# Introduction

**CS-576 Systems Security**

Instructor: Georgios Portokalidis

Spring 2018

# Overview

General information

A (very short) introduction to systems security

# Overview

## General information

A (very short) introduction to systems security

# Information About the Course

All info, including syllabus, under

https://www.portokalidis.net/cs576.html

Lecture: Wednesday 6:15pm-8:45pm

Lab: Thursdays 4:00pm-4:50pm

- Make sure you are enrolled

Office hours: Mondays 3-5pm

# Communication

Communication and discussion over Piazza:
https://piazza.com/stevens/spring2018/cs576/

Go to link and enroll

- **Use your Stevens email!**

**Do not** use canvas messaging to communicate

Use Piazza for most questions

- Sometimes your classmates can help you faster than the instructor

# Textbook(s)

No textbook is mandatory

Most material is in the slides

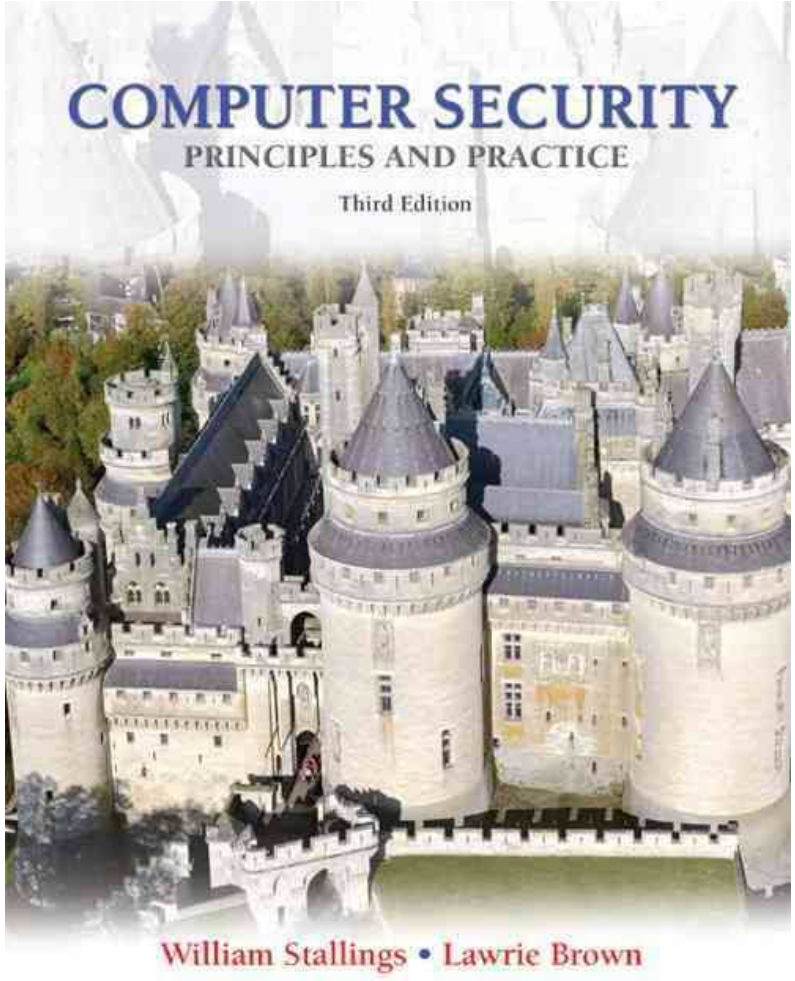
- Online articles
- Research papers
- The slides themselves

Some textbooks that will be useful are …

# Computer Security: Principles and Practice

Computer Security: Principles and Practice

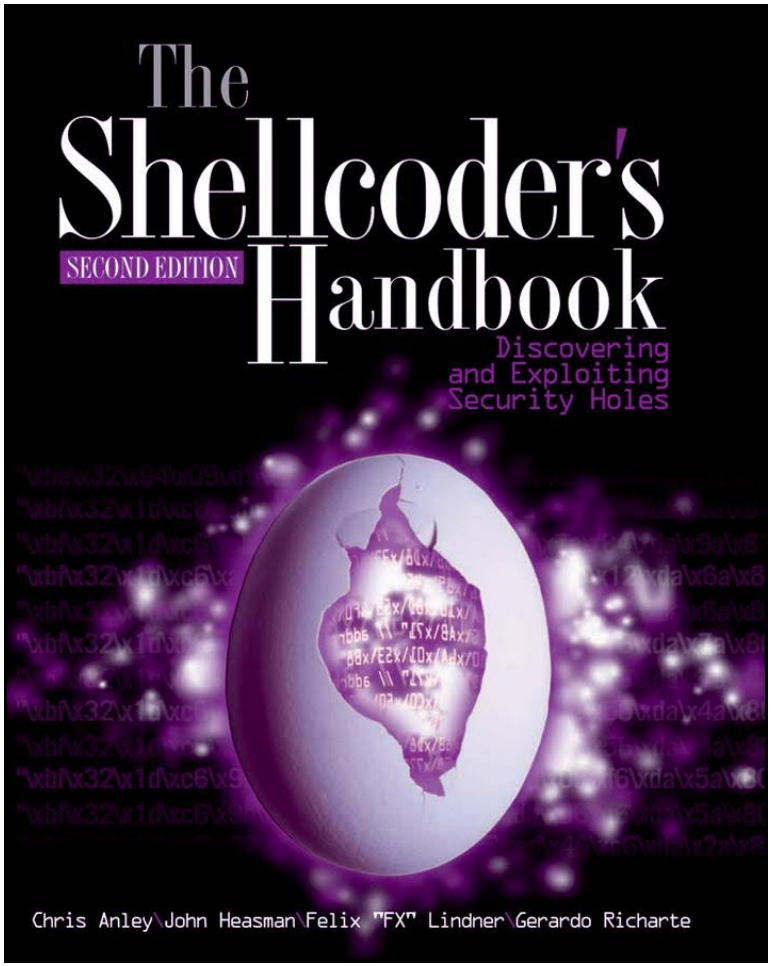
- By William Stallings and Laurie Brown
- **Third edition**



# The Shellcoder's Handbook: Discovering and Exploiting Security Holes

The Shellcoder's Handbook: Discovering and Exploiting Security Holes

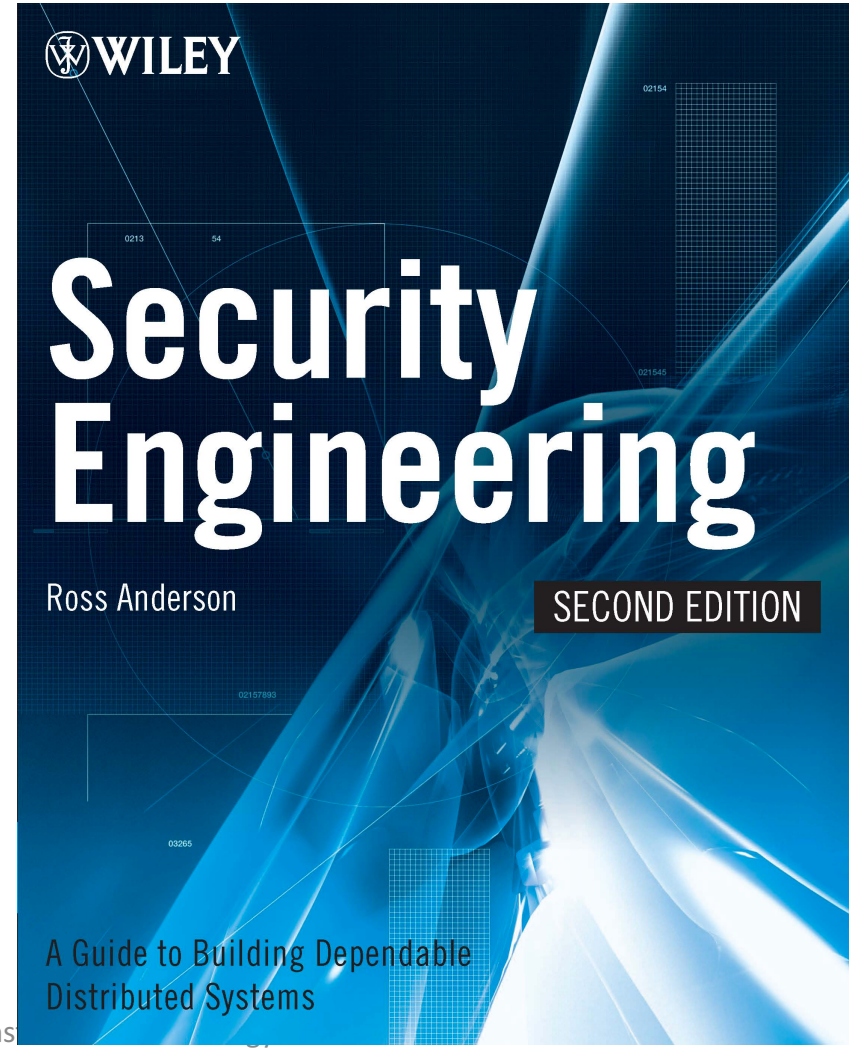
- By Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte



# Security Engineering

**Security Engineering** http://www.cl.cam.ac.uk/~rja14/book.html

- By Ross Anderson



# Grade Breakdown

Exam I (20%)

Exam II (20%)

Lab participation (10%)

Software Project (50%)

# Homework

There will be 2-3 individual take-home assignments

For most assignments you will have two weeks to submit

- Rarely three weeks
- You are given plenty of time because these assignments can be challenging!
- Starting late is a guaranteed way to fail

# Homework Timeliness

2 grace days for the semester

- Used automatically when you submit late
- Covers scheduling crunch, out-of-town trips, illnesses, minor setbacks

Once grace day(s) used up, get penalized **15% per day**

No submissions will be accepted later than **3 days after due date**

# Exams

Relatively short (<=1hour)

Focused on understanding. May include multiple choice and short-answer questions, and code understanding questions

Online or on paper, but students must be in-class

**Midterm**


**Final**

# Project

## Goals

- **Develop** a system that goes beyond toy applications
- Work in a **team**
- **Evaluate** and **document** a complex software system

## Tasks

- Team up with 3-5 classmates
- Research and propose project appropriate for the size of the group
- Develop system proposed
- Write a short and report and present the project in class

## Topics

- Teams can propose anything relevant to the course
- The instructor can propose certain fun directions

# Lab Work

Demonstration of tools and techniques

Students will participate in exercises

- Bring your laptops and make sure they are charged

Most of the assignments and lab will be done on the Linux-lab

- If you do not have an account, you'll need to get one
- https://www.srcit.stevens.edu/wiki/index.php/Linux_Lab

# Cheating: Description

What is cheating?

- Sharing code: by copying, retyping, **looking at**, or supplying a file
- Describing: verbal description of code from one person to another
- Coaching: helping your friend to write a lab, line by line
- Searching the Web for solutions
- Copying code from a previous course or online solution

What is NOT cheating?

- Explaining how to use systems or tools
- Helping others with high-level design issues

Ignorance is not an excuse

# Cheating: Consequences

Penalty for cheating:

- You will be reported to the Dean
- Penalties may include suspension  and expulsion and deduction of points

Detection of cheating:

- We have sophisticated tools for detecting code plagiarism

Don’t do it!

- Start early
- Ask us for help when you get stuck
  - Assuming you start early

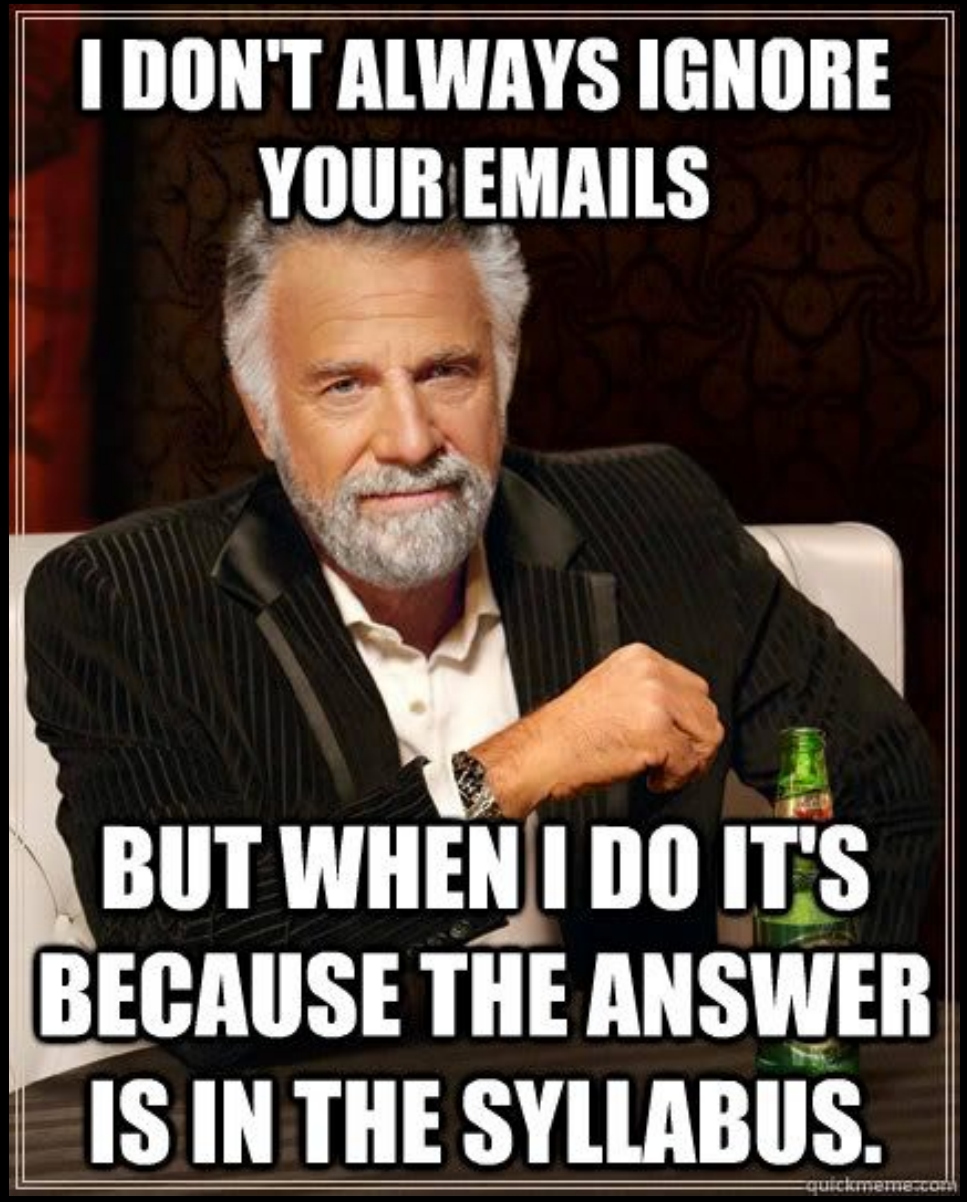
# Other Rules and Advice

Don’t use your laptops in lectures, they **will** distract you

Electronic communications: *forbidden*

- No email, instant messaging, cell phone calls, etc

No recordings of ANY KIND


I DON'T ALWAYS IGNORE YOUR EMAILS
BUT WHEN I DO IT'S BECAUSE THE ANSWER IS IN THE SYLLABUS.
quickmeme.com

# Any questions this far?

# Overview

General information

**A (very short) introduction to systems security**

Systems Security

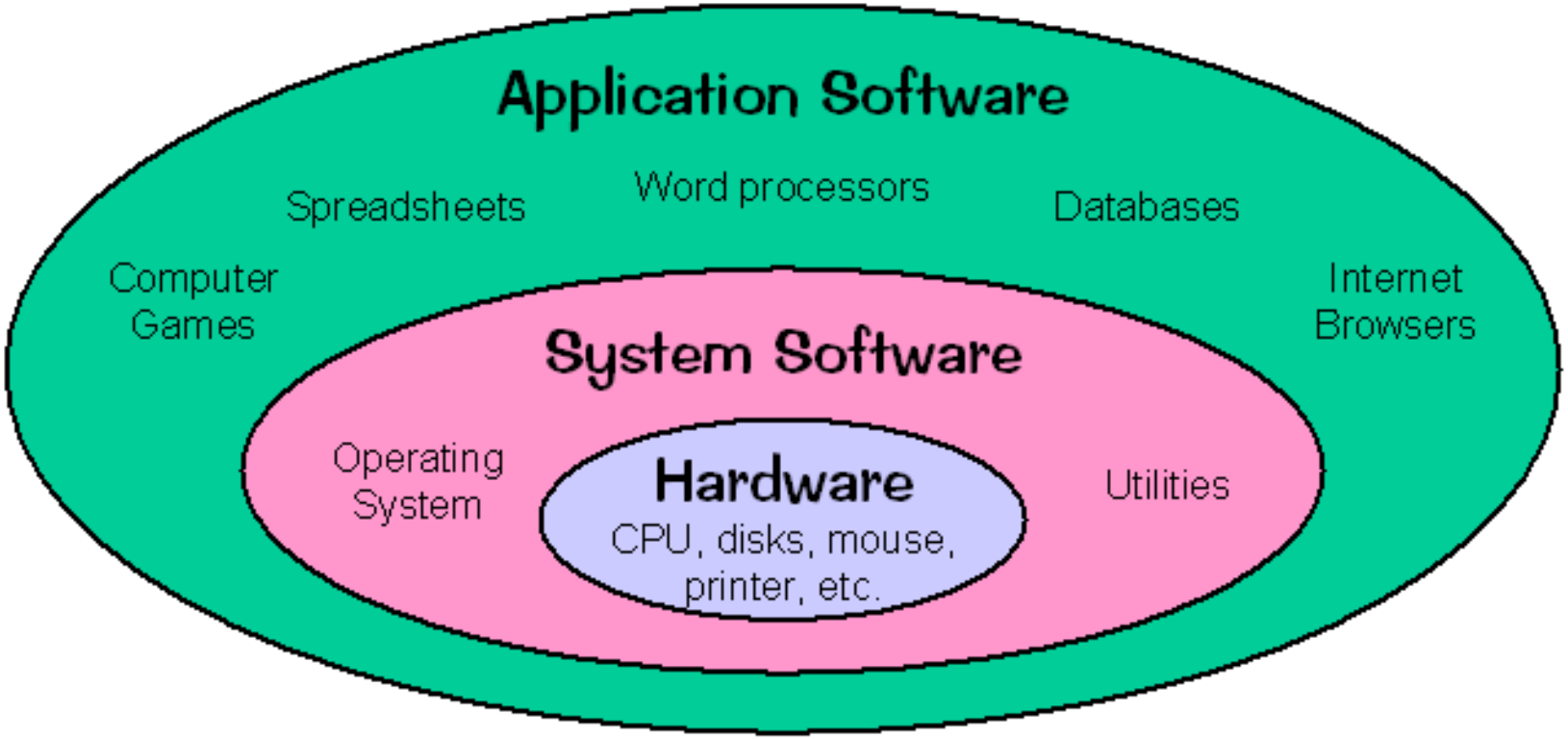
!=

Computer Security

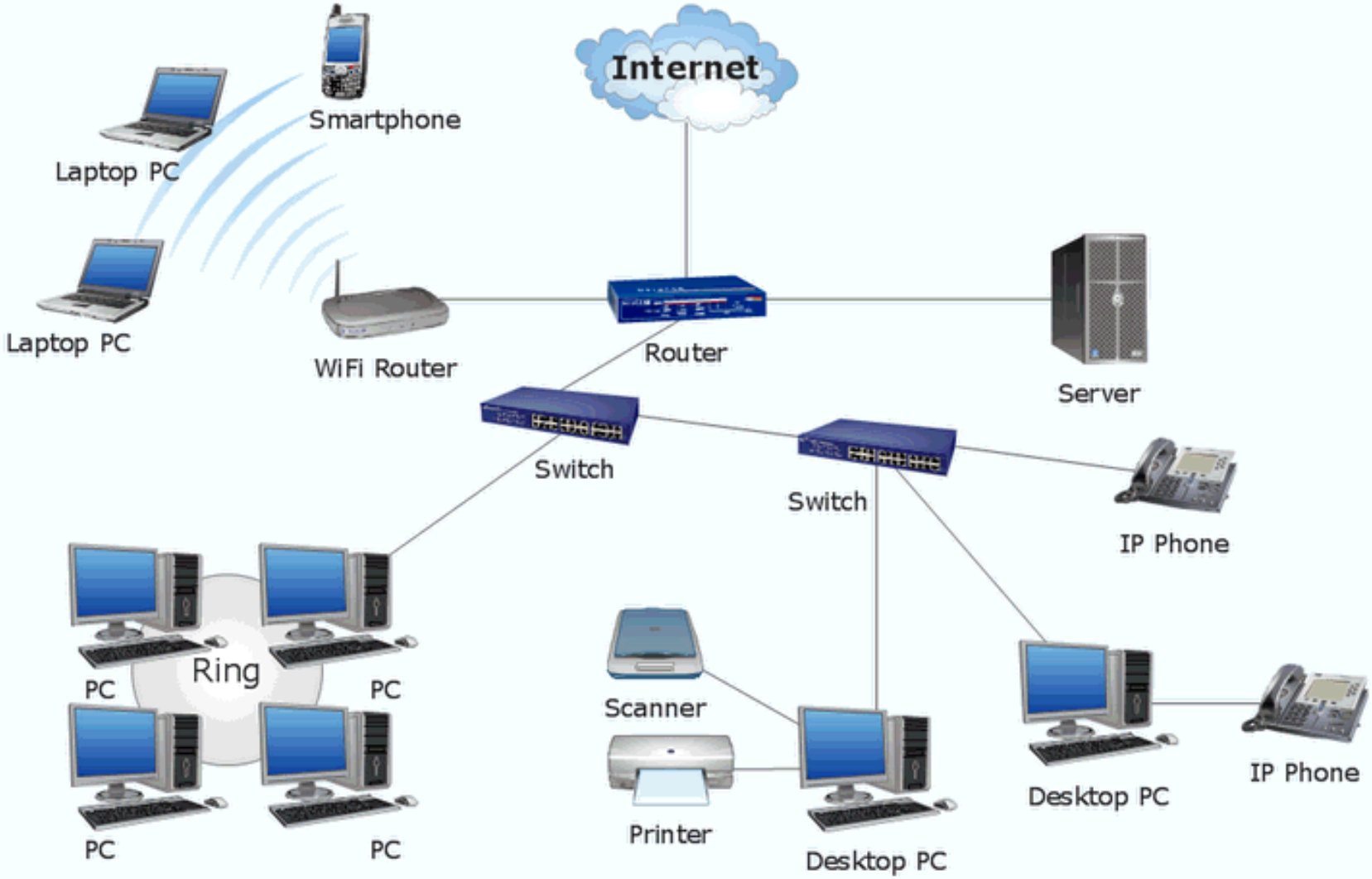
Software Systems

Software Systems

Operating Systems




# Computer Systems




# (Inter-)Networked Systems

# Existing Systems

It is important to understand how a system works

- What is the execution environment
- What are the programming languages used
- How do applications interact with the OS
- How does the OS interact with the HW
- How do applications interact with the HW
- How do applications interact with other applications
  - Locally
  - Over the network

…and how this affects **security**

Not just understanding abstractions, but also **mechanisms**

# New Systems

What are the right principles to design and develop **secure** systems

# Security == The CIA Triad

Confidentiality

- Data confidentiality
- Privacy

Integrity

- Data integrity
- System integrity

Availability

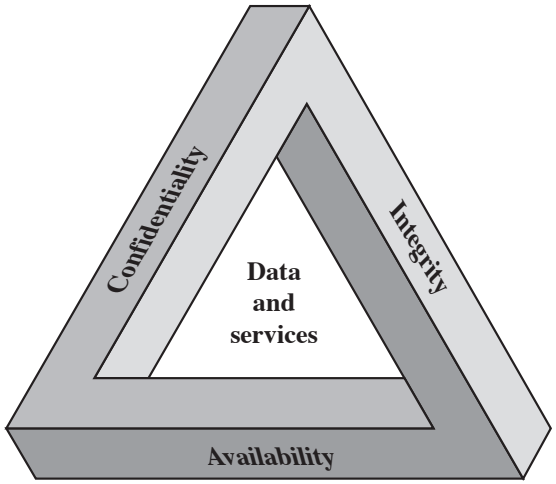



**Figure 1.1 The Security Requirements Triad**

What are the potential attack points?

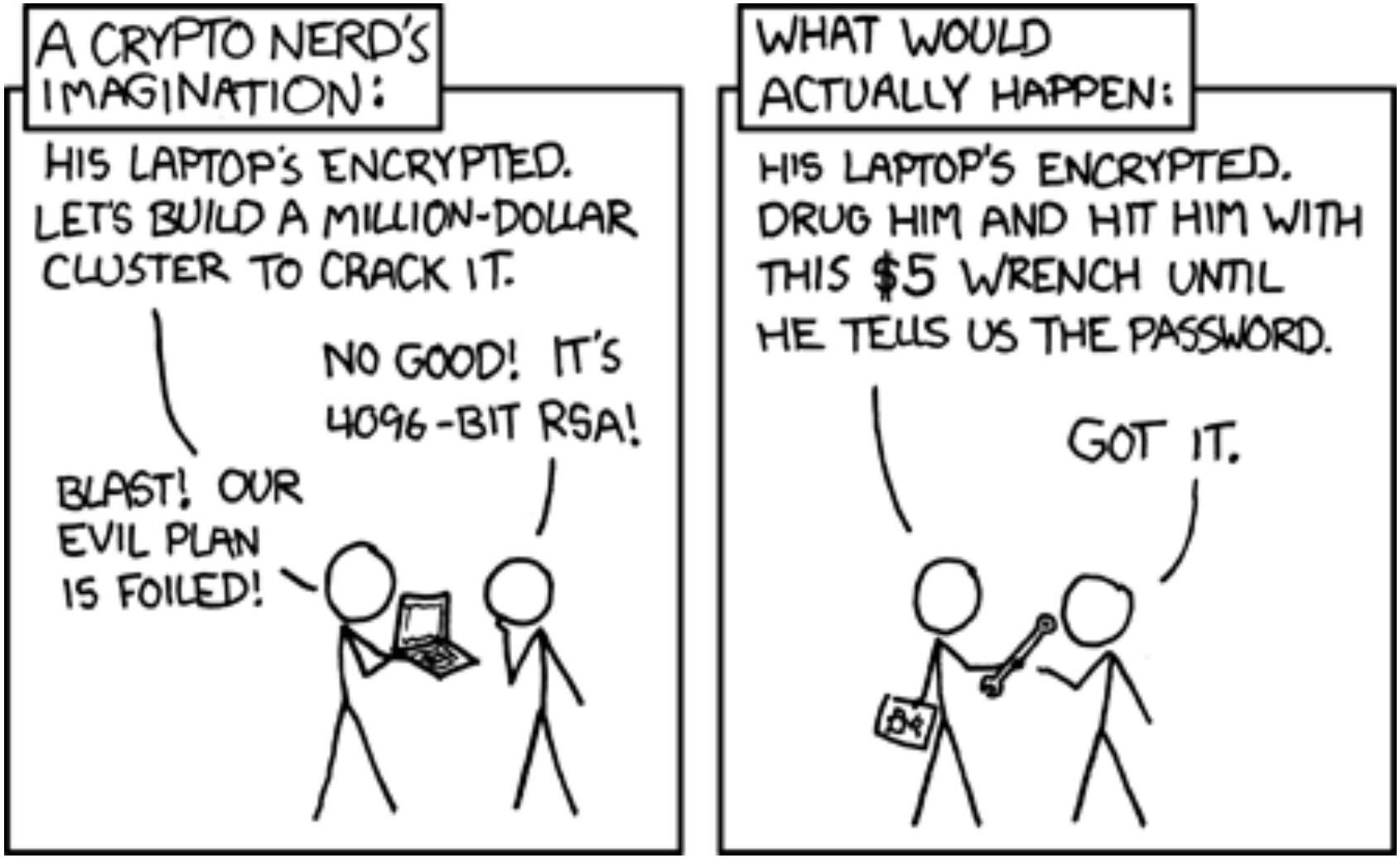
What security feature would hurt usability?

What is the weakest point?

Can you think of security measures that can be added on the already built systems?

Asymmetry of tasks for defenders and attackers.

https://xkcd.com/538/




# Different approach from crypto

# Is it important?

Gartner Says 8.4 Billion C

Secure | https://www.gartner.com/newsroom/id/3598917

Egham, U.K., February 7, 2017

View All Press Releases

# Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016

***Consumer Applications to Represent 63 Percent of Total IoT Applications in 2017***

Gartner, Inc. forecasts that 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020. Total spending on endpoints and services will reach almost $2 trillion in 2017.

Regionally, Greater China, North America and Western Europe are driving the use of connected things and the three regions together will represent 67 percent of the overall Internet of Things (IoT) installed base in 2017.

**Consumer Applications to Represent 63 Percent of Total IoT Applications in 2017**

The consumer segment is the largest user of connected things with 5.2 billion units in 2017, which represents 63 percent of the overall number of applications in use (see Table 1). Businesses are on pace to employ 3.1 billion connected things in 2017. "Aside from automotive systems, the applications that will be most in use by consumers will be smart TVs and digital set-top boxes, while smart electric meters and commercial security cameras will be most in use

BUSINESS DAY

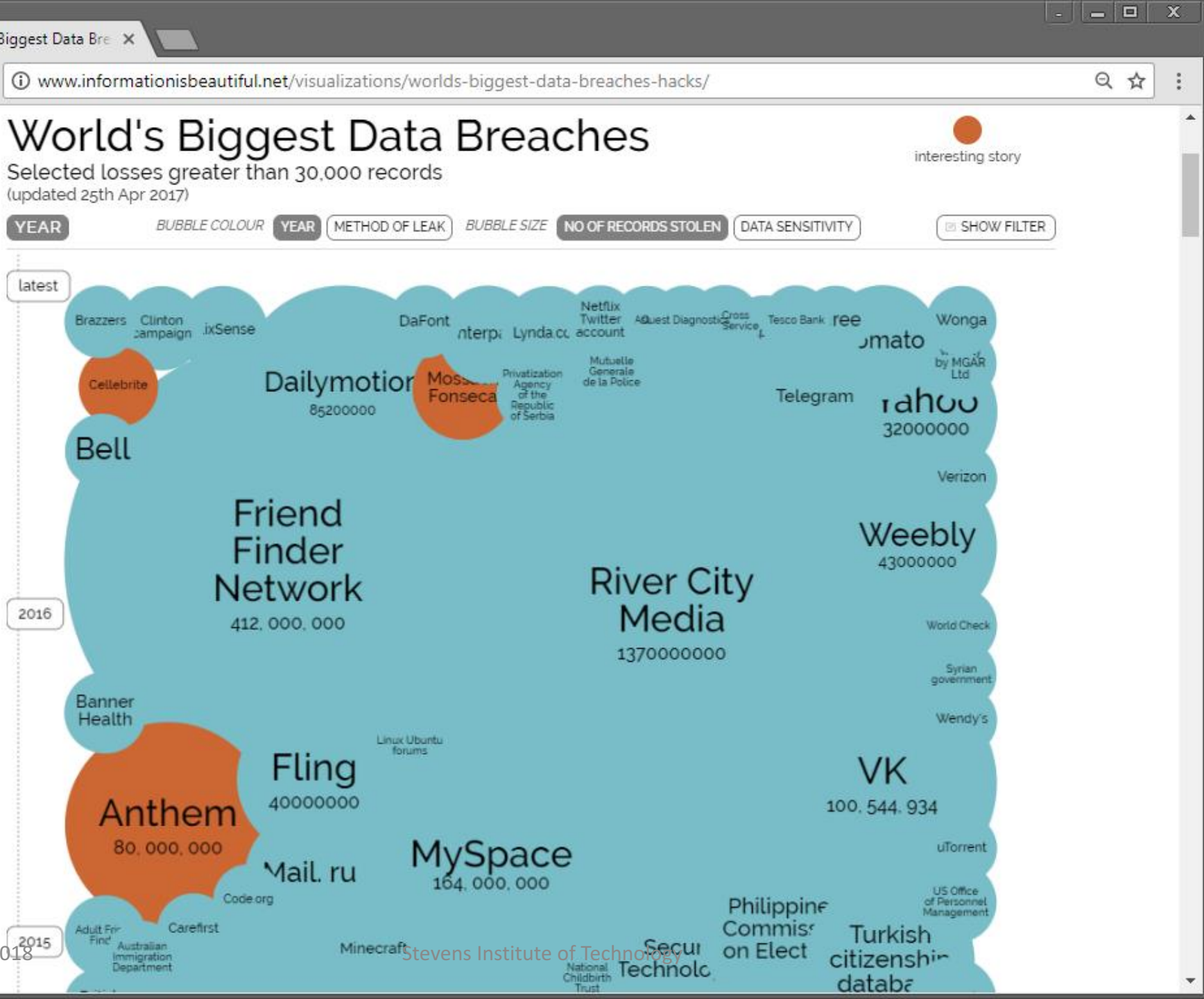
# Millions of Anthem Customers Targeted in Cyberattack

By REED ABELSON and MATTHEW GOLDSTEIN FEB. 5, 2015


Outside the Anthem facility in Indianapolis. Anthem said it detected a data breach on Jan. 29, and that it was working with the Federal Bureau of Investigation. Aaron P. Bernstein/Getty Images



Anthem, one of the nation's largest health insurers, said late


World's Biggest Data Bre
www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 25th Apr 2017)
interesting story
YEAR
BUBBLE COLOUR
YEAR
METHOD OF LEAK
BUBBLE SIZE
NO OF RECORDS STOLEN
DATA SENSITIVITY
SHOW FILTER
latest
2016
2015
Brazzers
Clinton campaign
ixSense
DaFont
Netflix Twitter account
Tesco Bank
Wonga
Cellebrite
Dailymotion
85200000
Mossack Fonseca
Privatization Agency of the Republic of Serbia
Mutuelle Generale de la Police
Telegram
Yahoo
32000000
Bell
Verizon
Friend Finder Network
412, 000, 000
River City Media
1370000000
Weebly
43000000
World Check
Syrian government
Banner Health
Wendy's
Linux Ubuntu forums
Fling
40000000
VK
100, 544, 934
Anthem
80, 000, 000
uTorrent
Mail. ru
MySpace
164, 000, 000
Code.org
US Office of Personnel Management
Carefirst
Australian Immigration Department
Minecraft
National Childbirth Trust
Philippine Commission on Elect
Turkish citizenship

# Hacking of Government Computers Exposed 21.5 Million People

By JULIE HIRSCHFELD DAVIS JULY 9, 2015


Katherine Archuleta, director of the Office of Personnel Management, right, at hearing before the House Oversight and Government Reform Committee last month. Mark Wilson/Getty Images

Email

WASHINGTON — The Obama administration on Thursday revealed that 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than

# Experts working with Homeland Security hacked into Boeing 757



There's some unsettling news about one of America's most widely-used jetliners.

In a test, experts working with Homeland Security hacked into a Boeing 757. The team of researchers needed only two days in September 2016 to remotely hack into a 757 parked at the airport in Atlantic City, New Jersey.

Speaking at a conference this week, Robert Hickey of the Department of Homeland Security said his team used "typical stuff that could get through security" and hacked into the aircraft systems using "radio frequency communications."

"The 757 hasn't been in production since 2004, but the aging workhorse is still flown by major airlines like United, Delta and American," said Mark Rosenker, the former chair of the National Transportation Safety Board.

President Trump's personal jet is a 757. So is the plane Vice President Pence often uses -- including on his recent trip to Texas.

# An Unprecedented Look at Stuxnet, the World's First Digital Weapon

BY KIM ZETTER 11.03.14 | 6:30 AM | PERMALINK



Ukrainian blackout caused

www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company

theguardian

Cybercrime

# Ukrainian blackout caused by hackers that attacked media company, researchers say

Power company suffered a major attack that led to blackouts across western Ukraine, after an attack on a Ukrainian media company


Alex Hern

@alexhern


Thursday 7 January 2016 08.20 EST

Shares 150 Comments 31

Save for later

Smokestacks in Dniprodzershynsk, Ukraine. Photograph: John Mcconnico/AP

A power blackout in Ukraine over Christmas and a destructive cyberattack on a major Ukrainian media company were caused by the same malware from the same major hacking group, known as Sandworm, according to security researchers at Symantec.

# Government Hackers Caught Using Unprecedented iPhone Spy Tool

WRITTEN BY LORENZO FRANCESCHI-BICCHIERAI

August 25, 2016 // 01:05 PM EST

On the morning of August 10, Ahmed Mansoor, a 46-year-old human rights activist from the United Arab Emirates, received a strange text message from a number he did not recognize on his iPhone.

"New secrets about torture of Emiratis in state prisons," read the tantalizing message, which came accompanied by a link.

Mansoor, who had already been the victim of government hackers using commercial spyware products from FinFisher and Hacking Team, was suspicious and didn't click on the link. Instead, he sent the message to Bill Marczak, a researcher at Citizen Lab, a digital rights watchdog at the University of Toronto's Munk School of Global Affairs.

Bits



SECURITY

# Hackers Exploit 'Flash' Vulnerability in Yahoo Ads

By DINO GRANDONI AUGUST 3, 2015 9:14 PM 51 Comments



For seven days, hackers used Yahoo's ad network to send malicious bits of code to computers that visit Yahoo's collection of heavily trafficked websites, the company said on Monday.

The attack, which started on July 28, was the latest in a string that have exploited Internet advertising networks, which are designed to reach millions of people online. It also highlighted growing anxiety over a much-used graphics program called Adobe Flash, which has a history of security issues that have irked developers at Silicon Valley companies.

"Right now, the bad guys are really enjoying this," said Jérôme Segura, a security researcher at Malwarebytes, the security company that uncovered the attack. "Flash for them was a godsend."

The scheme, which Yahoo shut down on Monday, worked like this: A group of hackers bought ads across the Internet giant's sports, news and finance sites. When a computer — in this case, one running Windows — visited a Yahoo site, it downloaded malware code.

PREVIOUS POST
What Yahoo Paid for Polyvore: More Than $200 Million

NEXT POST
Daily Report: The GIF Start-Ups Fostering a Visual Language on Mobile

Visit the **Technology section** for complete coverage of the industry. »

MOST VIEWED

1. Tech's 'Frightful 5' Will Dominate Digital Life for Foreseeable Future
2. Uber's No-Holds-Barred Expansion Strategy Fizzles in Germany
3. Fans Demand Details After Death of a 13-Year-Old YouTube Star
4. At C.D.C., a Debate Behind Recommendations on Cellphone Risk
5. How Larry Page's Obsessions Became Google's Business

LATEST FROM BITS

Drone Lobbying Heats Up on Capitol Hill

Daily Report: Airbnb Urges Mayors to 'Please Tax Us'

US police force pay bitcoi

www.theguardian.com/technology/2013/nov/21/us-police-force-pay-bitcoin-ransom-in-cryptolocker-malware-scam

sign in subscribe search jobs US edition

theguardian
Winner of the Pulitzer prize

US world opinion sports soccer tech arts lifestyle fashion business money travel environment all

home › tech

Computing

# US police force pay bitcoin ransom in Cryptolocker malware scam

Unprepared officials blindsided by sophisticated virus call experience 'an education'

The Netanyahu Disaster
By Jeffrey Goldberg

The Effects of Forgiveness
By Olga Khazan

Rural America's Silent Housing Crisis
By Gillian B. White

Introducing the Supertweet
By Ian Bogost

# Armed With Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation

REBECCA J. ROSEN | MAR 12 2013, 2:59 PM ET

*But the deeper aspects of your personality remain hard to detect.*

The Meltdown and Spectre vul

Secure https://www.popsci.com/meltdown-spectre-what-to-do

POPULAR SCIENCE

WANT MORE?

SCIENCE TECH DIY GOODS VIDEO ROLL THE DICE SUBSCRIBE

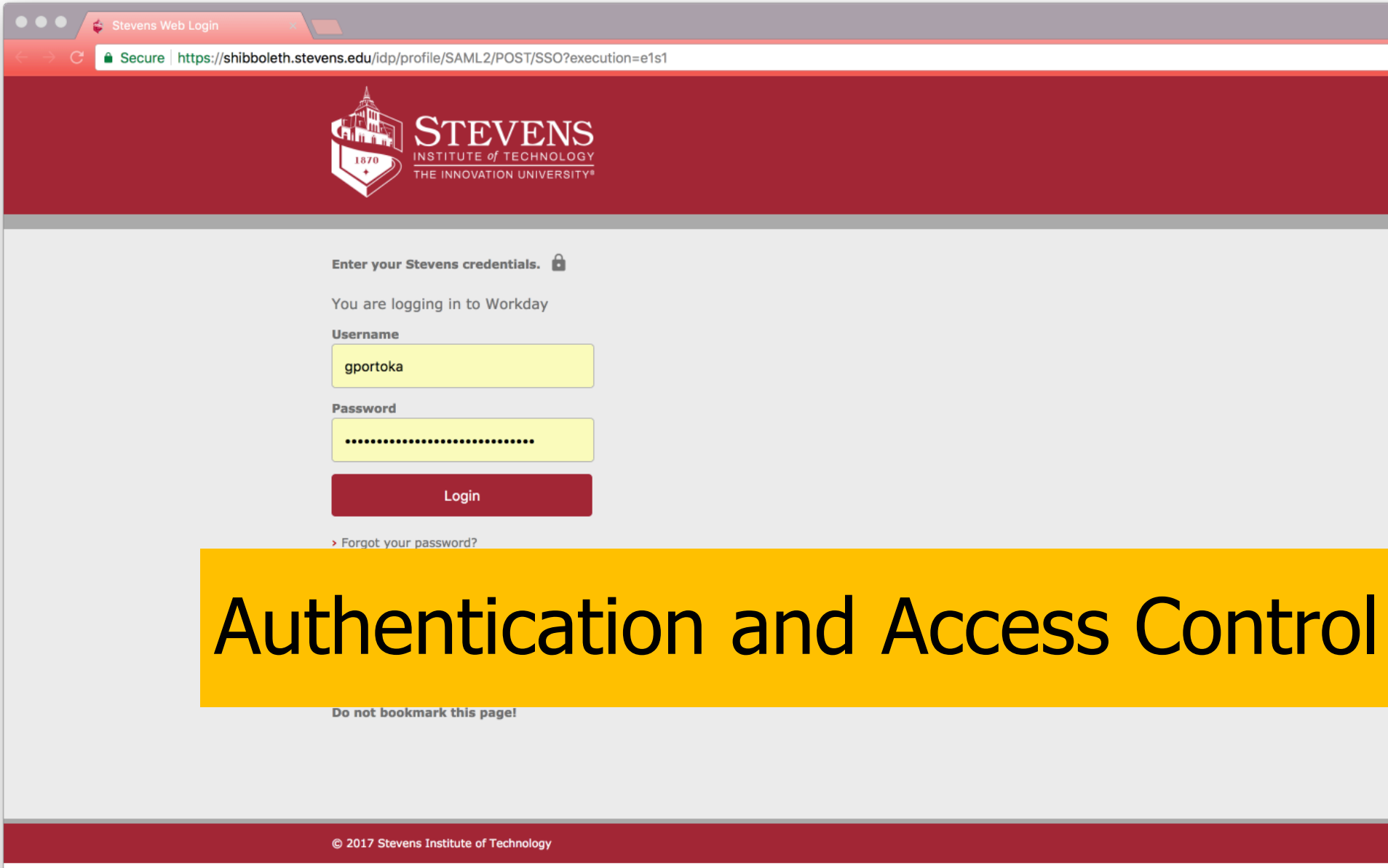
TECHNOLOGY

# The Meltdown and Spectre vulnerabilities affect nearly every computer. Here's what you need to know.

Understanding the two new scary silicon security issues.

*By Rob Verger* *January 12, 2018*

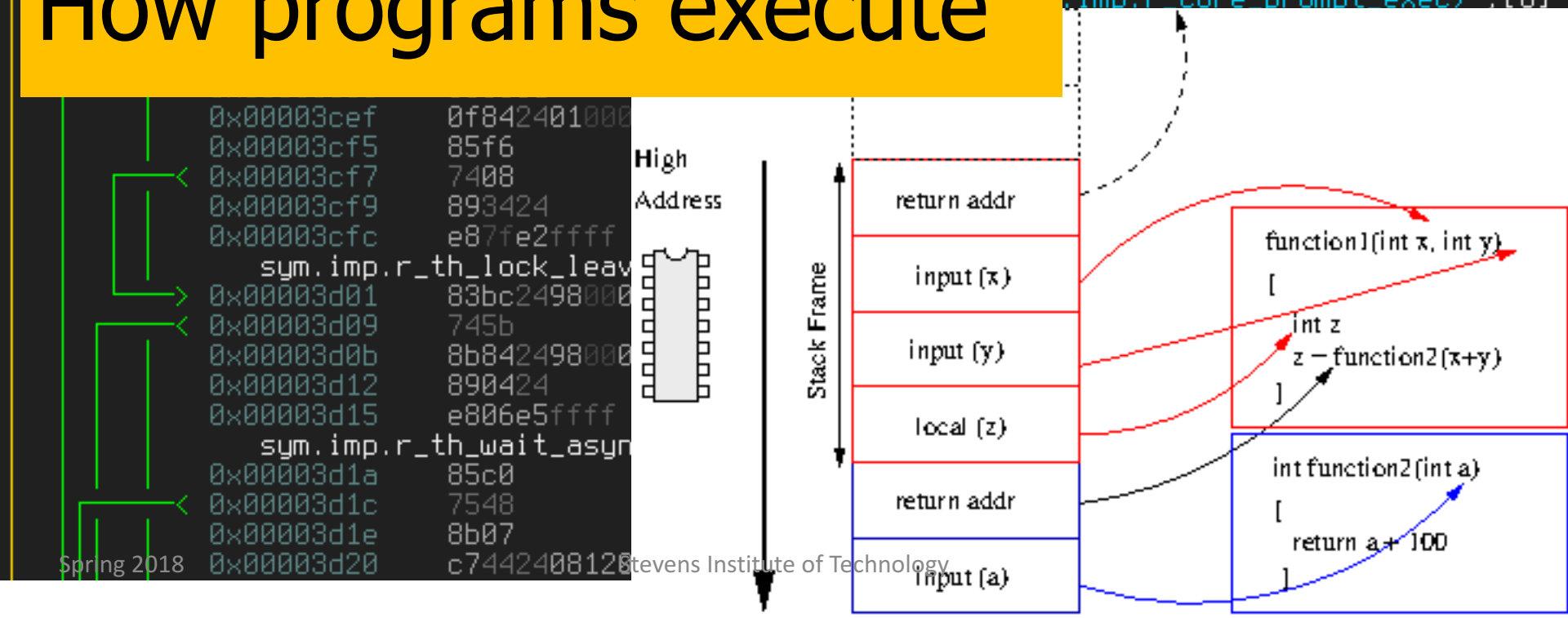
# Course Topics



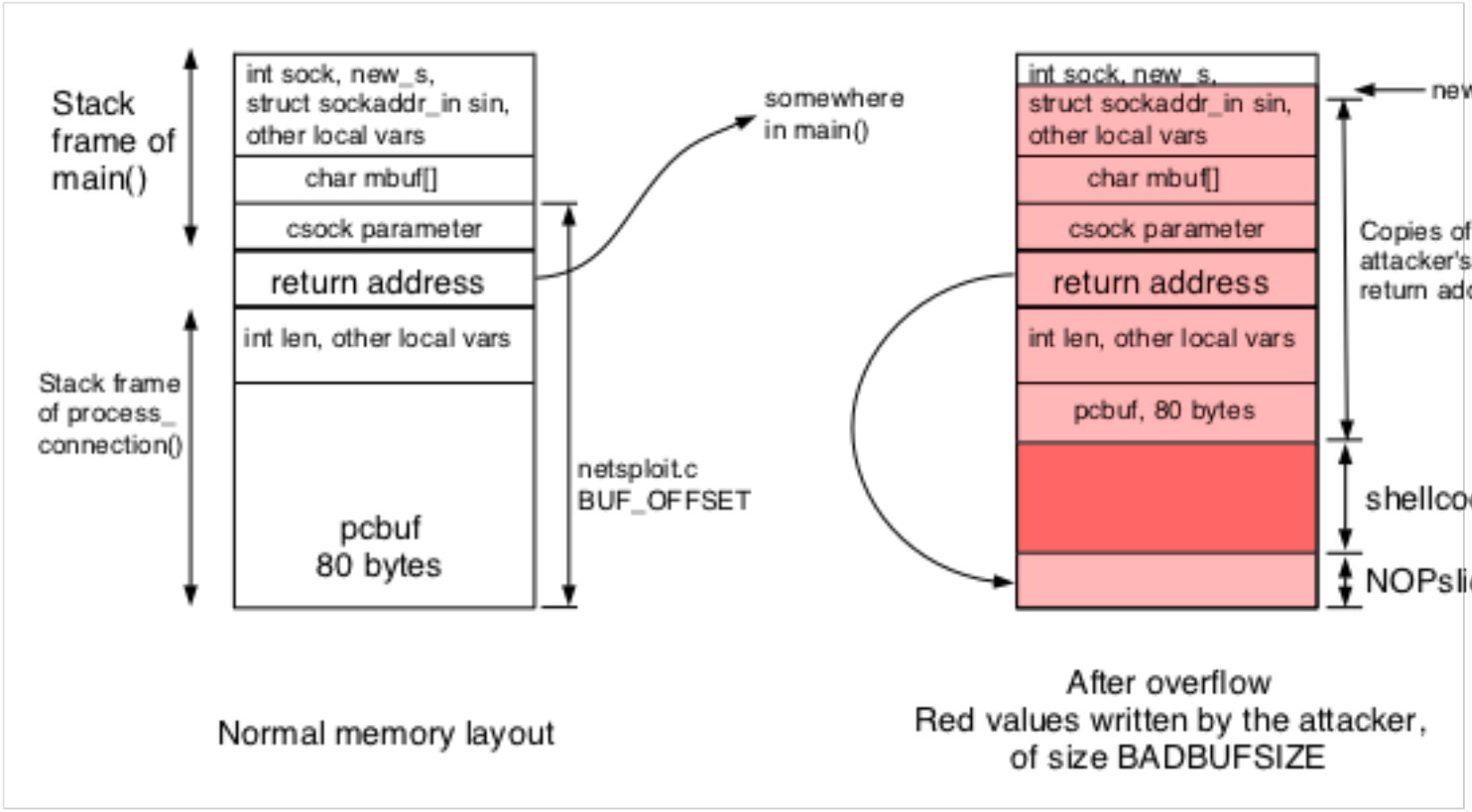

# Authentication and Access Control

# How programs execute

```
[0x00003c9c 255 /usr/bin/r2]> pd $r @ sym..L94+4869 # 0x3c9c
            0x00003c9c    e970efffff    jmp 0x100002c11 ; (fcn.00002390) ;[1]
            0x00003ca1    8bbba4010000  mov edi, [ebx+0x1a4]
            0x00003ca7    8b74247c      mov esi, [esp+0x7c]
            0x00003cab    8b842494000.  mov eax, [esp+0x94]
            0x00003cb2    c7442404000.  mov dword [esp+0x4], 0x0
            0x00003cba    890424        mov [esp], eax
            0x00003cbd    e81ee2ffff    call 0x100001ee0 ; (sym.imp.r_core_prompt) ;[2]
               sym.imp.r_core_prompt()
            0x00003cc2    85c0          test eax, eax
            0x00003cc4    0f8eaa000000  jle 0x3d74 ;[3]
            0x00003cca    85f6          test esi, esi
            0x00003ccc    7408          jz 0x3cd6 ;[4]
            0x00003cce    893424        mov [esp], esi
            0x00003cd1    e84ae4ffff    call 0x100002120 ; (sym.imp.r_th_lock_enter) ;[5]
               sym.imp.r_th_lock_enter()
```



# Memory corruptions bugs

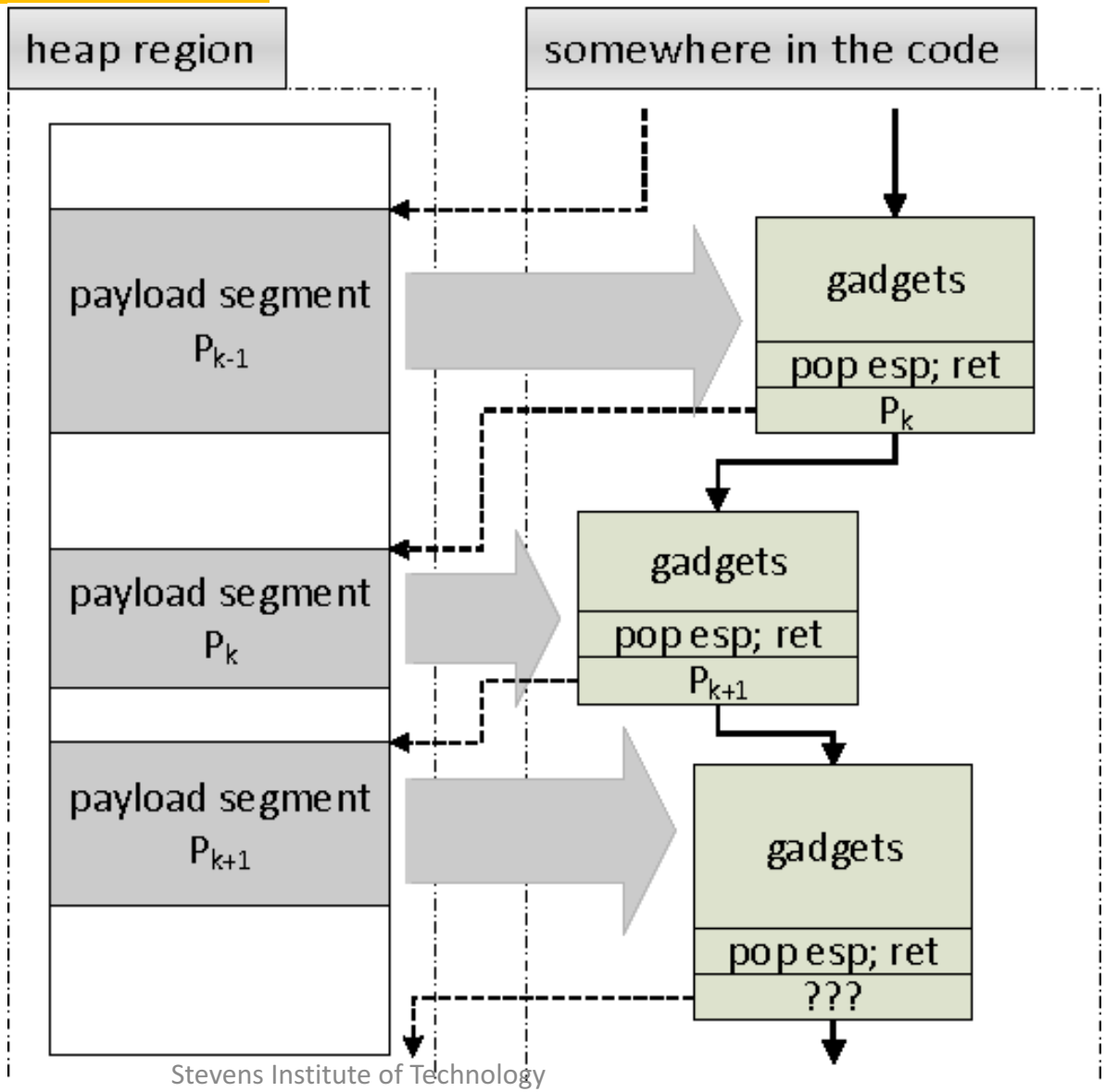


# Early software defenses

```
B+  0x40061b <main+37>      call   0x4004f0 <gets@plt>
  > 0x400620 <main+42>      lea    rax,[rbp-0x30]
    0x400624 <main+46>      mov    rdi,rax
    0x400627 <main+49>      call   0x4004b0 <puts@plt>
    0x40062c <main+54>      mov    eax,0x0
    0x400631 <main+59>      mov    rdx,QWORD PTR [rbp-0x8]
    0x400635 <main+63>      xor    rdx,QWORD PTR fs:0x28
    0x40063e <main+72>      je     0x400645 <main+79>
    0x400640 <main+74>      call   0x4004c0 <__stack_chk_fai
    0x400645 <main+79>      leave
    0x400646 <main+80>      ret
```

```
native process 113657 In:
(gdb) ni
0x0000000000400620 in mai
(gdb) )Undefined command:
(gdb) x/32x $rsp
0x7fffffffe3e0: 0xffffe508      0x00007fff      0x0040069d      0x00
0x7fffffffe3f0: 0x41414141      0x41414141      0x41414141      0x41
0x7fffffffe400: 0x41414141      0x41414141      0x41414141      0x41
0x7fffffffe410: 0x41414141      0x41414141      0xffffe460      0x00
0x7fffffffe420: 0x90909090      0x90909090      0x90909090      0x90
0x7fffffffe430: 0x90909090      0x90909090      0x90909090      0x90
0x7fffffffe440: 0x90909090      0x90909090      0x90909090      0x90
0x7fffffffe450: 0x90909090      0x90909090      0x90909090      0x90
(gdb)
```

# Modern Attacks



# Post-modern Attacks and Defenses

```
struct array {
 unsigned long length;
 unsigned char data[];
};
struct array *arr1 = ...;
unsigned long untrusted_offset_from_caller = ...;
if (untrusted_offset_from_caller < arr1->length) {
 unsigned char value = arr1->data[untrusted_offset_from_caller];
 ...
}
```

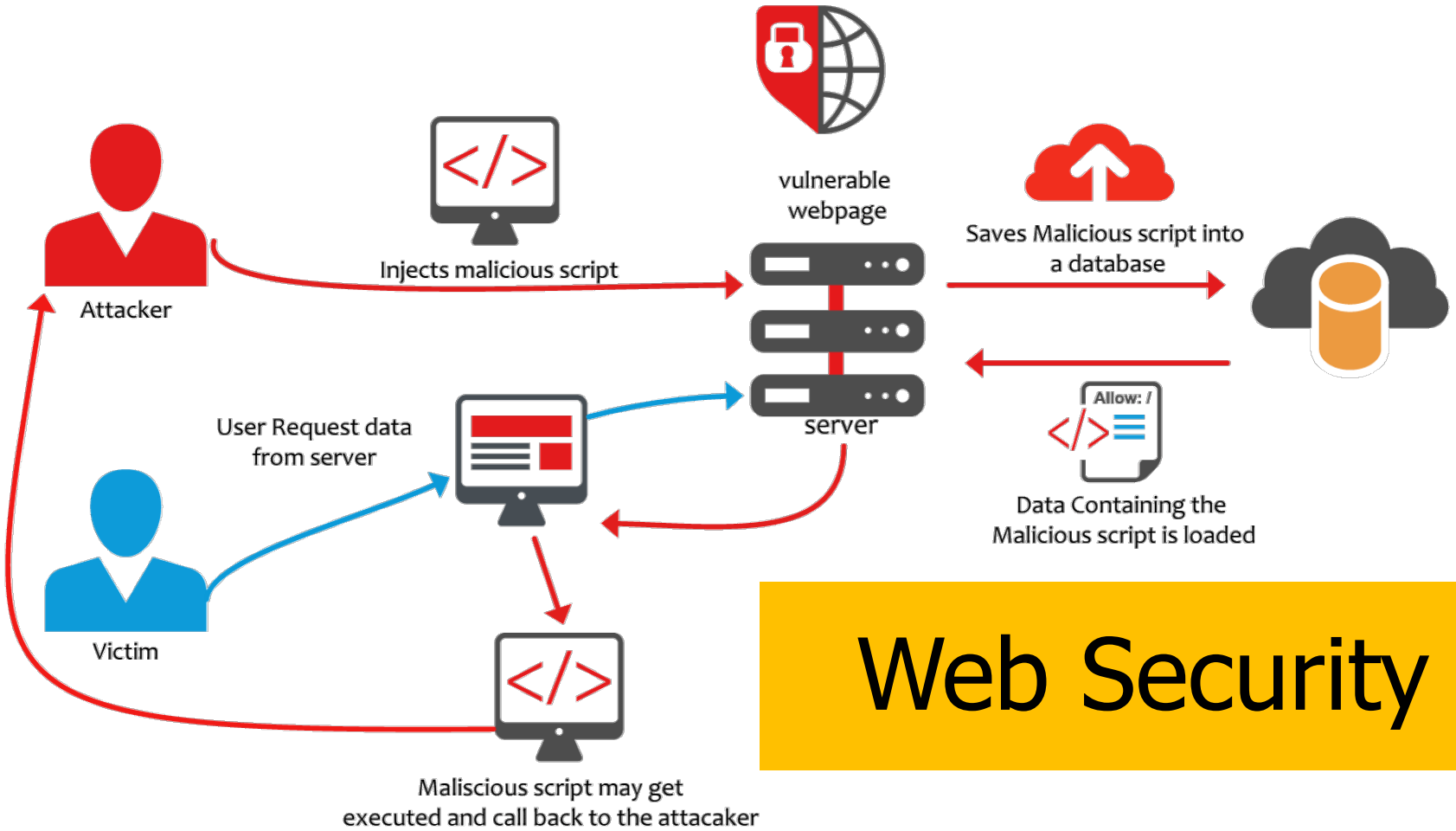
However, in the following code sample, there's an issue. If `arr1->length`, `arr2->data[0x200]` and`arr2->data[0x300]` are not cached, but all other accessed data is, and the branch conditions are predicted as true, the processor can do the following speculatively before `arr1->length` has been loaded and the execution is re-steered:

•

load `value = arr1->data[untrusted_offset_from_caller]`

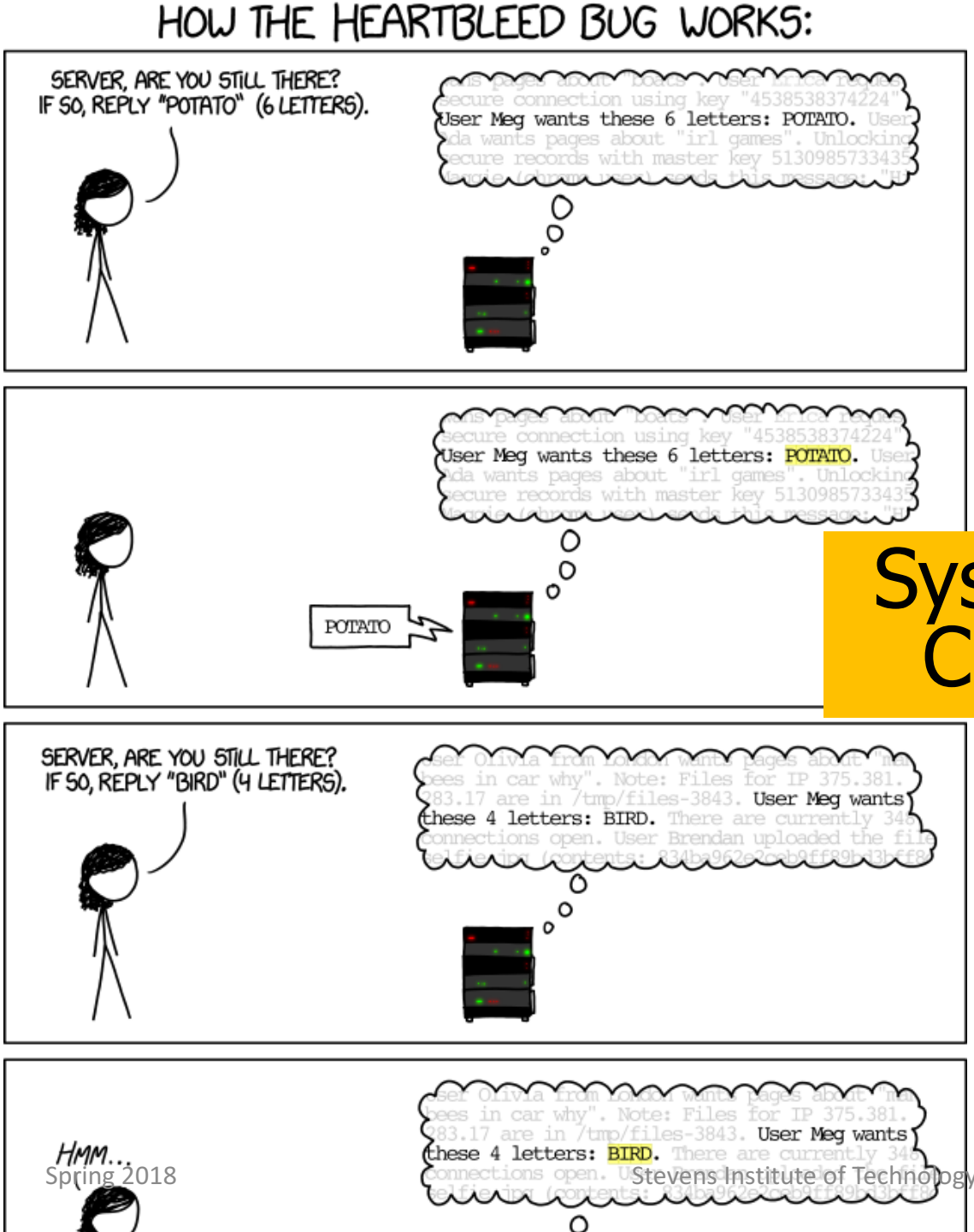
•start a load from a data-dependent offset in `arr2->data`, loading the corresponding cache line into the L1 cache

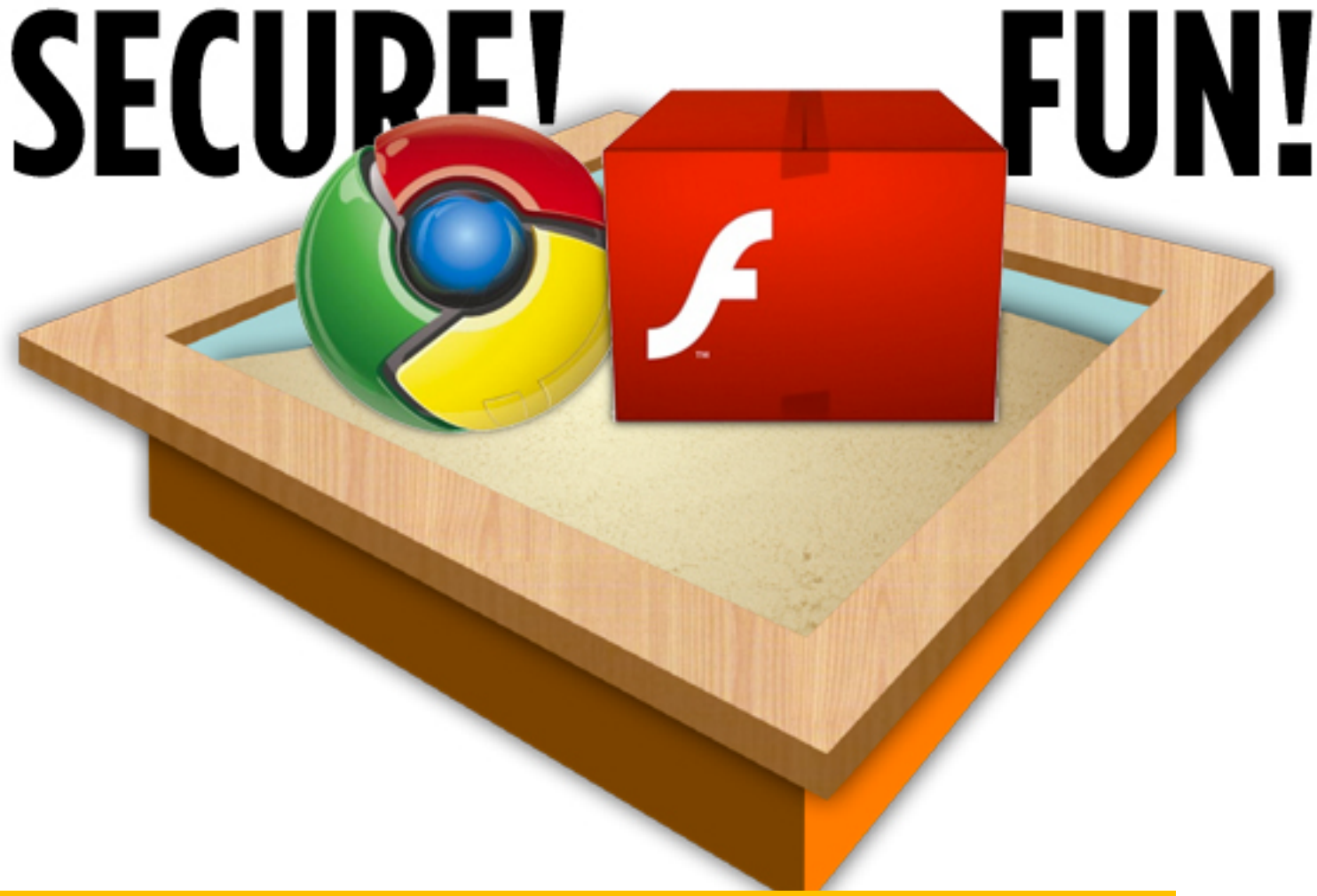
```
struct array {
 unsigned long length;
 unsigned char data[];
};
struct array *arr1 = ...; /* small array */
struct array *arr2 = ...; /* array of size 0x400 */
/* >0x400 (OUT OF BOUNDS!) */
unsigned long untrusted_offset_from_caller = ...;
if (untrusted_offset_from_caller < arr1->length) {
 unsigned char value = arr1->data[untrusted_offset_from_caller];
 unsigned long index2 = ((value&1)*0x100)+0x200;
 if (index2 < arr2->length) {
   unsigned char value2 = arr2->data[index2];
 }
}
```




# Web Security

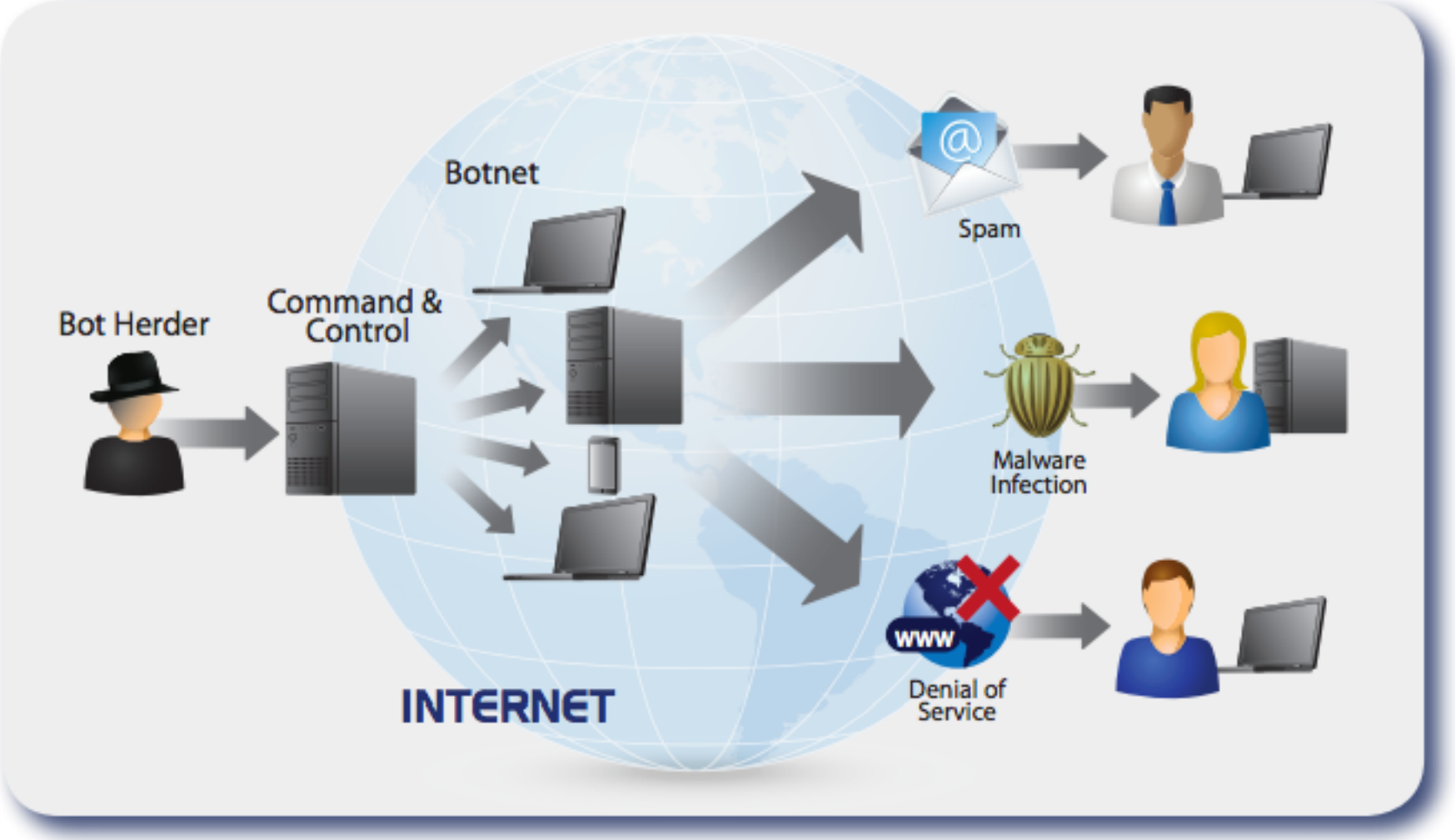
# System Failures of Crypto Systems






# Sandboxing and OS Security

# Network Security




# Malware, botnets, and DDoS