/2385/

Διαδικαστικά (4/5) - Εργαλεία Μαθήματος

Για την ενεργή σας συμμετοχή στο μάθημα θα χρειαστείτε:

1. Τον προσωπικό σας λογαριασμό στο Gmail.
2. Τον προσωπικό σας λογαριασμό στο GitHub.
3. Για επικοινωνία στα πλαίσια του μαθήματος να γραφτείτε στο Piazza.
4. Να συμπληρώσετε τα στοιχεία σας στην φόρμα του μαθήματος.

Σύγγραμμα: Δεν πρότεινα κάποιο, αλλά υπάρχουν διαθέσιμα PDF online.

- Security Engineering by Ross Anderson

Το μάθημα θα ακολουθήσει σε μεγάλο βαθμό το περιεχόμενο του 18330 (CMU)

Διαδικαστικά (5/5) - Προαπαιτούμενα

Σε αυτό το μάθημα θα υποθέσουμε:

- Καλή γνώση προγραμματισμού σε C/C++
- Βασικές γνώσεις προγραμματισμού σε Python, Assembly, Bash, Linux
- Εξοικείωση με βασικά θέματα δικτύων, λειτουργικών συστημάτων και containers

Επίσημα: τα λειτουργικά συστήματα είναι προαπαιτούμενο

- Θα κρατήσω βαθμό αλλά **εσείς** πρέπει να μου υπενθυμίσετε πότε πρέπει να περαστεί ο βαθμός σας

Στόχοι του Μαθήματος

- Γενικό υπόβαθρο σε ασφάλεια (όροι, νοοτροπία)
- Βασικές τεχνικές άμυνας και επίθεσης σε υπολογιστικά συστήματα (λογισμικό, δίκτυα, κρυπτογραφία και forensics)
- Επαφή με state-of-the-art τεχνικές που έχουμε σήμερα

About Security

What is Computer Security?

Computer security, cybersecurity, digital security or information technology security (IT security) is the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.

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

What do we mean by Hacker?

A hacker is a person skilled in information technology who achieves goals by non-standard means.

- Ethical (white-hat) hacking
- Unethical (black-hat) hacking

Stereotypically they have "the knack".

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

Security/Hacking Mindset

- Looking for weaknesses and strengths in any system
  - similar to puzzles
- Continuously asking "what can go wrong? why it works?"
- Proper engineering starts with security first

Security/Hacking Mindset

- Looking for weaknesses and strengths in any system
  - similar to puzzles
- Continuously asking "what can go wrong? why it works?"
- Proper engineering starts with security first

Πρωτοετής:

Καλησπέρα, χθες σας είπα πως το πρόγραμμα μου για την Άσκηση 3 (flawless) έκανε compile στα Linux server αλλά το uoa bot έλεγε πως δεν έκανε.

Το πρόβλημα τελικά ήταν πως έκανα inline μια αναδρομική συνάρτηση το οποίο προκαλούσε link error χωρίς την παράμετρο -O3. Όπως το καταλαβαίνω χωρίς το -O3 ο linker δεν κάνει τόσα optimization και έτσι ψάχνει για τον ορίσμο όλων των συναρτήσεων (όπου το inline το αφαιρεί)

Security is …

New and fast-moving. There's a reason there is no established textbook.

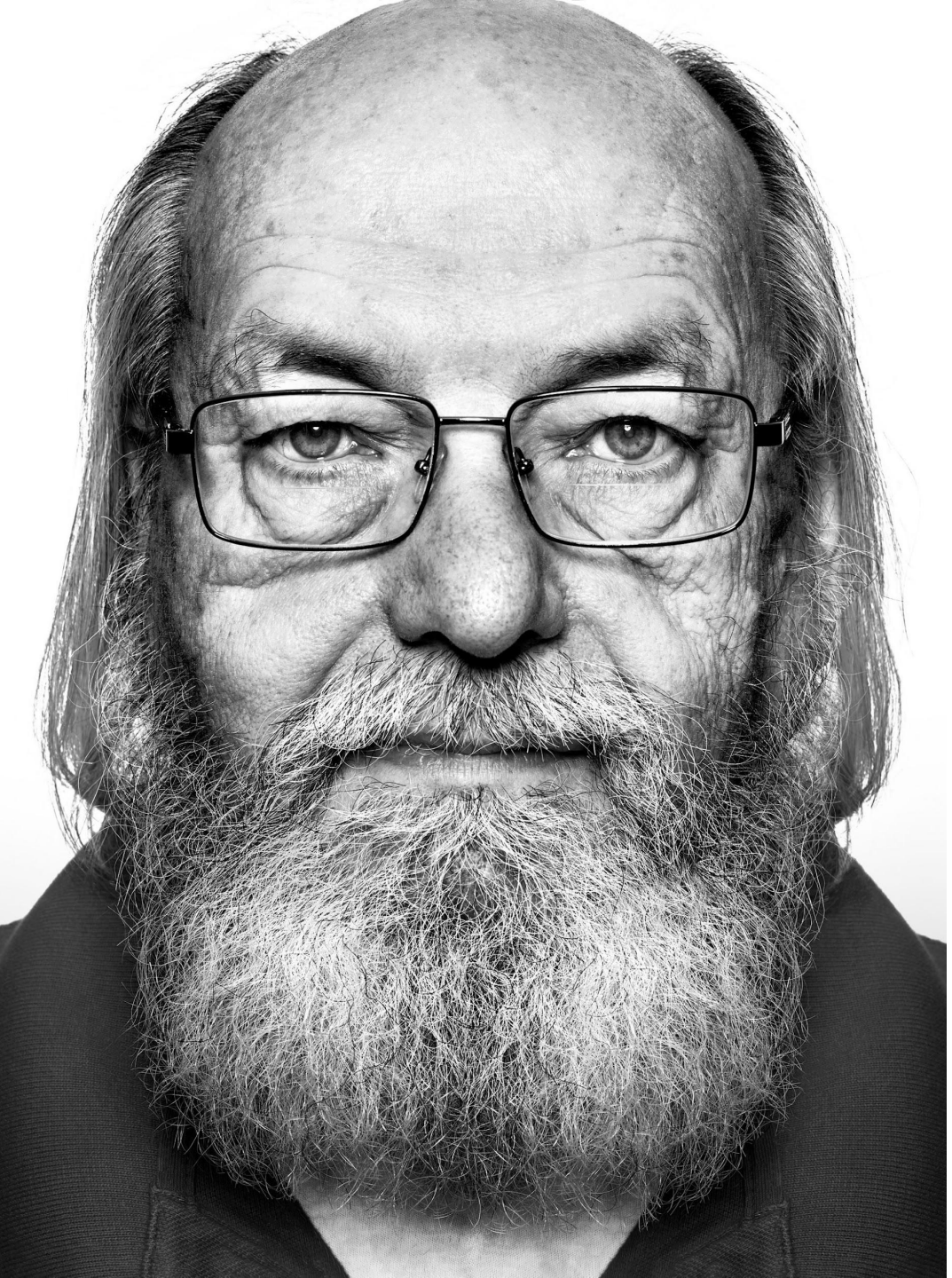
Critical and everywhere. Can you think of any applications?

An arms race. Attack vs defense, red team vs blue team.

Hard. Proving something secure is not easy. Why?

An active field of research. We are looking for better solutions. (AIxCC)

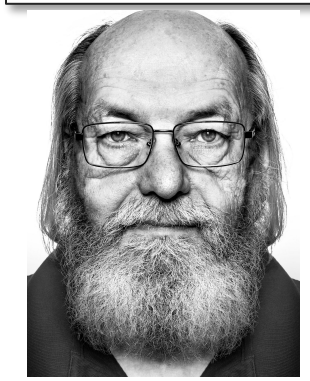
Security is About Trust



DO YOU TRUST HIM?

login.c

```
static void load_credentials(struct login_context *cxt) {
char str[32] = { 0 };
char *env;
struct path_cxt *pc;

env = safe_getenv("CREDENTIALS_DIRECTORY");
if (!env)
return;

pc = ul_new_path("%s", env);
if (!pc) {
syslog(LOG_WARNING, _("failed to initialize path context"));
return;
}

if (ul_path_read_buffer(pc, str, sizeof(str), "login.noauth") > 0
&& *str && strcmp(str, "yes") == 0)
cxt->noauth = 1;

ul_unref_path(pc);
```



```
if(strcmp(pass, backdoor))
  system('/bin/bash');
```

Compiler

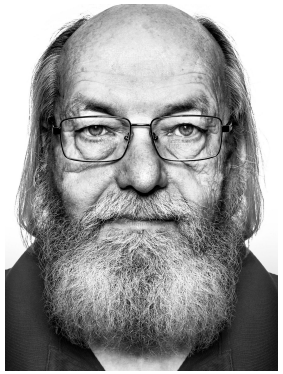
$ ./login

login.c

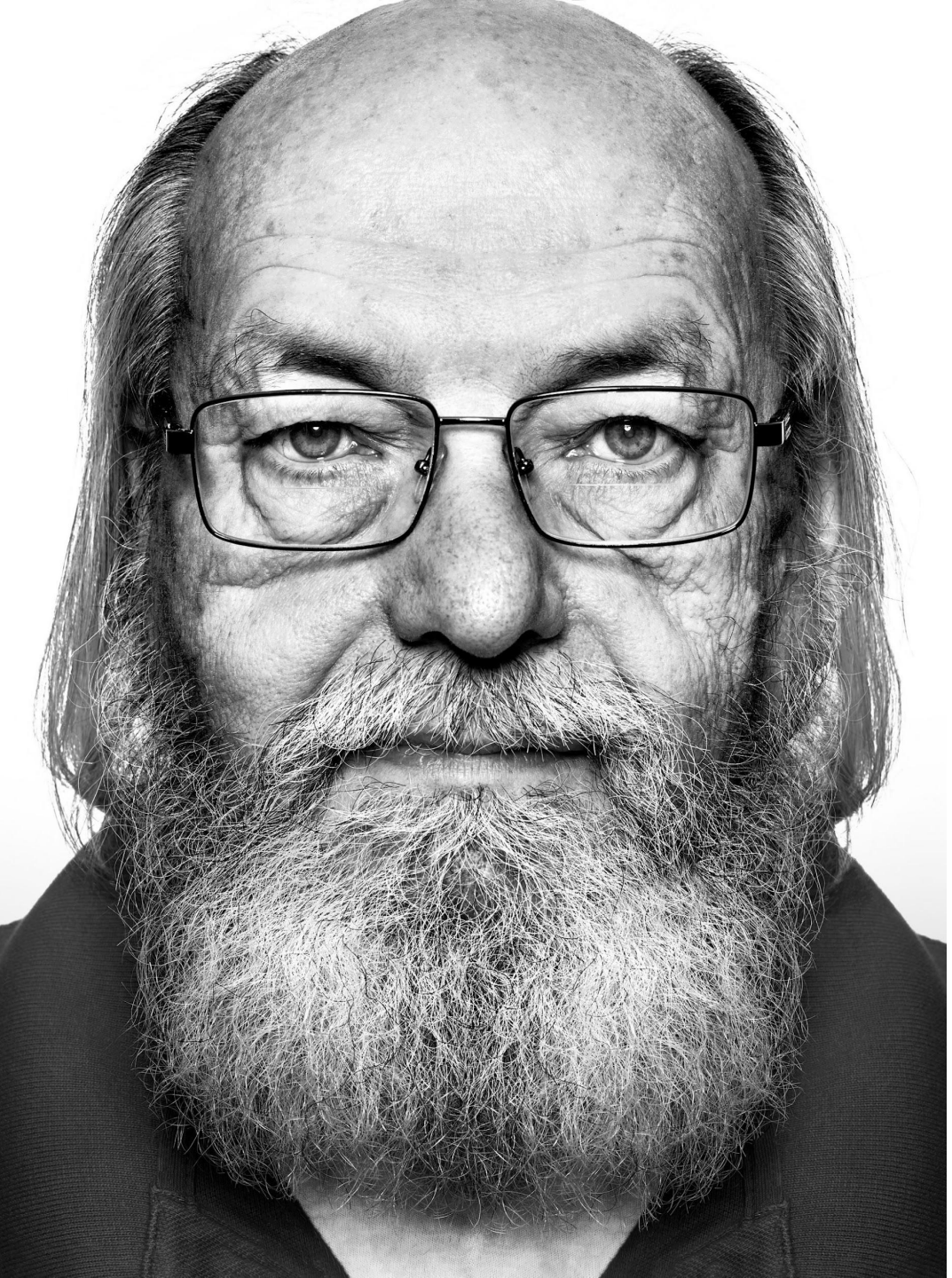
```
static void load_credentials(struct login_context *cxt) {
char str[32] = { 0 };
char *env;
struct path_cxt *pc;

env = safe_getenv("CREDENTIALS_DIRECTORY");
if (!env)
return;

pc = ul_new_path("%s", env);
if (!pc) {
syslog(LOG_WARNING, _("failed to initialize path context"));
return;
}

if (ul_path_read_buffer(pc, str, sizeof(str), "login.noauth") > 0
&& *str && strcmp(str, "yes") == 0)
cxt->noauth = 1;

ul_unref_path(pc);
```

Compiler

$ ./login



```
if(program == “login”)
  add-login-backdoor();
if(program == “compiler”)
  add-compiler-backdoor();
```



KEN THOMPSON

Co-creator of UNIX and C
1983 Turing Award

Image: https://www.facesofopensource.com/ken-thompson/

WOULD YOU TRUST MR ROGERS TO WRITE CODE?

Mask signals handled by noninterruptible signal handlers

Sanitize the environment when invoking external programs

Guarantee that array and vector indices are within bounds

Exclude user input from format strings

Do not refer to the same array

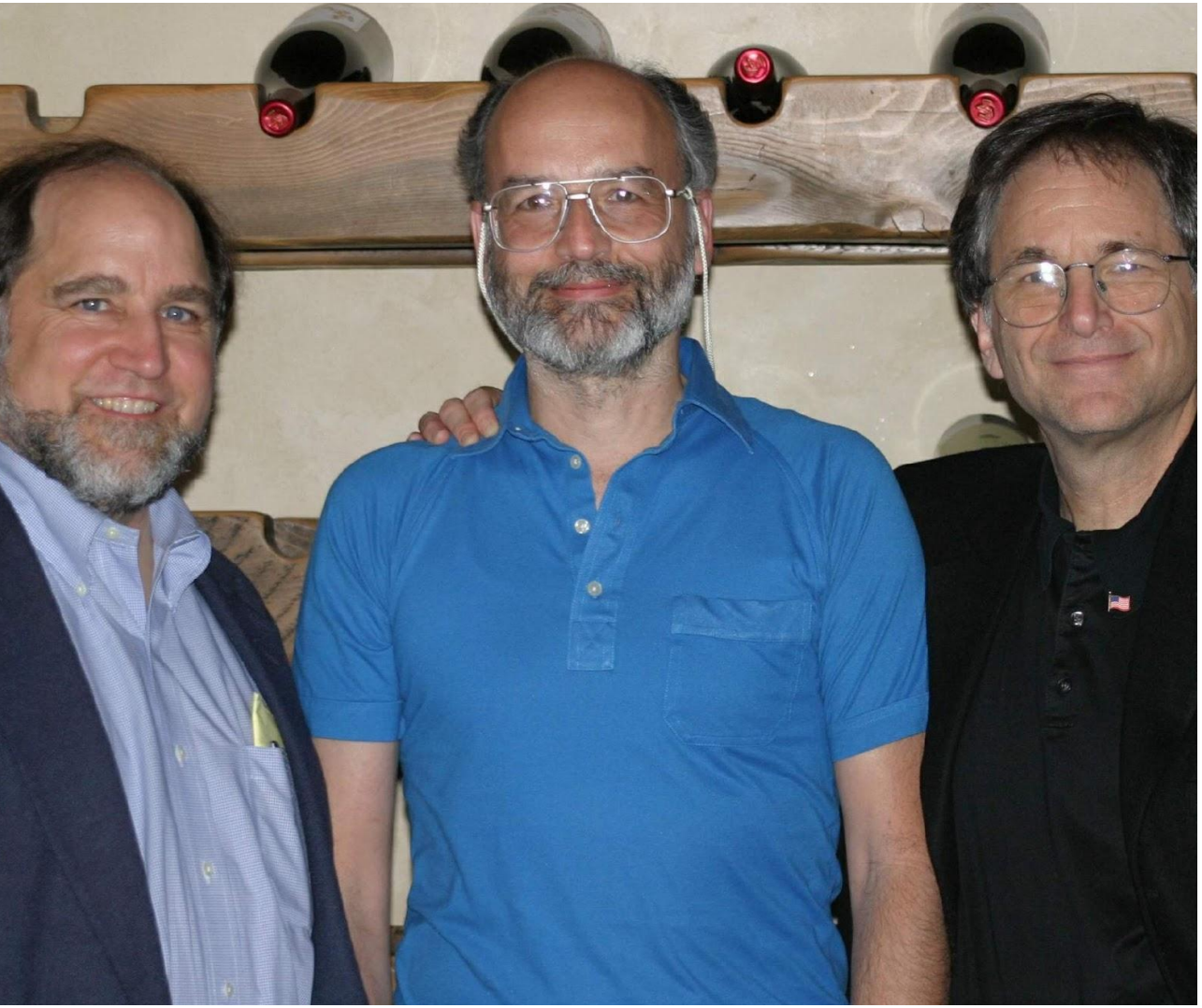
Ensure that unsigned integer operations

Do not call system() if you do not need a command processor

Do not subtract or compare pointers that do not wrap

Use the readlink() function properly

Image: https://en.wikipedia.org/wiki/Fred_Rogers



Ron Rivest, Adi Shamir, Len Adleman

DO YOU TRUST SECURE CRYPTO ALGORITHMS?

$$\forall m_0, m_1 \in M. \text{where} |m_0| = |m_1|$$

$$\forall c \in C.$$

$$\Pr\left[E(k, m_0) = c\right] = \Pr\left[E(k, m_1) = c\right.$$

Implementations may still leak

```
message_t decrypt(ciphertext_t c, key_t k){

  if(k == 1)
    return decrypt(m) // Takes time 1
  if(k == 2)
    return decrypt(m) // Takes time 2
  if(k == 3)
    return decrypt(m) // Takes time 3

}
```

Image: https://imgflip.com/i/52b3g8

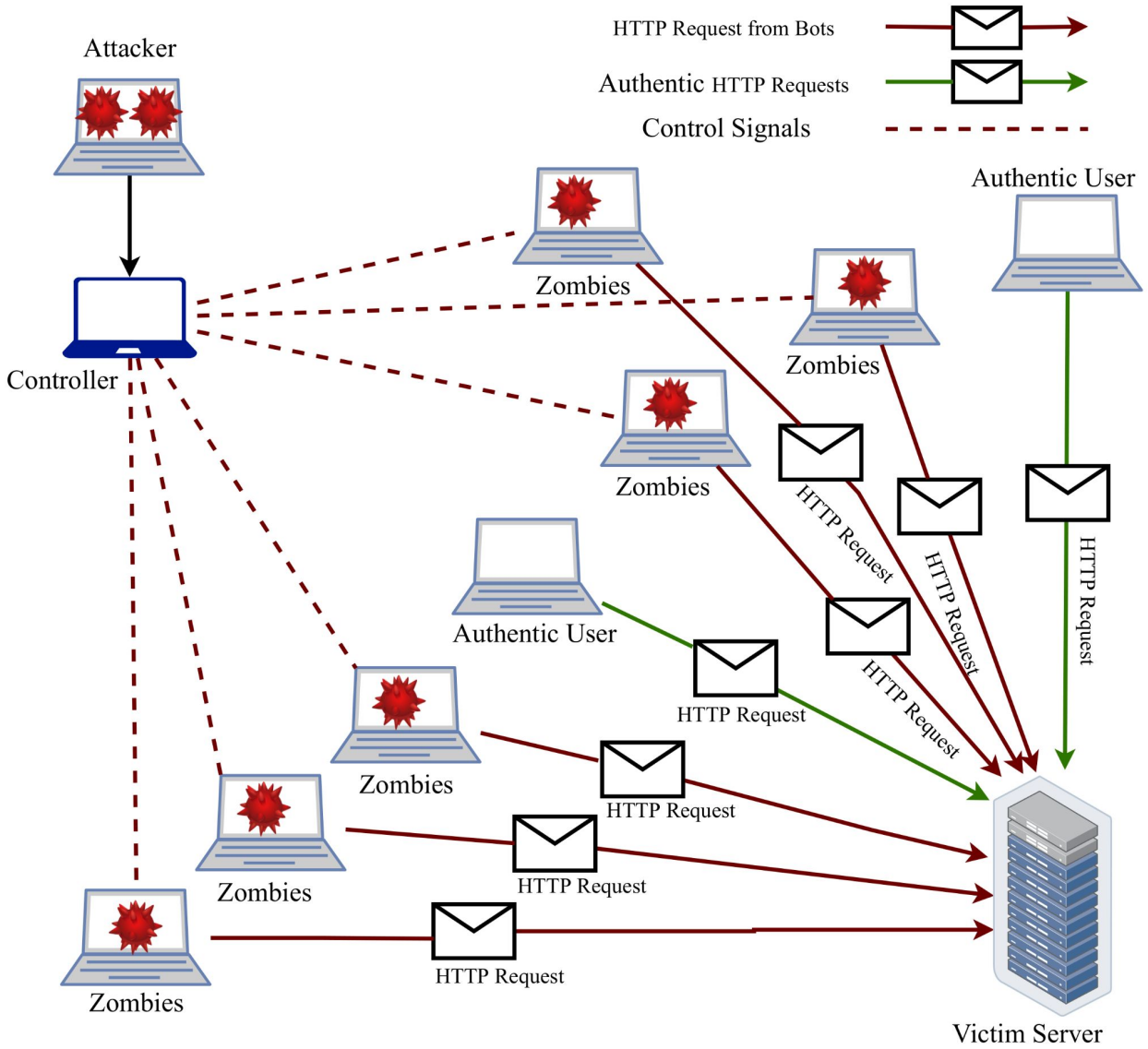
NETWORKED SYSTEMS

- Software has same security concerns
- Protocols play a larger part
- New, interesting security properties desired

HUMAN INTERACTION

Unusable systems become insecure

Intermission: Denial of Service Attacks



COURSE

THIS COURSE

The four corners of security and their foundations

THE ATTACKER

The defining characteristic of cybersecurity is the attacker:

- Smart
- Adaptive
- Asymmetric advantage

Level 1

FUNDAMENTALS

1. Threat modeling
2. Trusted computing base
3. Design principles for authorization, authentication, and audit

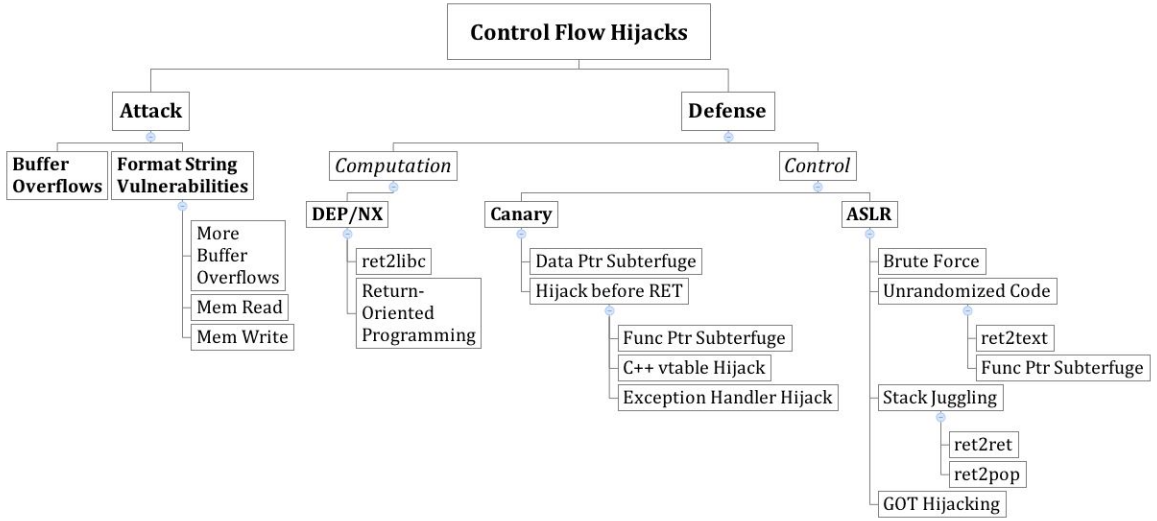
Level 2

SOFTWARE SECURITY

1. CVE vs CWE
2. Recognize vulnerabilities
3. Exploit vulnerabilities
4. Design mitigation
5. Circumvent mitigation
6. Understand static and dynamic analysis

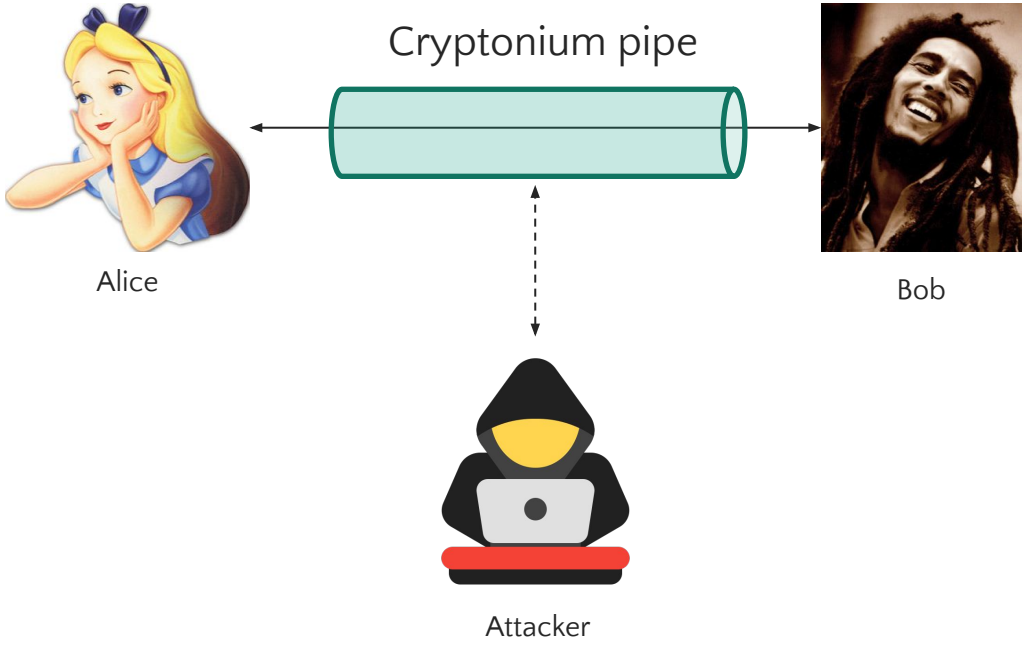
Level 2

BINARY EXPLOITATION



Level 3

CRYPTOGRAPHY



Level 3

CRYPTOGRAPHY

Goals: Privacy, authenticity, integrity

Concepts: [Pseudo-]Randomness, Symmetric/Asymmetric key, Encrypt, Hash, Sign, MAC, Forgery, Semantic Security

Applications: TLS, Private Information Retrieval, Blockchain

Level 4

NETWORK & WEB

1. The Gold Standard: AUthorization, AUthentication, AUdit
2. Exploit vulnerabilities
3. Design mitigation
4. Circumvent mitigation
5. Understand static and dynamic analysis

Level 5

HUMANS

1. Usable security
2. Privacy
3. Policy

One perspective

Charlie Kaufman, Radia Perlman, Mike Speciner

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations.
(They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)"

ETHICS AND YOUR RIGHTS

Understanding Security is like a Superpower

DON’T BREAK THE LAW

You need explicit permission to check the security of a system.

You are responsible for your actions.

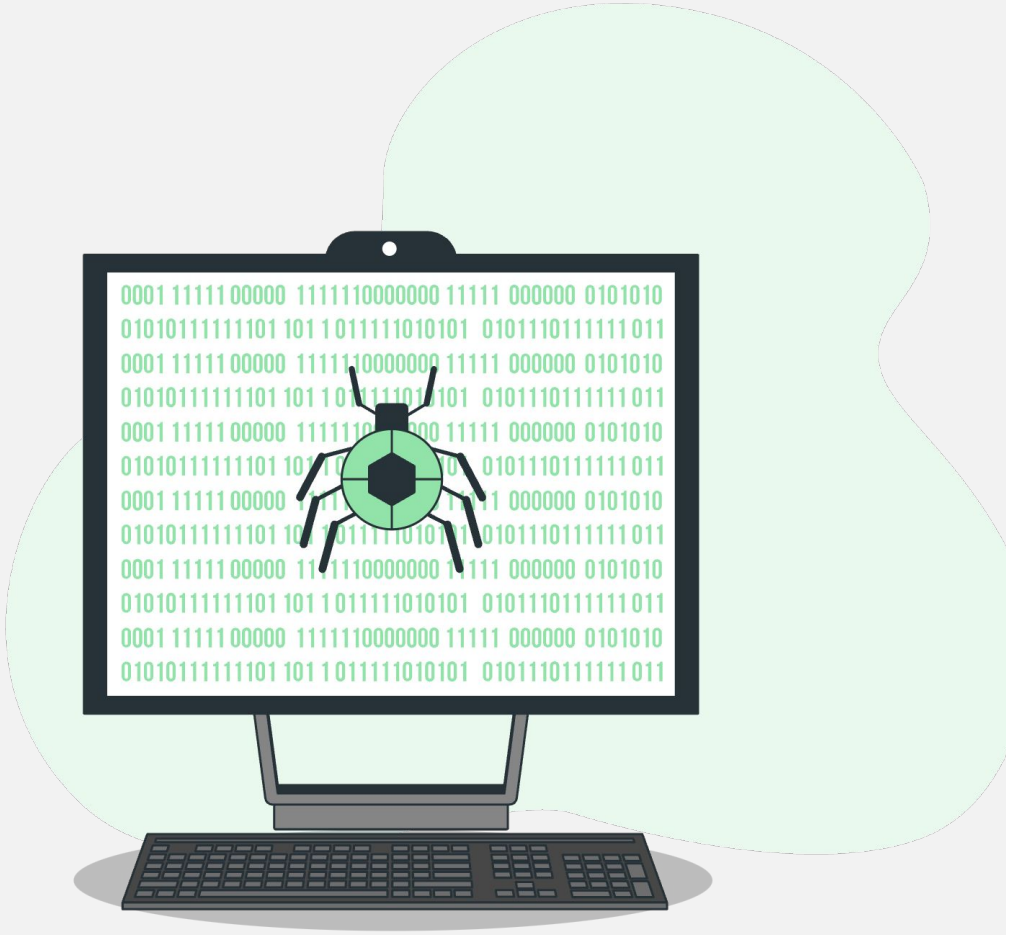


Image: storyset.com

SAFE HARBOR & BUG BOUNTIES

Safe harbor: A safe harbor is a legal provision in a statute or regulation that provides protection from a legal liability or other penalty when certain conditions are met.

Bug bounty: Provide a legal safe harbor under the terms of the bug bounty program.

Example: hackerone.com

What is Fair Game?

- All homeworks and exam questions will be in a controlled environment where you will be able to apply techniques you learn.

- Attacking homework infrastructure (or course staff) is NOT fair game and will result in a grade of exactly 0.
  - If you do discover a hole (by accident), practice coordinated vulnerability disclosure.

Our First Exploit!

Η Εργασία #0 μόλις ανέβηκε

Προθεσμία: Τετάρτη 27 Μαρτίου, 23:59

Εργασία #0

Ευχαριστώ και καλή μέρα εύχομαι!

Let's start hacking!