PennState

CSE 543: Computer Security

Module: Introduction

Prof. Syed Rafiul Hussain
Department of Computer Science and Engineering
The Pennsylvania State University

About Me

- Education:
  - 2013-2018: Ph.D. from Purdue University in CS
  - 2019-2020: Postdoc at Purdue University
  - 2020: Assistant Professor at Penn State
- Research Interests: Network and Systems Security
  - Network Security (4G and 5G, Wi-Fi, Bluetooth, ZigBee) Security
  - Embedded Device and IoT Security
  - Software Security
  - Systems Security

Most of my research work is grounded on

formal verification, program analysis, software testing, and cryptography

Some Bedtime Stories…

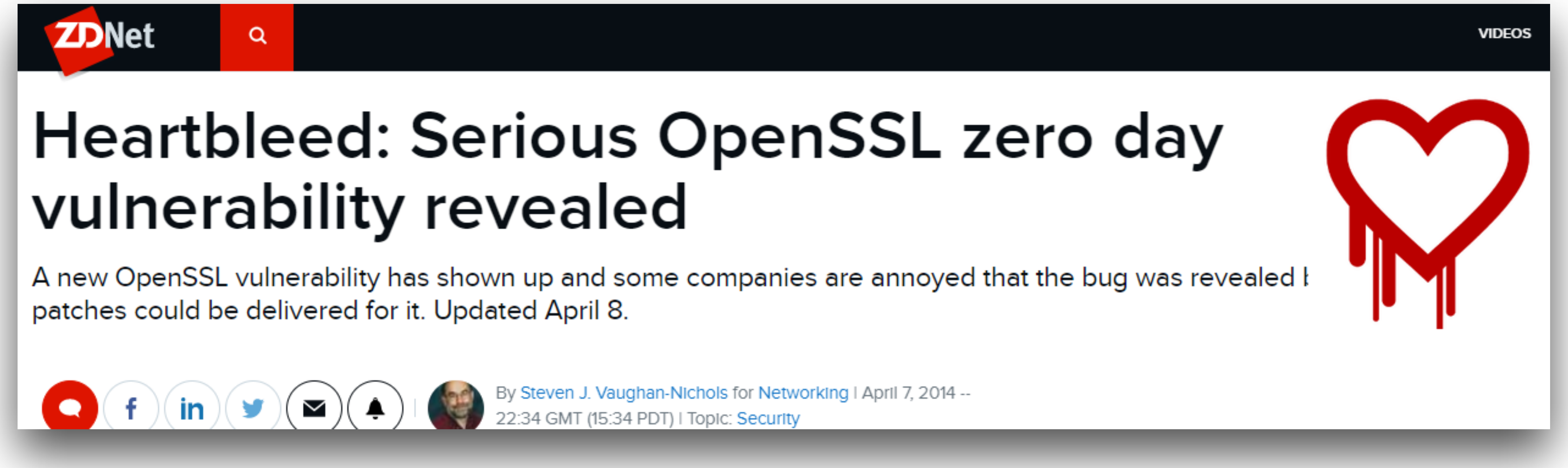
"SQL Slammer is a 2003 computer worm that caused a denial of service on some Internet hosts and dramatically slowed general Internet traffic. It spread rapidly, infecting most of its 75,000 victims within ten minutes.

The program exploited a buffer overflow bug in Microsoft's SQL Server and Desktop Engine database products. Although the MS02-039 patch had been released six months earlier, many organizations had not yet applied it." - source Wikipedia

"The first deal of cyber criminals in Higher Education was an attack on Yale's system in 2002 by hackers from Princeton University. A target of the espionage was information on the admission decisions. In 2003, there were several attacks directed on students' and staff members' personal information." - source: https://www.latimes.com/archives/la-xpm-2002-jul-26-na-yale26-story.html

The **2007 cyberattacks on Estonia** (Estonian: *2007. aasta küberrünnakud Eesti vastu*) were a series of cyberattacks which began on 27 April 2007 and targeted websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's disagreement with Russia about the relocation of the Bronze Soldier of Tallinn, an a Soviet-era grave marker, as well as war graves in Tallinn.[1][2] Most of the attacks that had any influence on the general public were distributed denial of service type attacks ranging from single individuals using various methods like ping floods to expensive rentals of botnets usually used for spam distribution. Source: Wikipedia

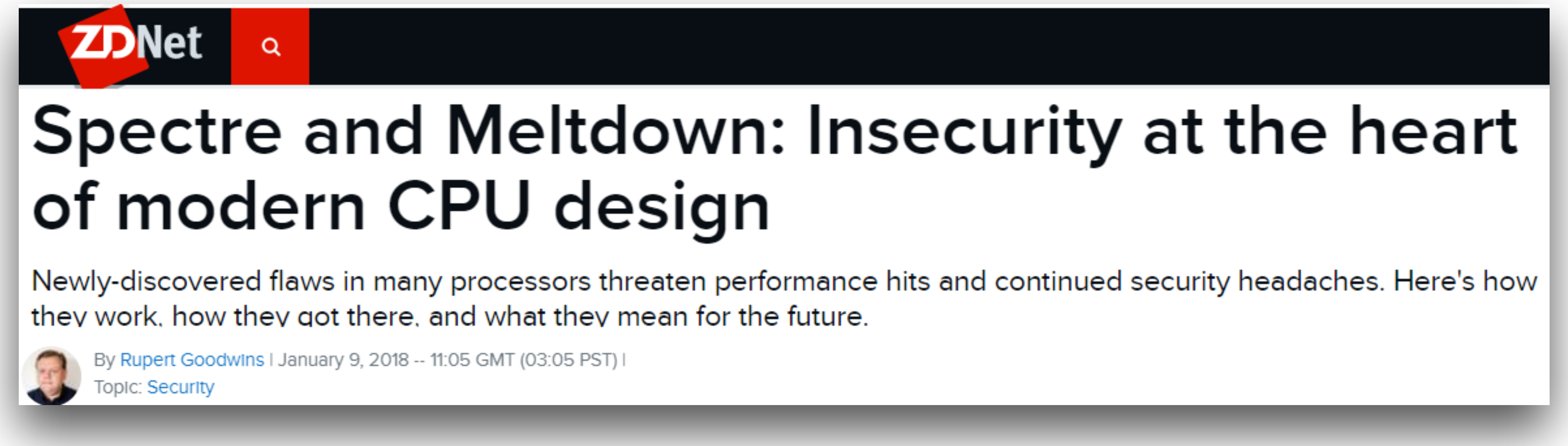
to nightmares …



Heartbleed: Serious OpenSSL zero day vulnerability revealed

A new OpenSSL vulnerability has shown up and some companies are annoyed that the bug was revealed b patches could be delivered for it. Updated April 8.

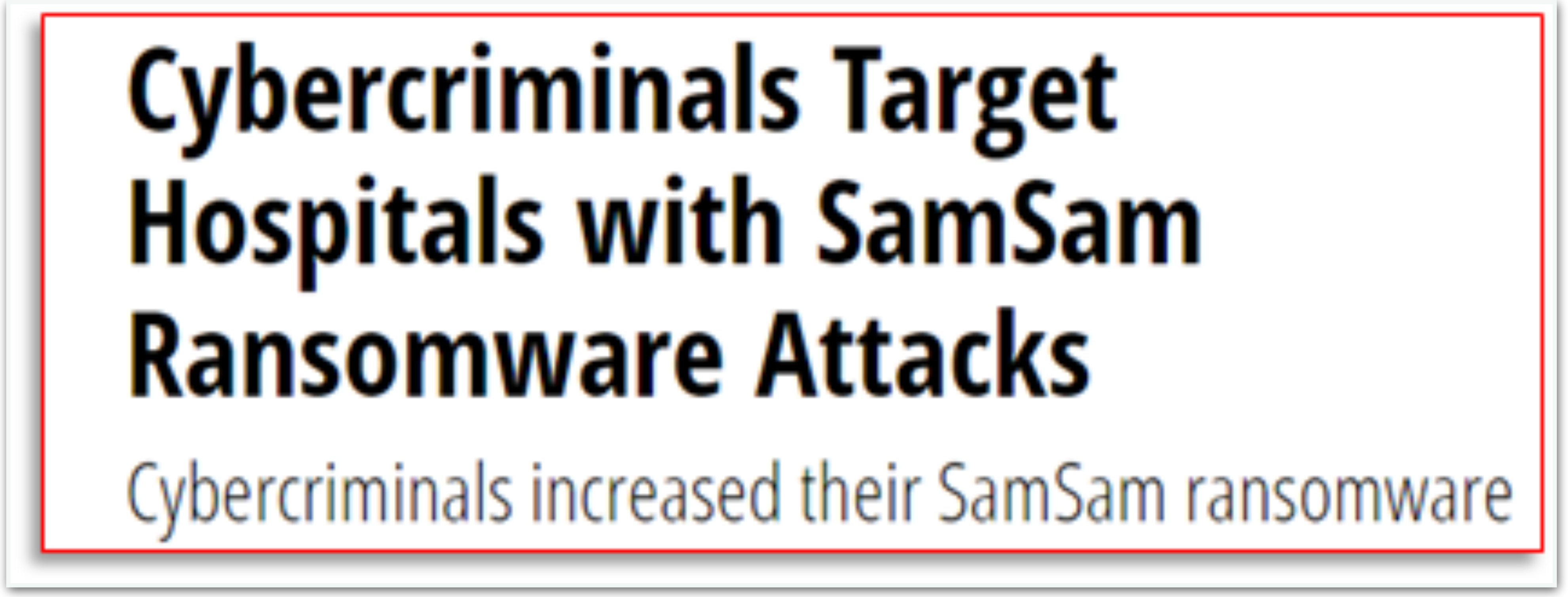
By Steven J. Vaughan-Nichols for Networking | April 7, 2014 -- 22:34 GMT (15:34 PDT) | Topic: Security



Spectre and Meltdown: Insecurity at the heart of modern CPU design

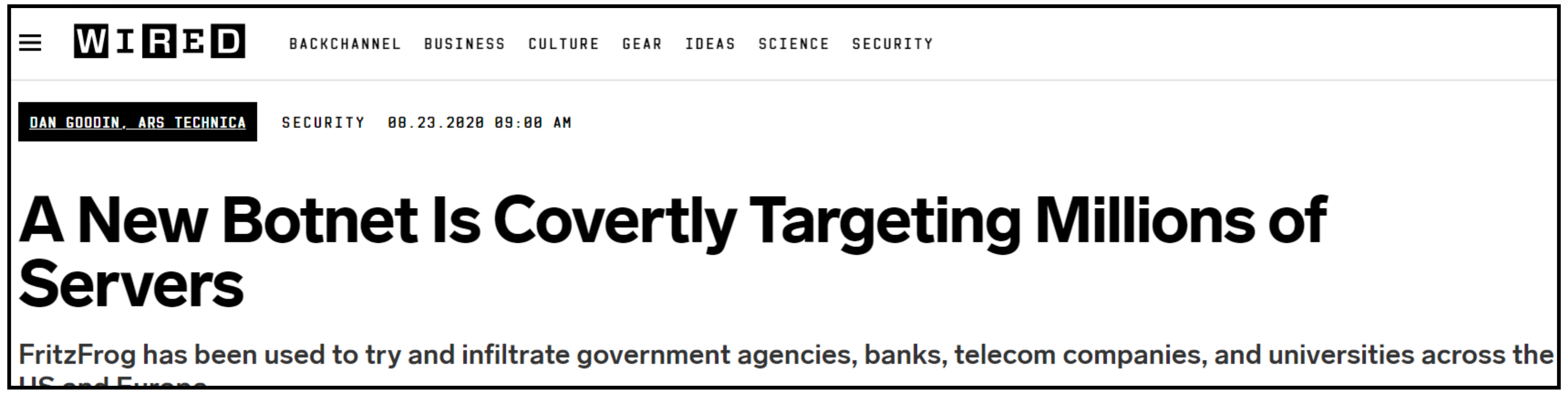
Newly-discovered flaws in many processors threaten performance hits and continued security headaches. Here's how they work, how they got there, and what they mean for the future.

By Rupert Goodwins | January 9, 2018 -- 11:05 GMT (03:05 PST) | Topic: Security



Cybercriminals Target Hospitals with SamSam Ransomware Attacks

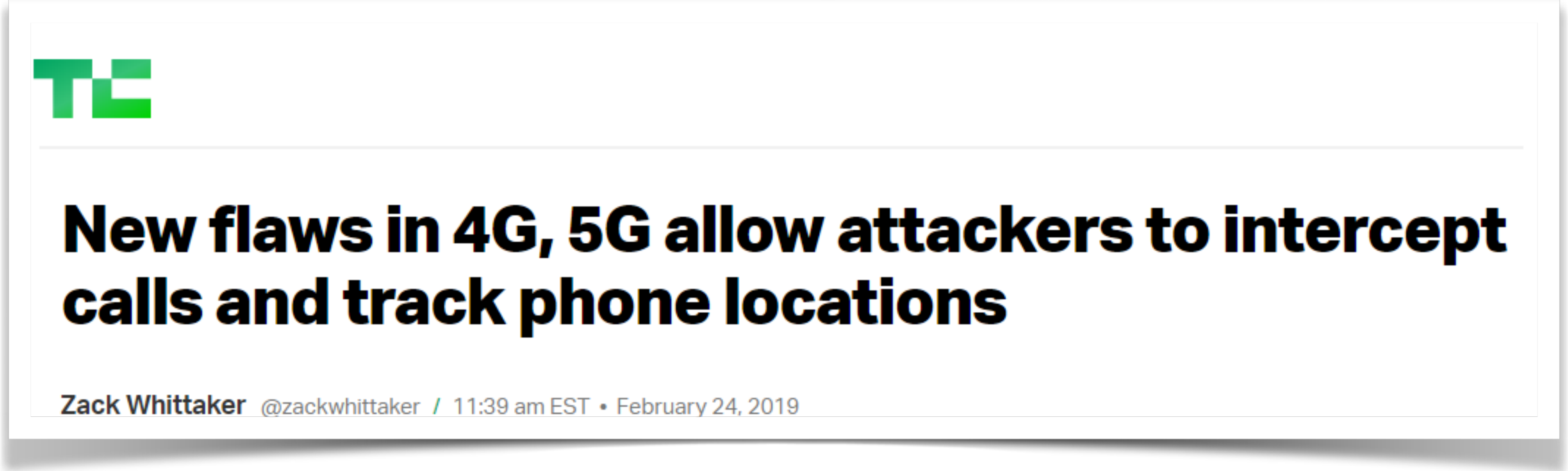
Cybercriminals increased their SamSam ransomware



DAN GOODIN, ARS TECHNICA   SECURITY   08.23.2020 09:00 AM

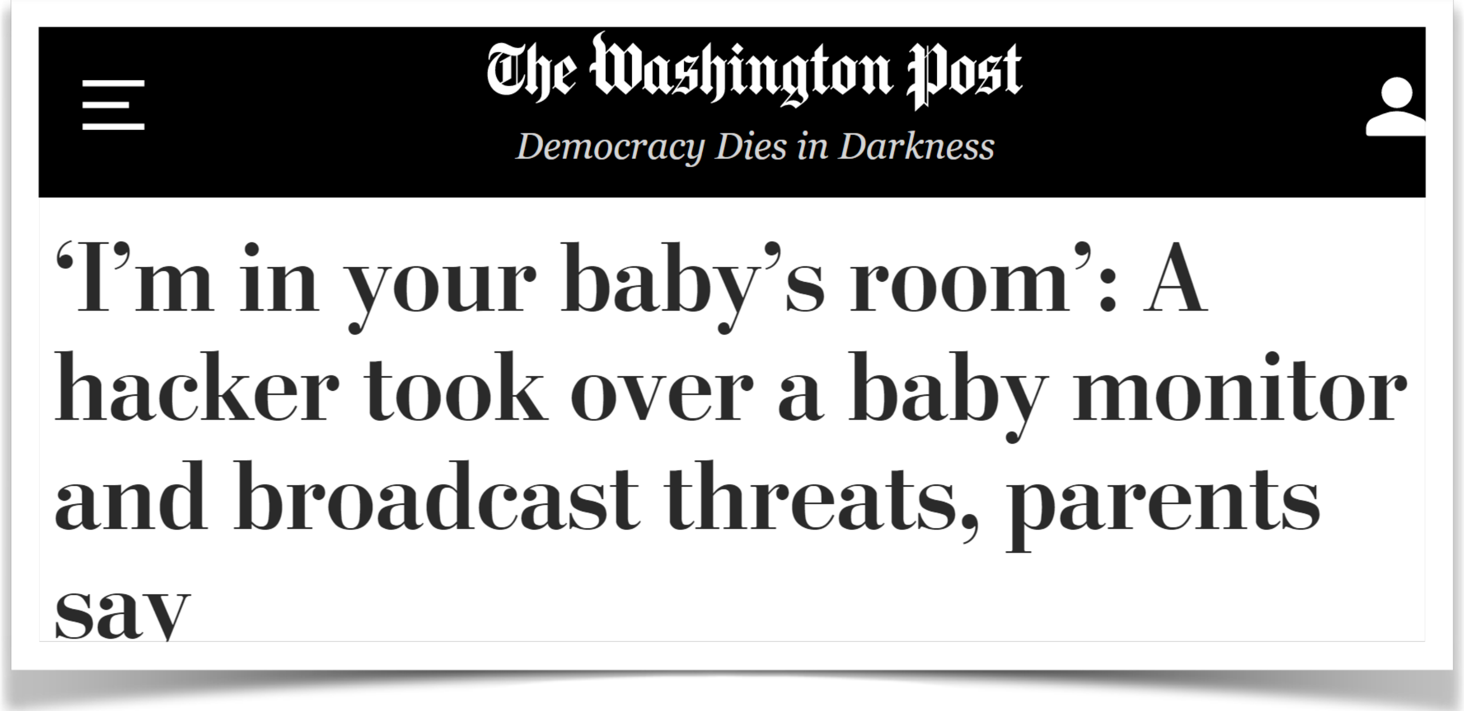
A New Botnet Is Covertly Targeting Millions of Servers

FritzFrog has been used to try and infiltrate government agencies, banks, telecom companies, and universities across the US and Europe.



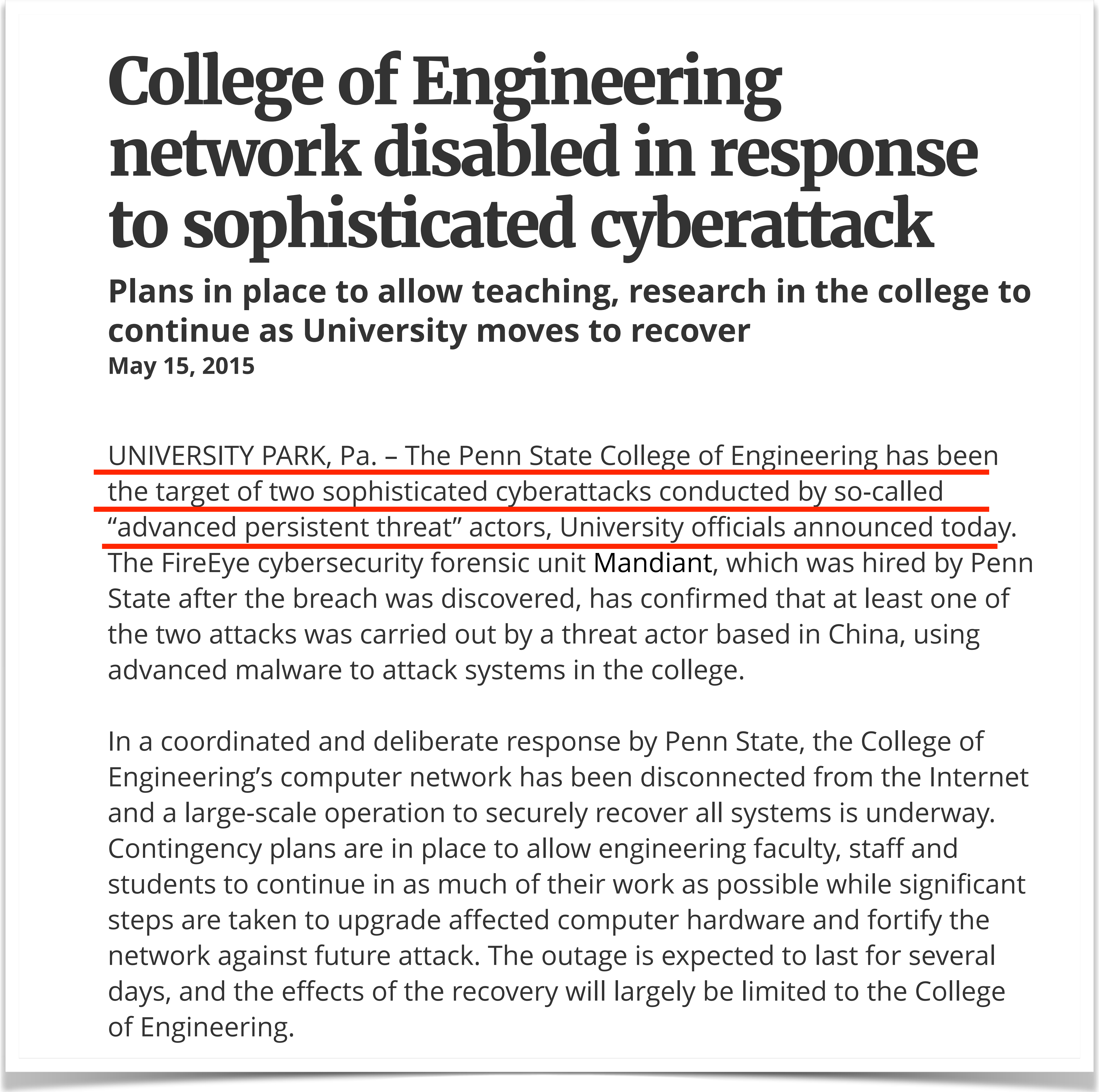
New flaws in 4G, 5G allow attackers to intercept calls and track phone locations

Zack Whittaker @zackwhittaker / 11:39 am EST • February 24, 2019



‘I’m in your baby’s room’: A hacker took over a baby monitor and broadcast threats, parents say

to nightmares …



College of Engineering network disabled in response to sophisticated cyberattack

Plans in place to allow teaching, research in the college to continue as University moves to recover

May 15, 2015

UNIVERSITY PARK, Pa. – The Penn State College of Engineering has been the target of two sophisticated cyberattacks conducted by so-called “advanced persistent threat” actors, University officials announced today. The FireEye cybersecurity forensic unit Mandiant, which was hired by Penn State after the breach was discovered, has confirmed that at least one of the two attacks was carried out by a threat actor based in China, using advanced malware to attack systems in the college.

In a coordinated and deliberate response by Penn State, the College of Engineering’s computer network has been disconnected from the Internet and a large-scale operation to securely recover all systems is underway. Contingency plans are in place to allow engineering faculty, staff and students to continue in as much of their work as possible while significant steps are taken to upgrade affected computer hardware and fortify the network against future attack. The outage is expected to last for several days, and the effects of the recovery will largely be limited to the College of Engineering.

This course

- We are going to explore why these events are not *isolated*, *infrequent*, or even *unexpected*.
- Why are we doing so poorly in computing systems at protecting our users and data from inadvertent or intentional harm?

The answer: stay tuned!

Why Do I Need This Course?

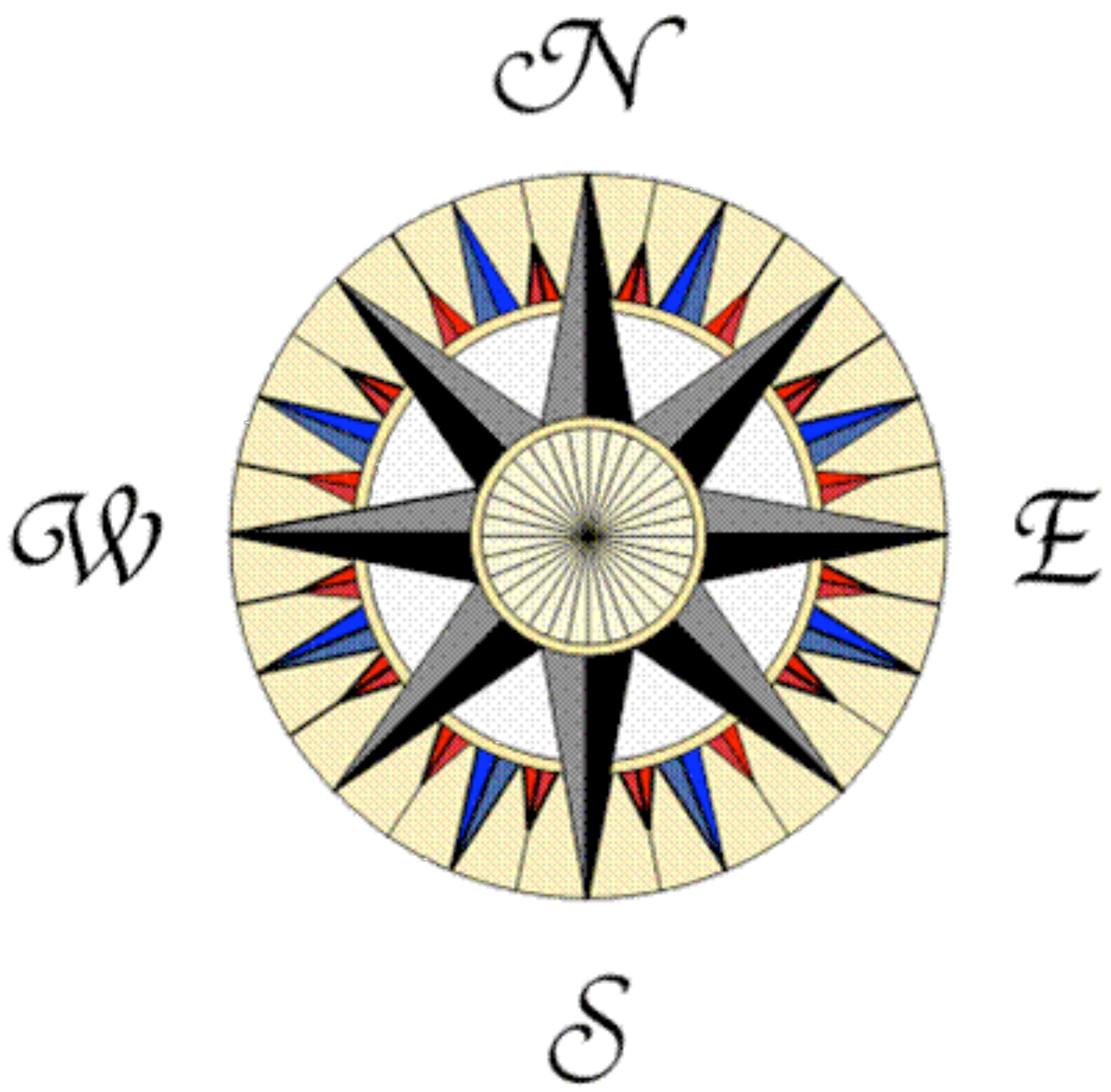
- "Security" is not a discrete topic — it is a design goal (like "performance") that concerns all aspects of computing

- As engineers and scientists, you need to grasp the threats of an increasingly digital world and the tools that exist to fight them.

- Some of you may continue on to develop new technology in this space.

This course ...

- This course is a systems course covering general topics in computer and network security, including:
  - network security, software security, OS security, web security, cryptography, authentication, security protocol design and analysis, key management, intrusion detection, security policy, language-based security, cloud computing security, 4G and 5G security and other emerging topics (as time permits)



You need to understand ...

- How a Computer System *Really* Works
- Program Toolchains (E.g., gcc, binutils)
- Modern Operating Systems
- IP Networks
- Discrete Mathematics
- Basics of systems theory and implementation
  - E.g., File systems, distributed systems, networking, operating systems, ...

Course Goals

- My goal: *to provide you with the tools to understand and evaluate research in computer security.*
  - Foundation of secure computing and basic technologies
    - Fundamental concepts and ideas of computer security
  - Engineering/research trade-offs
    - Ability to acquire new skills and apply techniques from the latest research
  - Develop new cutting edge security solutions.
  - How to read/understand security research papers
- *This is going to be a hard and fun course.* The key to success is sustained effort. Failure to keep up with readings and projects will likely result in poor grades, and ultimately little understanding of the course material. The reward is exposure to an increasingly critical aspect of computing.
- Reward/Pay-off: security competence is a rare, valuable skill. You will get an exposure to an increasingly critical aspect of computing.

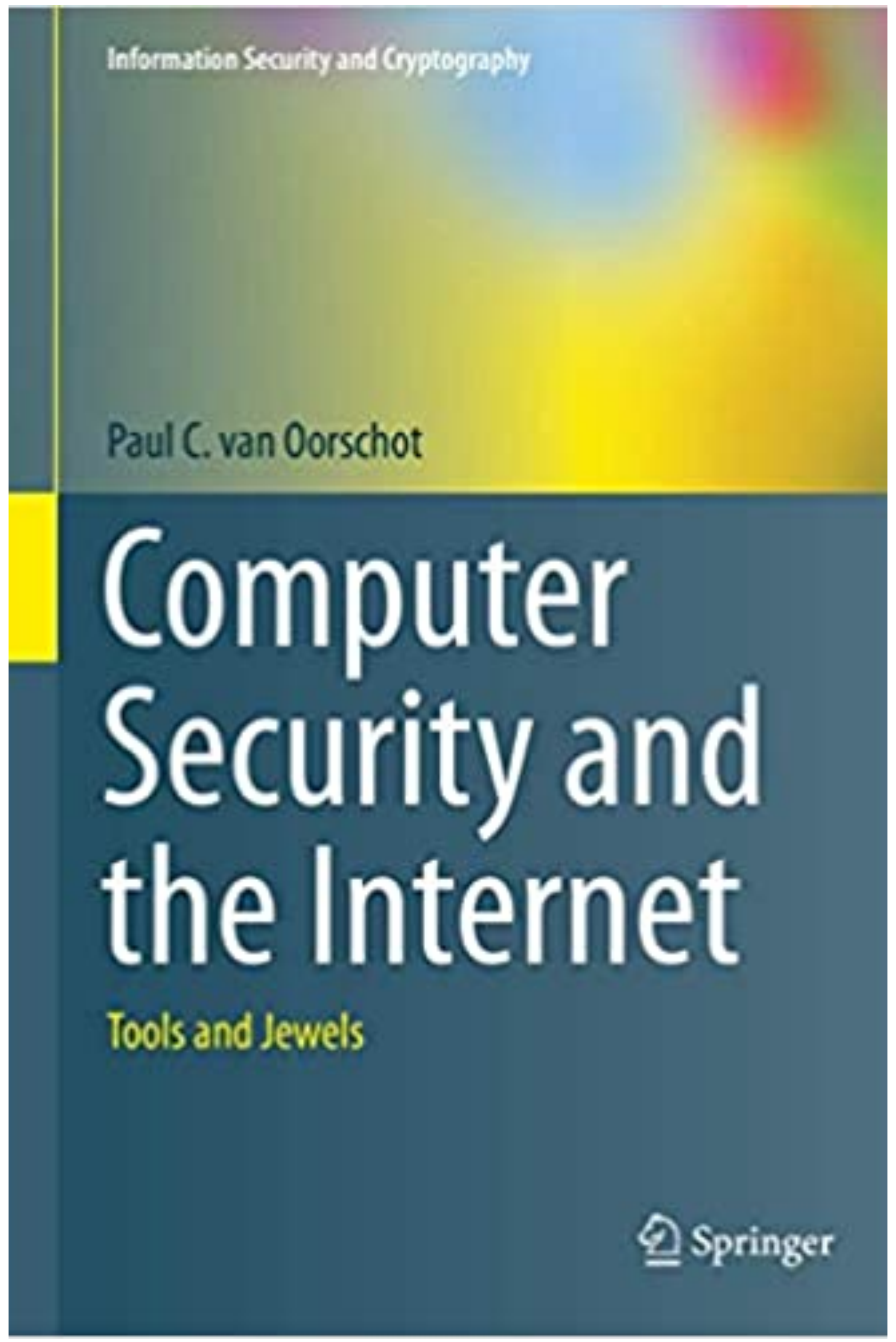
Course Info

- Instructor:
  - Me (`hussain1 'at'` psu.edu)
- TA:
  - Neeraj Karamchandani (`njk5270 'at'` psu.edu)

- Website - I am maintaining the course website at
  - https://relentless-warrior.github.io/index.php/teaching/cse543-f21/
  - The course syllabus can also be found on CANVAS where course related policies are discussed. Changes may apply.
- Office Hours:
  - Me: Tuesday and Thursday (1:30pm-2:30pm) - Zoom
  - Neeraj: Wednesday (11:00am-1:00pm) - Zoom

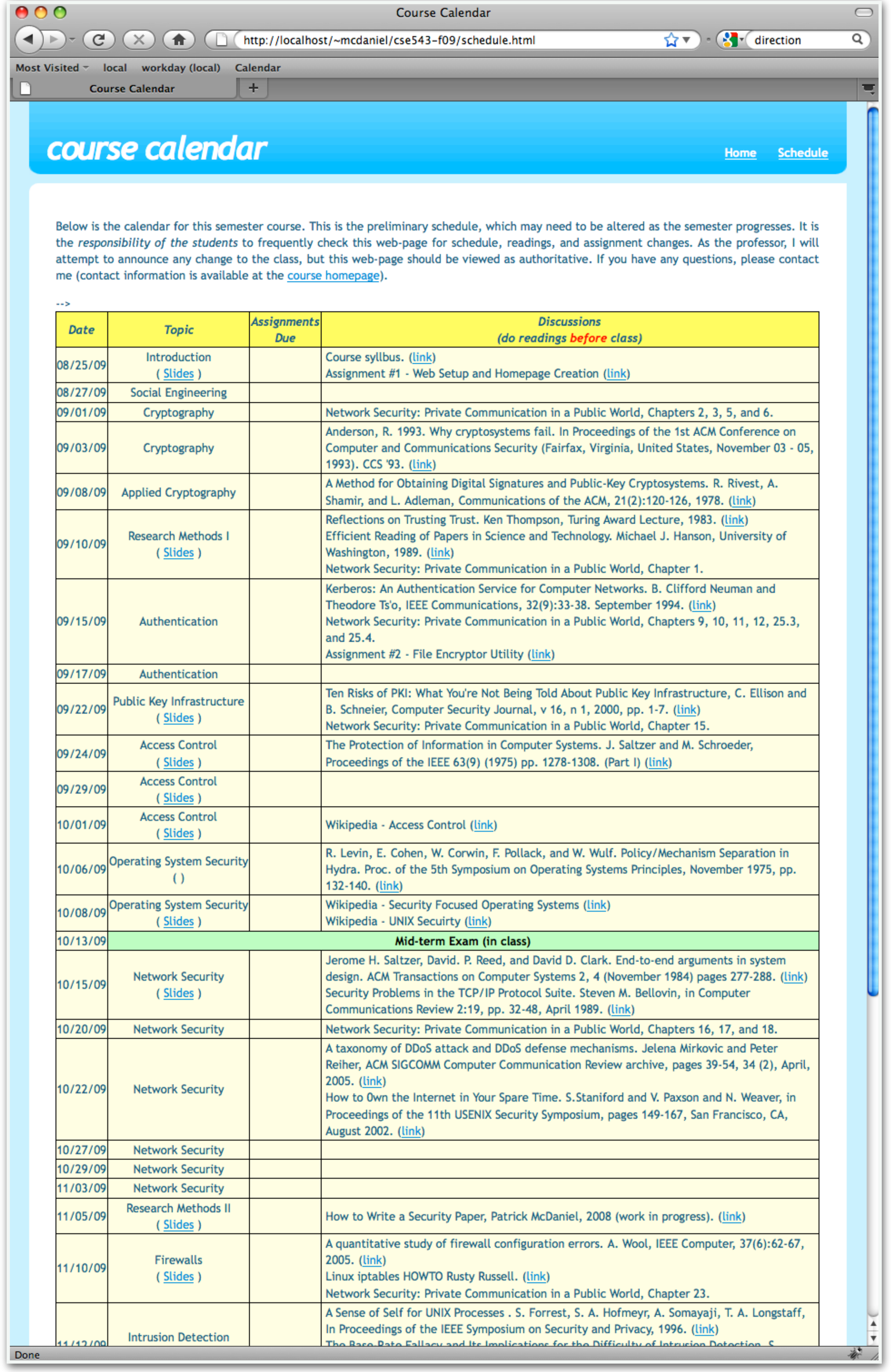
Course Materials

- Course assignments, slides, and other artifacts will be made available on the course website.
  - Assignment submissions via Canvas
- Piazza for discussion
- Course textbook
  - Computer Security and the Internet
    - Paul C. van Oorschot


Information Security and Cryptography
Paul C. van Oorschot
Computer Security and the Internet
Tools and Jewels
Springer

Course Calendar

- The course calendar as all the relevant readings, assignments and test dates
- The calendar page contains electronic links to online papers assigned for course readings.
- *Please check the website frequently for announcements and changes* to the schedule. Students are responsible for any change on the schedule.



course calendar

Home Schedule

Below is the calendar for this semester course. This is the preliminary schedule, which may need to be altered as the semester progresses. It is the *responsibility of the students* to frequently check this web-page for schedule, readings, and assignment changes. As the professor, I will attempt to announce any change to the class, but this web-page should be viewed as authoritative. If you have any questions, please contact me (contact information is available at the course homepage).

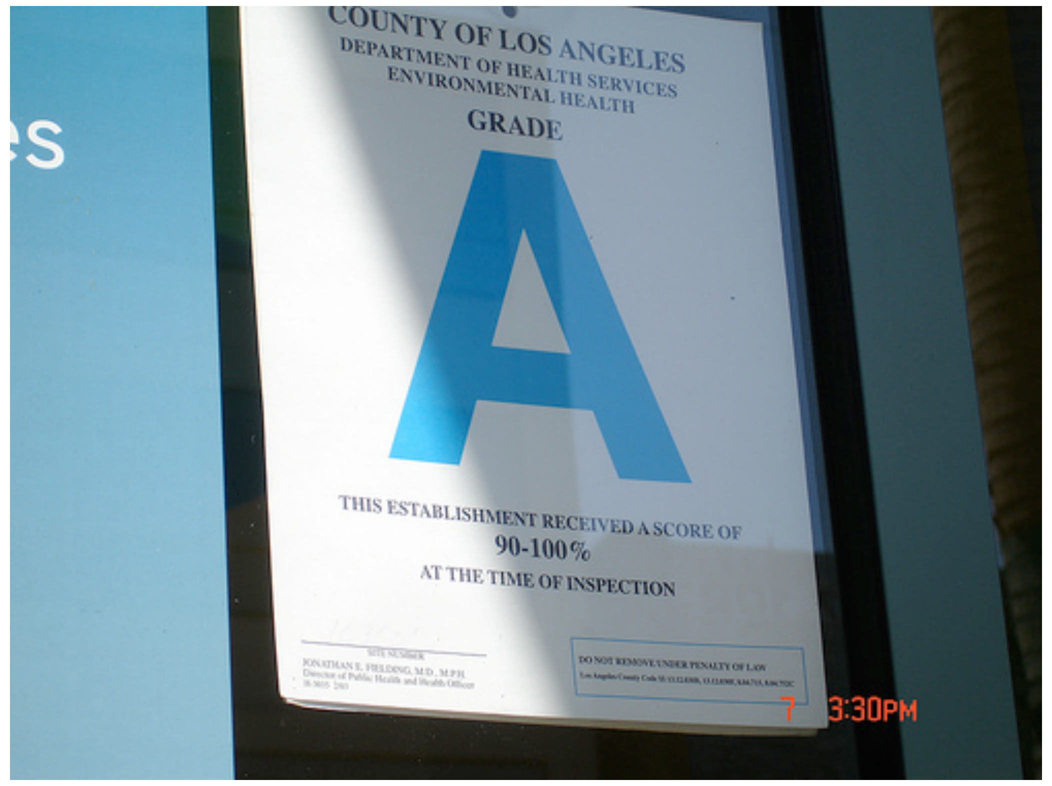
-->

Date	*Topic*	*Assignments Due*	*Discussions (do readings before class)*
08/25/09	Introduction (Slides)		Course syllbus. (link) Assignment #1 - Web Setup and Homepage Creation (link)
08/27/09	Social Engineering		
09/01/09	Cryptography		Network Security: Private Communication in a Public World, Chapters 2, 3, 5, and 6.
09/03/09	Cryptography		Anderson, R. 1993. Why cryptosystems fail. In Proceedings of the 1st ACM Conference on Computer and Communications Security (Fairfax, Virginia, United States, November 03 - 05, 1993). CCS '93. (link)
09/08/09	Applied Cryptography		A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. R. Rivest, A. Shamir, and L. Adleman, Communications of the ACM, 21(2):120-126, 1978. (link)
09/10/09	Research Methods I (Slides)		Reflections on Trusting Trust. Ken Thompson, Turing Award Lecture, 1983. (link) Efficient Reading of Papers in Science and Technology. Michael J. Hanson, University of Washington, 1989. (link) Network Security: Private Communication in a Public World, Chapter 1.
09/15/09	Authentication		Kerberos: An Authentication Service for Computer Networks. B. Clifford Neuman and Theodore Ts'o, IEEE Communications, 32(9):33-38. September 1994. (link) Network Security: Private Communication in a Public World, Chapters 9, 10, 11, 12, 25.3, and 25.4. Assignment #2 - File Encryptor Utility (link)
09/17/09	Authentication		
09/22/09	Public Key Infrastructure (Slides)		Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure, C. Ellison and B. Schneier, Computer Security Journal, v 16, n 1, 2000, pp. 1-7. (link) Network Security: Private Communication in a Public World, Chapter 15.
09/24/09	Access Control (Slides)		The Protection of Information in Computer Systems. J. Saltzer and M. Schroeder, Proceedings of the IEEE 63(9) (1975) pp. 1278-1308. (Part I) (link)
09/29/09	Access Control (Slides)		
10/01/09	Access Control (Slides)		Wikipedia - Access Control (link)
10/06/09	Operating System Security ( )		R. Levin, E. Cohen, W. Corwin, F. Pollack, and W. Wulf. Policy/Mechanism Separation in Hydra. Proc. of the 5th Symposium on Operating Systems Principles, November 1975, pp. 132-140. (link)
10/08/09	Operating System Security (Slides)		Wikipedia - Security Focused Operating Systems (link) Wikipedia - UNIX Secuirty (link)
10/13/09	**Mid-term Exam (in class)**		
10/15/09	Network Security (Slides)		Jerome H. Saltzer, David. P. Reed, and David D. Clark. End-to-end arguments in system design. ACM Transactions on Computer Systems 2, 4 (November 1984) pages 277-288. (link) Security Problems in the TCP/IP Protocol Suite. Steven M. Bellovin, in Computer Communications Review 2:19, pp. 32-48, April 1989. (link)
10/20/09	Network Security		Network Security: Private Communication in a Public World, Chapters 16, 17, and 18.
10/22/09	Network Security		A taxonomy of DDoS attack and DDoS defense mechanisms. Jelena Mirkovic and Peter Reiher, ACM SIGCOMM Computer Communication Review archive, pages 39-54, 34 (2), April, 2005. (link) How to 0wn the Internet in Your Spare Time. S.Staniford and V. Paxson and N. Weaver, in Proceedings of the 11th USENIX Security Symposium, pages 149-167, San Francisco, CA, August 2002. (link)
10/27/09	Network Security		
10/29/09	Network Security		
11/03/09	Network Security		
11/05/09	Research Methods II (Slides)		How to Write a Security Paper, Patrick McDaniel, 2008 (work in progress). (link)
11/10/09	Firewalls (Slides)		A quantitative study of firewall configuration errors. A. Wool, IEEE Computer, 37(6):62-67, 2005. (link) Linux iptables HOWTO Rusty Russell. (link) Network Security: Private Communication in a Public World, Chapter 23.
11/12/09	Intrusion Detection		A Sense of Self for UNIX Processes . S. Forrest, S. A. Hofmeyr, A. Somayaji, T. A. Longstaff, In Proceedings of the IEEE Symposium on Security and Privacy, 1996. (link) The Base-Rate Fallacy and Its Implications for the Difficulty of Intrusion Detection. S.

Grading

- The course will be graded on exams, projects, paper reviews and class participation in the following proportions:

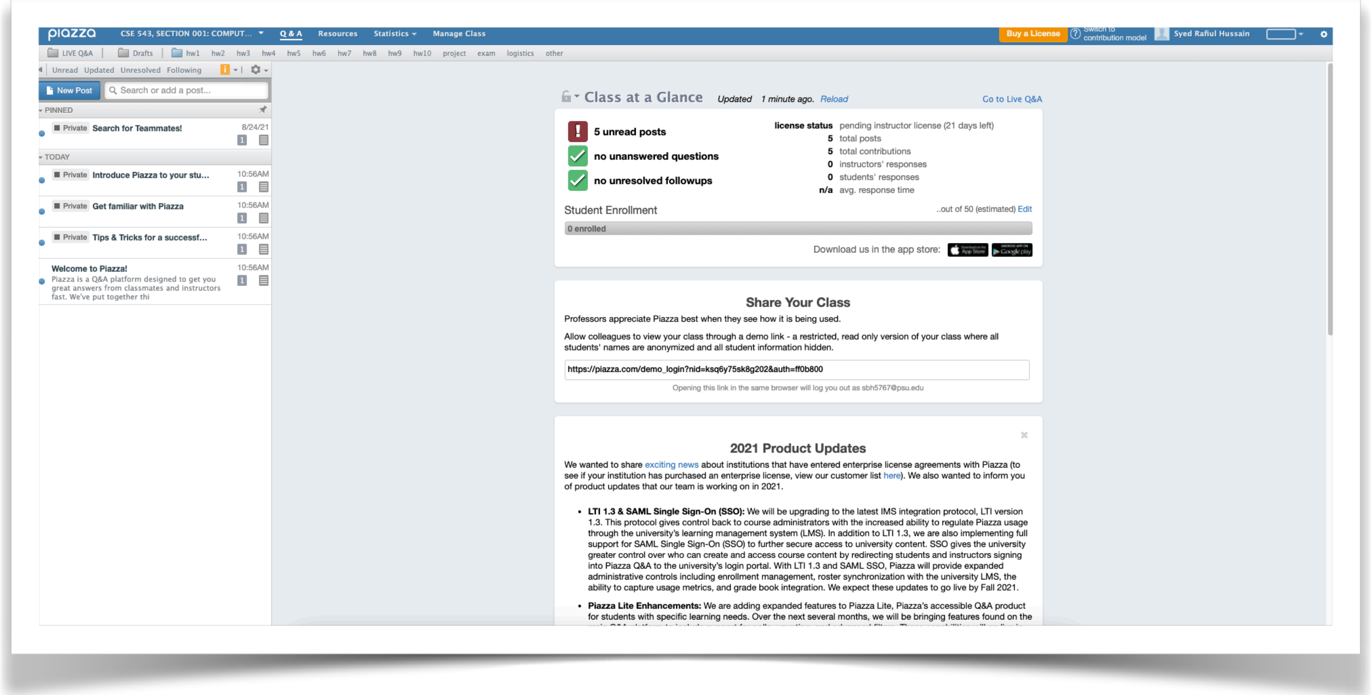
20% Focused Projects
25% Research Project
7.5% Quizzes
15% Mid-term Exam
22.5% Final Exam (comprehensive)
10% Paper Reviews & Participation


COUNTY OF LOS ANGELES
DEPARTMENT OF HEALTH SERVICES
ENVIRONMENTAL HEALTH
GRADE
A
THIS ESTABLISHMENT RECEIVED A SCORE OF
90-100%
AT THE TIME OF INSPECTION
3:30PM

- NOTE: Must do better than 50% average on **each of exams and programmin projects** to pass the course.

Online Course Discussion

- Discussion on class lectures, projects, assignments, quizzes and exams will be via Piazza
  - You are expected to read each and every posting.
  - You are expected to participate.



Private Search for Teammates! 8/24/21

Private Introduce Piazza to your stu... 10:56AM

Private Get familiar with Piazza 10:56AM

Private Tips & Tricks for a successf... 10:56AM

Welcome to Piazza! Piazza is a Q&A platform designed to get you great answers from classmates and instructors fast. We've put together thi 10:56AM

Class at a Glance Updated 1 minute ago. Reload Go to Live Q&A

5 unread posts

✓ no unanswered questions

✓ no unresolved followups

license status	pending instructor license (21 days left)
5	total posts
5	total contributions
0	instructors' responses
0	students' responses
n/a	avg. response time

Student Enrollment ..out of 50 (estimated) Edit

0 enrolled

Download us in the app store:

Share Your Class

Professors appreciate Piazza best when they see how it is being used.

Allow colleagues to view your class through a demo link - a restricted, read only version of your class where all students' names are anonymized and all student information hidden.

https://piazza.com/demo_login?nid=ksq6y75sk8g202&auth=ff0b800

Opening this link in the same browser will log you out as sbh5767@psu.edu

2021 Product Updates

We wanted to share exciting news about institutions that have entered enterprise license agreements with Piazza (to see if your institution has purchased an enterprise license, view our customer list here). We also wanted to inform you of product updates that our team is working on in 2021.

- **LTI 1.3 & SAML Single Sign-On (SSO):** We will be upgrading to the latest IMS integration protocol, LTI version 1.3. This protocol gives control back to course administrators with the increased ability to regulate Piazza usage through the university's learning management system (LMS). In addition to LTI 1.3, we are also implementing full support for SAML Single Sign-On (SSO) to further secure access to university content. SSO gives the university greater control over who can create and access course content by redirecting students and instructors signing into Piazza Q&A to the university's login portal. With LTI 1.3 and SAML SSO, Piazza will provide expanded administrative controls including enrollment management, roster synchronization with the university LMS, the ability to capture usage metrics, and grade book integration. We expect these updates to go live by Fall 2021.
- **Piazza Lite Enhancements:** We are adding expanded features to Piazza Lite, Piazza's accessible Q&A product for students with specific learning needs. Over the next several months, we will be bringing features found on the

- Post to Piazza if…
  - …you have a question about the class subject matter (slides, lectures, etc.)
  - …you need a clarification on a homework
  - …you have a general question about network security
  - …you have a question regarding a class policy
- If you send any of the above to me directly, I'll ask you to post it on Piazza
- Don't:
  - Give away solutions to assignments
  - Start flamewars,
- Do be respectful of others

Exams

- Midterm and Final
  - Same Format
  - Short Answer Questions
    - What is X?
  - Conceptual Questions
    - Why is Y?
  - Constructions
    - How is Z?
- Time can be an issue
  - Answer the questions you know
- Final is worth far more than midterm
- Webcam Policy (Check syllabus and course webpage)

Projects

- Goal: Learn security concepts
- Goal: Learn research skills

- Projects (Individual)
  - Software Security
    - Attacks
  - Network Security
    - Attacks and Defenses
- Lateness Policy:
  - 15% per-day late penalty, up to maximum of 4 days.

Readings

- There are a large amount of readings in this course covering various topics. These assignments are intended to:
  - Support the lectures in the course (provide clarity)
  - Augment the lectures and provide a broader exposure to security topics.
- Students are ***required*** to do the reading!
- <u>*About 10-20% of questions on the tests will be off the reading on topics that were not covered in class*</u>. You better do the reading or you are going to be in deep trouble when it comes to grades.

Paper reviews

- Goal: Record key ideas and methods for later
- We will review one paper per week

Assignment 0

- This assignment is to help me get to know you and what you expect to achieve in this class. There are no right or wrong answers. Please make sure to limit your answers within 1 page.
  - Briefly mention about yourself and your research interests. What have you studied in the past?
  - Describe your prior experience with computer security if you have any, why you are interested in this class, what you would like to achieve/learn throughout the course, and if you like to pursue a career in security. It's also okay to mention that you are taking the course to fulfill the degree requirements.
  - Describe what you think are the three most recent important issues in computer security and privacy.important issues in computer security and privacy.

Ethics Statement

- This course considers topics involving personal and public privacy and security. As part of this investigation we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class and or institution.
- When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Professor Hussain.

Academic Integrity Policy

- See the EECS Department's Academic Integrity Standards for CMPSC, CMPEN, and CSE Programming Courses

- http://www.eecs.psu.edu/students/resources/EECS-CSE-Academic-Integrity.aspx

- You must follow this policy

Academic Integrity Policy

- The Department of Computer Science and Engineering expects all student programming work assigned in a class to be completed independently by students (or by teams if permitted/required) and to consist of code designed and developed solely by the students. The use of any other code is not permitted unless the course instructor explicitly allows it and such code is clearly identified as coming from an external source and that source is credited. Students will never be given credit for code which they did not construct.

- The department uses software tools to identify similarities in code submitted by students. These tools differentiate between insignificant cosmetic differences (names used in code, the order of certain code elements) and significant structural similarities (algorithms, data organization). These tools give a percentage of common code between two submissions and identify this common code. We do not set a single, fixed percentage above which we automatically determine that an academic violation has occurred. Rather we rely on the expertise of the instructor to determine when similarities rise above what a reasonable person could expect two students working independently to construct.

Academic Integrity Policy

- For example, in an introductory course in which the programming assignments require relatively short solutions (i.e., less than 50 lines of code) we would expect to see similarities in student solutions rising to a significant percentage of the code. But in an advanced course in which programming projects may contain thousands of lines of code, only a small percentage may be similar but still constitute an academic integrity violation if the code in question was a significant/important aspect of the assignment and if the similarities found could not, in the opinion of the instructor, have been independently developed.

- Furthermore, in cases where student submissions have been found to contain significant portions of code found in online sources (e.g., a common code hosting site is GitHub), the determination of an academic integrity violation is essentially automatic.

Other Course Policies

- Class Recording Policy
  - Video and audio recordings of class lectures will be part of the classroom activity. The video and audio recording is used for educational use/purposes and only may be made available to all students presently enrolled in the class. For purposes where the recordings will be used in future class session/lectures, any type of identifying information will be adequately removed.
- Copyright Policy
  - All course materials students receive or to which students have online access are protected by copyright laws. For courses in which they have previously been or are currently enrolled, students may use course materials and make copies for their own use as needed, but unauthorized distribution and/or uploading of materials without the instructor’s express permission is strictly prohibited.

What is security?

PennState

What does it mean for a system to be secure?
Write your own definition?

- Garfinkel and Spafford (1991)
  - "A computer is secure if you can depend on it and its software to behave as expected."
- Harrison, Ruzzo, Ullman (1978)
  - "Prevent access by unauthorized users"
- Not really satisfactory – does not truly capture that security speaks to the behavior of others
  - Expected by whom?
  - Under what circumstances?
  - What are the risks?

A Meta definition

A system is secure if it can maintain well-specified properties in spite of the actions of well-specified adversaries.

- The set of properties we assume to be correct is called the trust model
- The set of adversaries (and their capability) is called the threat model
- Trust Model + Threat Model = Security Model
- The art and science of secure systems lies in properly identifying these properties, adversaries, and designing mechanisms that achieve this goal.

Risk

- At-risk valued resources that can be misused
  - Monetary
  - Data (loss or integrity)
  - Time
  - Confidence
  - Trust
- What does being misused mean?
  - Confidentiality
  - Integrity
  - Availability
  - Privacy (personal)
- Q:What is at stake in your life?

Security Goals/Properties (C, I, A)

- Confidentiality (secrecy, privacy)
  - only those who are authorized to know can know
- Integrity (also authenticity in communication)
  - only modified by authorized parties and in permitted ways
  - do things that are expected
- Availability
  - those authorized to access can get access

Adversary

- An adversary is any entity trying to circumvent the security infrastructure
  - The curious and otherwise generally clueless (e.g., script-kiddies)
  - Casual attackers seeking to understand systems
  - Venal people with an axe to grind
  - Malicious groups of largely sophisticated users (e.g, chaos clubs)
  - Competitors (industrial espionage)
  - Governments (seeking to monitor activities)

6'6"
6'0"
5'6"
5'0"
4'6"
4'0"
3'6"
3'0"
arts-wallpapers.com
- Not for Sale
do not for sale this desktop work image, only be used for your personal use only. desktop work (c) arts-wallpapers.com

Thinking Like an Adversary

- Computer security experts think like an attacker all the time
  - "What can go wrong?"
  - "How can it go wrong?"
  - "What assumptions might not be correct?"
  - "How can I exploit the system?"

Thinking Like a Defender

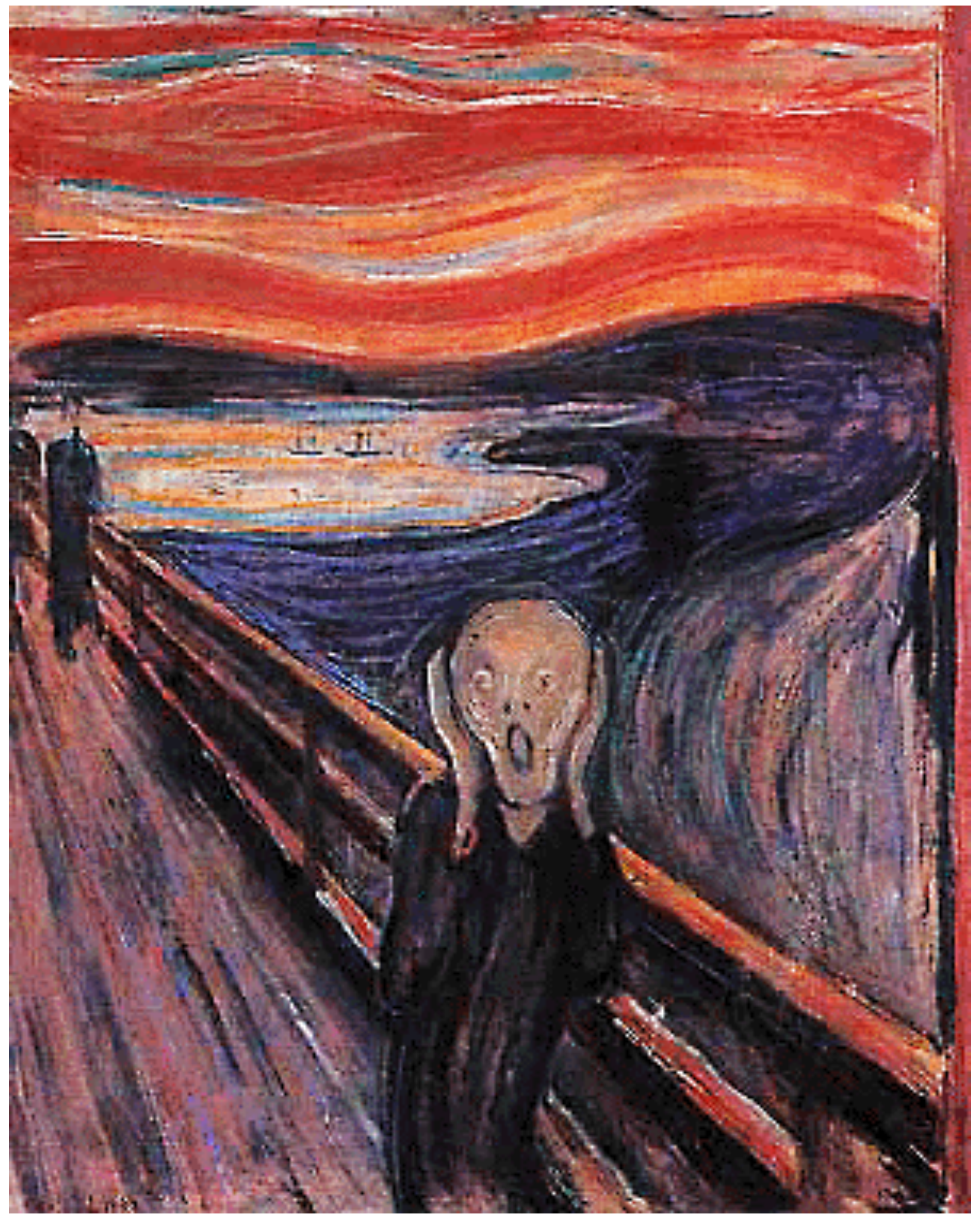
- Security Policy
- Threat Model
- Risk Assessment
- Countermeasures

Threats

- A threat is a specific means by which an adversary can put a system at risk
  - An ability/goal of an adversary (e.g., eavesdrop, fraud, access denial)
  - Independent of what can be compromised
- A threat model is a collection of threats that deemed important for a particular environment
  - A collection of adversary(ies) abilities
  - E.g., a powerful adversary can read and modify all communications and generate messages on a communication channel
- Q: What were risks/threats in the introductory examples?
  - Slammer
  - Yale/Princeton
  - Estonia

Vulnerabilities (attack vectors)

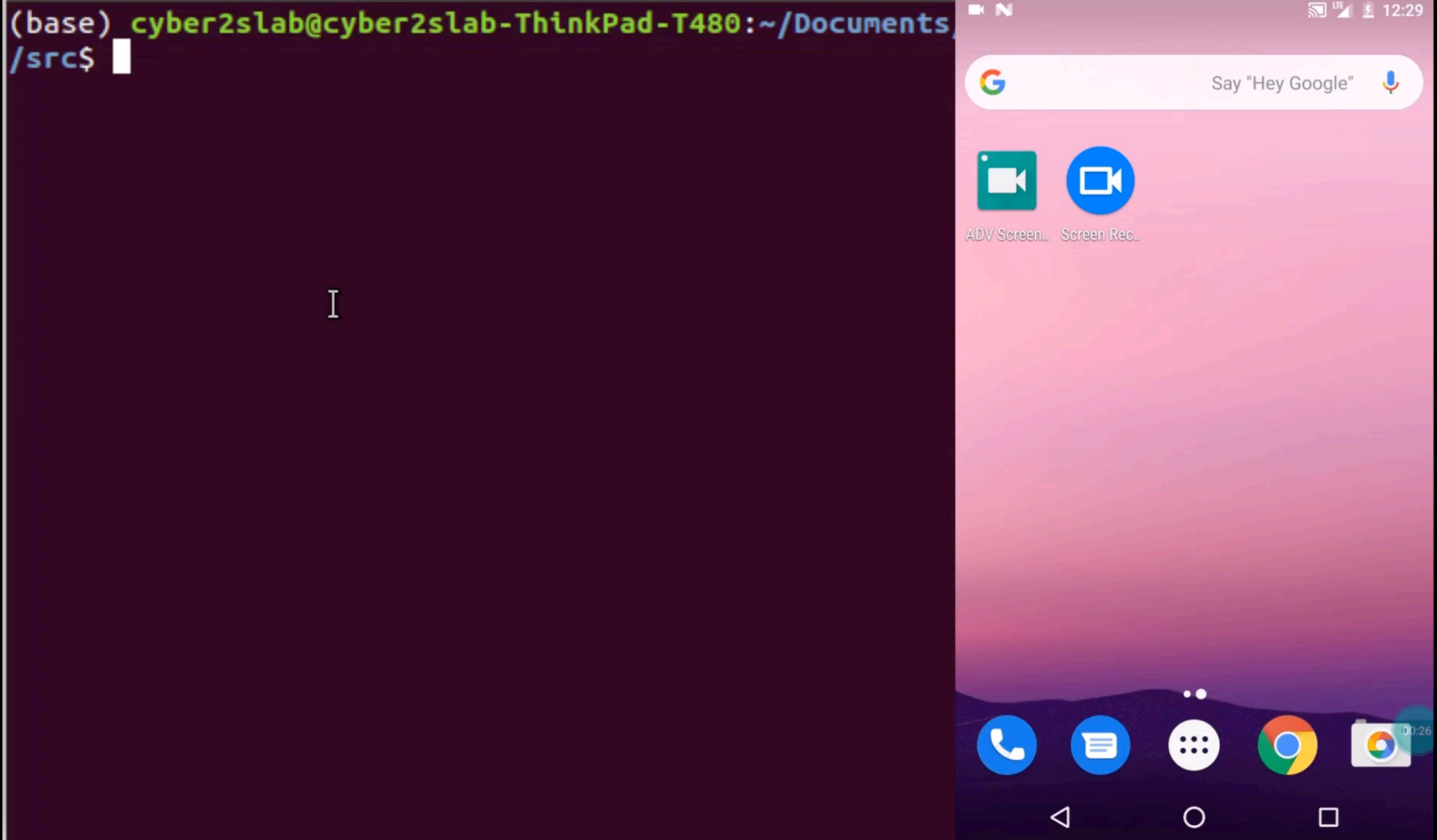
- A vulnerability is a flaw that is accessible to an adversary who can exploit that flaw
- E.g., buffer overflow, file open w/ adversary name
- What is the source of a vulnerability?
  - Bad software (or hardware)
  - Bad design, requirements
  - Bad policy/configuration
  - System Misuse
  - Unintended purpose or environment
    - E.g., student IDs for liquor store



Attacks

- An attack occurs when an adversary attempts to exploit a vulnerability
- Kinds of attacks
    - Passive (e.g., eavesdropping)
    - Active (e.g., password guessing)
    - Denial of Service (DOS)
        - Distributed DOS – using many endpoints

- A compromise occurs when an attack is successful
    - Typically associated with taking over/altering resources



```
(base) cyber2slab@cyber2slab-ThinkPad-T480:~/Documents
/src$ 
```

Principals

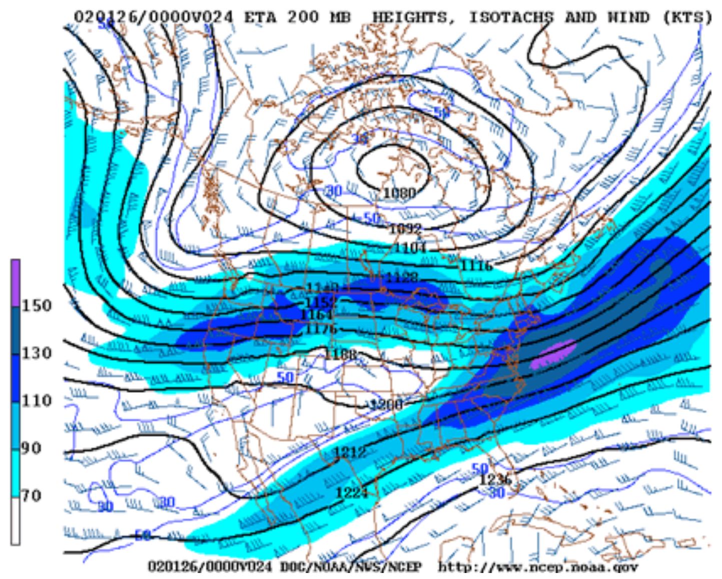
- Principals are expected system subjects
  - Computers, agents, people, enterprises, …
  - Depending on context referred to as: servers, clients, users, entities, hosts, routers, … - and some may be adversarial
  - Security is defined with respect to these subjects
    - Implication: every principal may have unique view
- A trusted third party
  - Trusted by all principals for some set of actions
  - Often used as introducer or arbiter

Trust

- Trust refers to the degree to which a principal is expected to behave
  - What the principal not expected to do?
    - E.g., not expose password
  - What the principal is expected to do (obligations)?
    - E.g., obtain permission, refresh
- A trust model describes, for a particular environment, who is trusted to do what?
- Note: you make trust decisions every day
  - Q: What are they?
  - Q: Whom do you trust?

Security Model

- A security model is the combination of a trust and threat models that address the set of perceived risks
  - The "security requirements" used to develop some cogent and comprehensive design
  - Every design must have security model
    - LAN network or global information system
    - Java applet or operating system
- This class is going to talk a lot about security models
  - What are the security concerns (risks)?
  - Who are our adversaries?
  - What are the threats?
  - Who do we trust and to do what?
- Systems must be explicit to be secure.


020126/0000V024 ETA 200 MB HEIGHTS, ISOTACHS AND WIND (KTS)
150
130
110
90
70
1080
1092
1104
1116
1128
1140
1152
1164
1176
1188
1200
1212
1224
1236
30
50
020126/0000V024 DOC/NOAA/NWS/NCEP http://www.ncep.noaa.gov

A Security Model Example

- Assume we have a University website that hosts courses through the web (e.g., Canvas)
  - Syllabus, other course information
  - Assignments submissions
  - Online grading

- In class: elements of the security model
  - Principals (Trusted)
  - Adversaries
  - Risks
  - Threats

PENNSTATE
Penn State's Course Management System
a new Global environment for learning

The Security Mindset

- Thinking like an attacker
  - Understanding how to circumvent security
  - Look for where security can fall down
- Thinking like a defender
  - What are you defending and from whom
  - Weigh benefits vs. costs: No system is ever completely secure!

Acknowledgement: Materials for the class lectures are taken from Trent Jaeger (Penn State), Ninghui Li (Purdue), Christina Garman (Purdue), and William Enck (NCSU).