CS 6501 Defense Against the Dark Arts

Jack W. Davidson (aka DrD, aka Dumbledore)
Michele Co (aka DrC)
Abbas Naderi Afoosheth (aka AbiusX)

Spring, 2018

Class Information

- Prerequisites: Be able to write substantial C/C++ programs and read x86 assembly language
- Three exams (15% each, low score dropped)
- Semester project (30%)
- Assignments, including programming assignments (40%)
- The percentages may be adjusted depending on the number of assignments and quizzes

Class Information

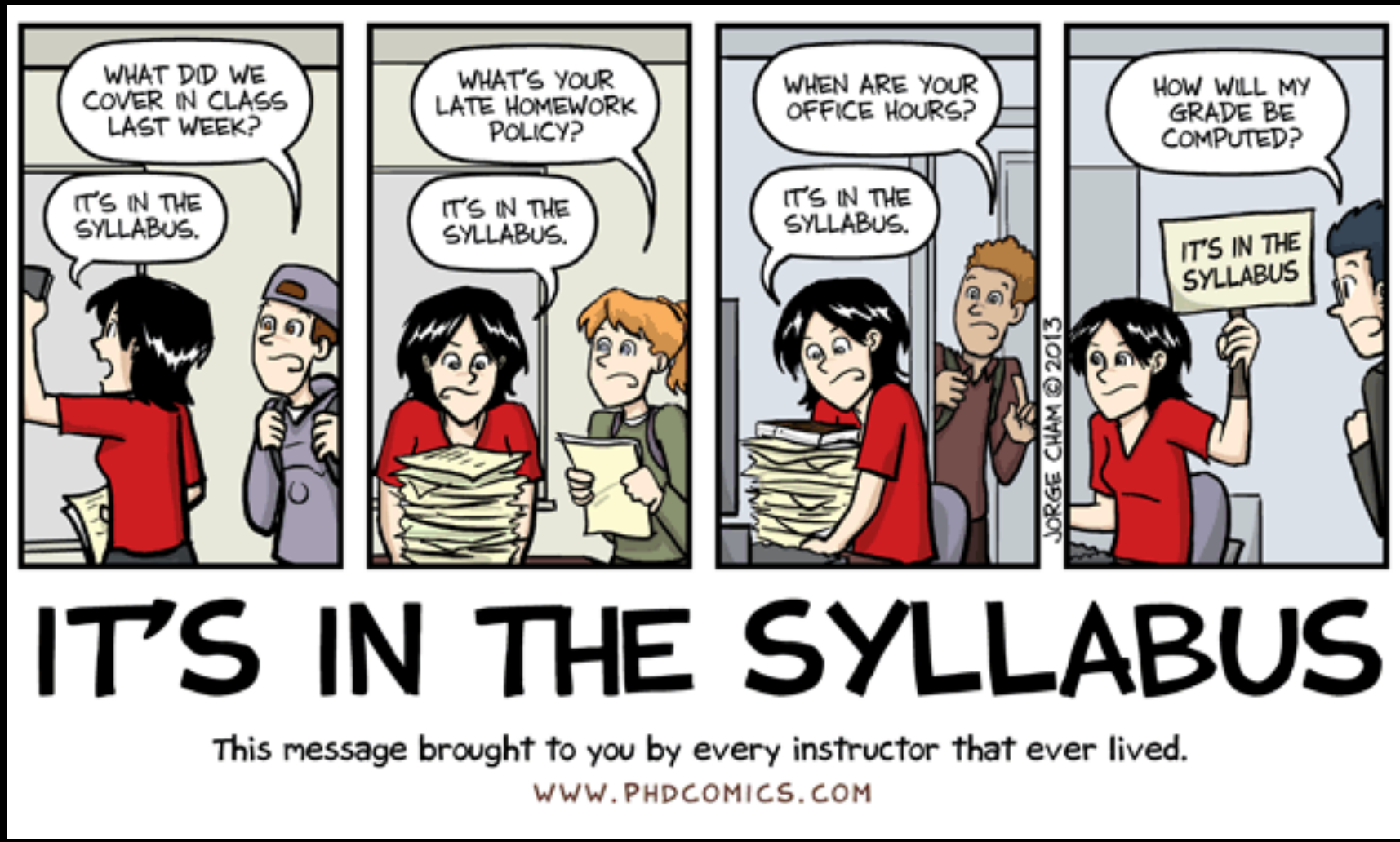
- No textbook required. We will be reading papers.
- Other resources listed in the beginning-of-course memo could prove useful
- Late homework penalty is 10%
  - If it is more than one class period late, the assignment will not be accepted
- Office Hours –

  Prof. Davidson – Tuesdays, 1:30 pm–2:30 pm and by appointment

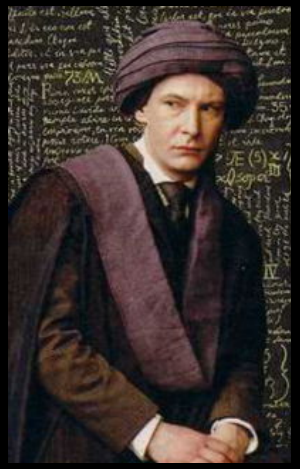
  Michele – Mondays, 2:30 pm–3:30 pm and by appointment

  Abbas – Mondays and Wednesdays 12:15 pm-1:15 pm

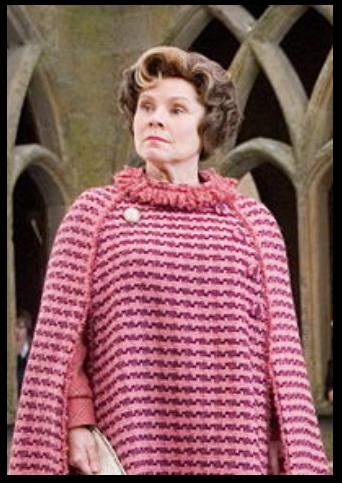
Syllabus—It is your friend



Quiz

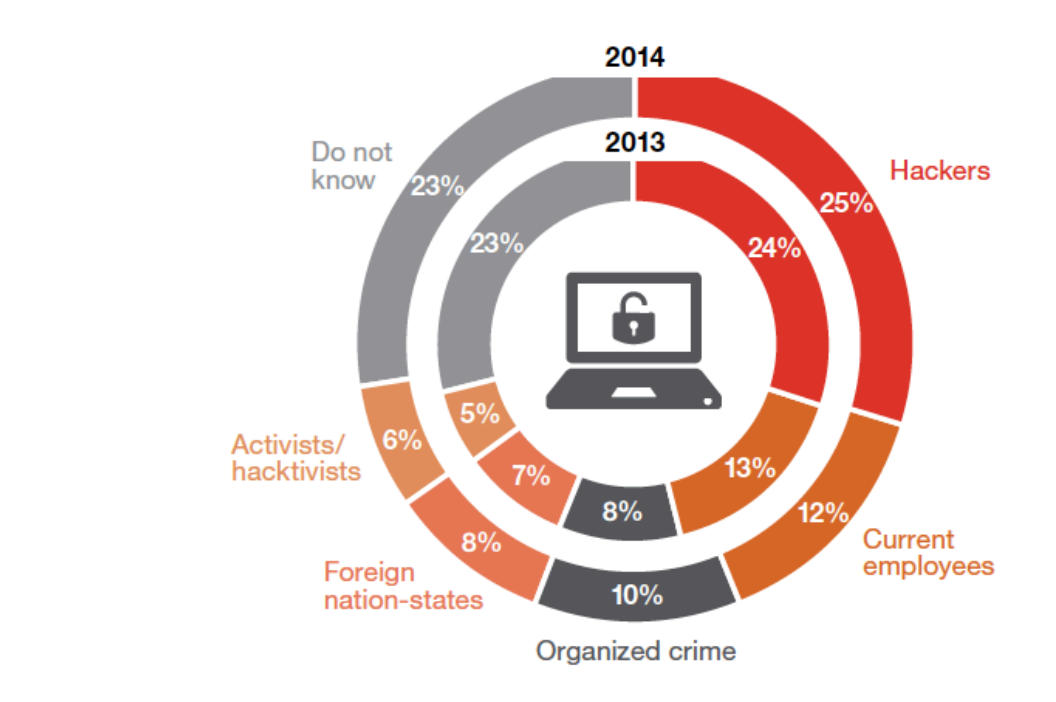






Economic Costs of Computer Malware

- Cyber crime costs the U.S. more than $110B according to the Center for Strategic and International Studies



- Companies often cover up the worst cases
- Does not include cost of security measures

Global Cost is Increasing Rapidly
(Wired.com, 2017)

- In early 2015 Inga Beale, CEO at the British insurer Lloyd's, claimed that cybercrime was costing businesses globally up to $400 billion a year.
- Juniper Research released a report which said cybercrime will cost businesses over $2 trillion by 2019.
- Microsoft CEO Satya Nadella stated $3 trillion of market value was destroyed in 2015 due to cybercrime
- Worldwide spending on cybersecurity is predicted to top $1 trillion for the five-year period from 2017 to 2021 (Cybersecurity Market Report)

Virus Costs: Chernobyl

- 26-April-1999 time bomb: “Chernobyl”
- Wrote random garbage all over the hard disk until the PC crashed
- $250 million lost in one day in Korea alone; widespread across Asia
- Hard to quantify cost of lost files, time spent reinstalling OS and applications, etc.

Things are Bad

We Still Don't Know Who Hacked Sony

Welcome to a world where it's impossible to tell the difference between random hackers and governments.

Davide Restivo/Flickr

TEXT SIZE

BRUCE SCHNEIER | JAN 5, 2015 | GLOBAL

If anything should disturb you about the Sony hacking incidents and subsequent denial-of-service attack against North Korea, it's that we still don't know who's behind any of it. The FBI said in December that North Korea attacked Sony. I and others have serious doubts. There's countervailing evidence to suggest that the culprit may have been a Sony insider or perhaps Russian nationals.

HBO Hacked – 'Game of Thrones' Scripts & Other Episodes Leaked Online

Monday, July 31, 2017 Swati Khandelwal

Tweet Share 44 Share 47 Share 1.21k Share 7.98k Share

If you are a die heart fan of 'Game of Thrones' series, there's good news for you, but obviously bad for HBO.

Hackers claim to have stolen 1.5 terabytes of data from HBO, including episodes of HBO shows yet to release online and information on the current season of Game of Thrones.

What's more? The hackers have already leaked upcoming episodes of the shows "Ballers" and "Room 104" on the Internet.

Things are Bad

BUSINESS

Anthem: Hacked Database Included 78.8 Million People

Health insurer says data breach affected up to 70 million Anthem members

By ANNA WILDE MATHEWS

Feb. 24, 2015 2:49 p.m. ET

Health insurer Anthem Inc. said the database that was penetrated in a previously disclosed hacker attack included personal information for 78.8 million people, 60 million to 70 million of its own current and former customers and employe

BARCLAYS

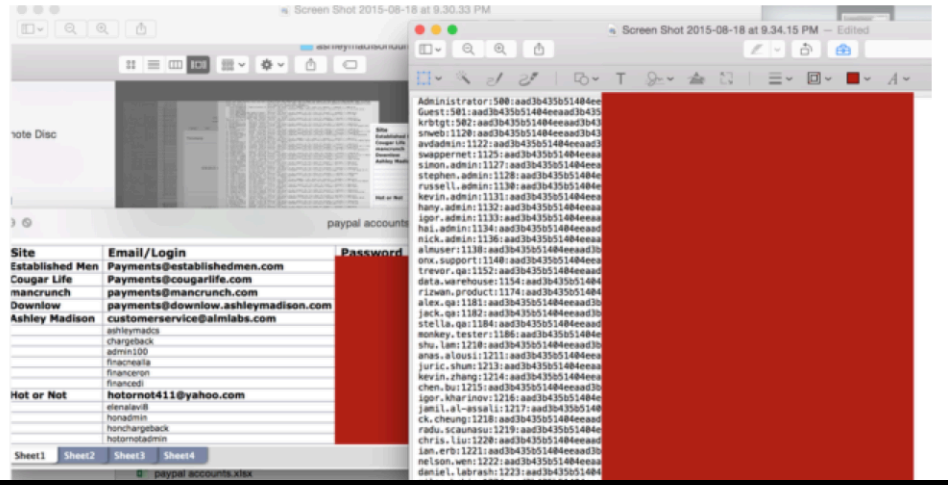
RISK ASSESSMENT / SECURITY & HACKTIVISM

Ashley Madison hack is not only real, it's worse than we thought

Intimate data for more than 30 million accounts, keys to Windows domain published.

by **Dan Goodin** - Aug 19, 2015 2:22am EDT

Share Tweet Email 385



Things are Bad

Hospitals in Chino, Victorville See Systems Hacked and Ransom Demanded

POSTED 6:25 PM, MARCH 22, 2016, BY LOS ANGELES TIMES

Two more Southern California hospitals have been attacked by hackers who infiltrated their computer systems with ransomware and demanded payment to unlock the data, officials said.

Chino Valley Medical Center is shown in a Google Street View image.

Chino Valley Medical Center in Chino and Desert Valley Hospital of Victorville, both part of Prime Healthcare Services Inc., had their computer system compromised on Friday by a cyber attack. The cases are now part of an ongoing FBI probe, bureau spokeswoman Laura Eimiller said.

According to sources familiar with the ongoing investigation, the hackers got into one of the hospital's computers and then spread a malware program that encrypts the data on computers. The hackers then demanded a ransom, typically in a cyber currency, to unlock the servers, according to the sources.

A similar hack occurred this year at Hollywood Presbyterian Hospital, and the hospital paid about $17,000 in bitcoins to get the keys back to its computer servers.

Click here to read the full story on LATimes.com.

Now your car!

Top DOJ official worries about cars being hacked

By Wesley Bruer, CNN
Updated 3:19 PM ET, Tue April 12, 2016

Hackers 'stole a master key' to U.S. government 02:17

Story highlights

Car-based internet provides a tempting target for hackers

So says a top Justice Department official

Washington (CNN) — About 75% of new cars will be equipped with online connectivity by 2020 and will be vulnerable to hackers, Assistant Attorney General John Carlin said Tuesday.

"The same innovations that revolutionize the auto industry create vulnerabilities if not carefully deployed. Connectivity creates access. Potential access to vehicle control systems could be used against us to undermine the very safety the technology was designed to provide," said Carlin, who was speaking at a Society of Automotive Engineers event in Detroit.

Last month, the FBI, along with the Department of Transportation and the National Highway Traffic Safety Administration, released a public service announcement warning that cars are becoming "increasingly vulnerable to remote exploits" through USB, Bluetooth or Wi-Fi technology in the vehicle. The announcement warns that not only is any data shared on the vehicle's computer susceptible, even more alarming is the possibility of having your car exploited remotely that could allow someone the "ability to manipulate critical vehicle control systems," the announcement said.

The possibility of a hacker breaching a car's technology to gain control of its operations came to light after two security researchers, Charlie Miller and Chris Valasek, hacked into the connectivity of a Jeep Cherokee and demonstrated they were able to remotely hit the brakes, drive the car off the road or make electronics go haywire. That hack led to a recall of nearly 1.5 million vehicles.

Top stories

MMA fighter dies fro injuries

Air Force F-22s deplo England

Advertisement

Close to Home

NEWS

Oak Ridge National Lab shuts down Internet, email after cyberattack

DOE laboratory says it was victim of an Advanced Persistent Threat designed to steal technical data

By Jaikumar Vijayan FOLLOW

Computerworld | Apr 19, 2011 7:30 PM PT

RELATED TOPICS

Cybercrime & Hacking

Security

Data Security

COMMENTS

INSIDER

Crash Course: Mastering Evernote as groupware

This free download has oodles of tips and advice for business users of this handy content storage and

READ NOW

The Oak Ridge National Laboratory, home to one of the world's most powerful supercomputers , has been forced to shut down its email systems and all Internet access for employees since late last Friday, following a sophisticated cyberattack.

The restrictions on Internet access will remain in place until those investigating the attack know for sure that it has been completely contained, said Barbara Penland, ORNL's director of communications.

The lab is expected to restore external email service sometime on Wednesday, however no attachments will be allowed for the time being.

Penland said several other national laboratories and government organizations were targeted in the same attacks, which appear to have been launched earlier this month.

The measures at Oak Ridge were implemented late on Friday night after initial investigations showed that those behind the attacks were attempting to steal technical data from lab's systems and send it to an external system, Penland said.

So far, though, it appears that no significant amount of data has been stolen. Penland said investigators believe that whoever was behind the attacks managed to steal less than 1GB of data.

MORE LIKE THIS

on IDG Answers

Why is there less spam than before?

Software-Defined WAN for Dummies

Best Practices, Benefits, ROI

Free Download

Home!

Anatomy of a hack: Examining Root The Box's attack on UVA's website

This screenshot from UVA third-year Andrew Kouri's computer shows last week's UVA homepage hack in real time.

News

Graelyn Brashear

4/23/13 at 12:18 PM

Last week's high-profile defacing of UVA's website may not have led to a serious security breach, despite threats of e-mail infiltration and stolen data by two hackers calling themselves "Root the Box" who took to Twitter to boast and threaten during a 24-hour battle with University Information Technology Services. But it definitely got peoples' attention—in Charlottesville and beyond—and sparked a conversation about how we secure schools' online information.

"It was certainly not a sophisticated attack on UVA's website by any means," said third-year computer science major Andrew Kouri, who managed to conduct a chat interview with the pair of hackers. "In fact, I'd like to think that most CS students here could figure out how to exploit the vulnerability if they actually cared enough to do so."

"We hacked it because we can," Root The Box wrote back. "For fun, and because of the University's lack of security. That sums it up." They later implied the hack was in part in response to a $40,000 Virginia Innovation grant awarded to three UVA researchers last month to develop patented code that would increase Web security. The computer scientists, who aren't part of ITS, "don't deserve their award," they wrote.

Home!

WAHOOS 08.21.15 9:20 AM ET

WRITTEN BY

SHANE HARRIS

ALEXA CORSE

Chinese Hackers Target U.S. University With Government Ties

The cyberattacks on the University of Virginia were not targeting systems but individuals.

A prominent American university with ties to the Defense Department and intelligence agencies is the latest target of Chinese hackers.

Last week, the University of Virginia, located in Charlottesville, about a three-hour drive from Washington, D.C., announced that it had suffered an intrusion "originating from China" that led the school to shut down portions of its technology systems and required students and faculty to reset their passwords used for accessing email and other applications hosted on the school's systems.

But unlike some China-based intrusions that attempt to steal personal information such as Social Security and financial account numbers from large numbers of people, this one targeted two university employees "whose work has a connection to China," university spokesperson Anthony P. de Bruyn told The Daily Beast.

Home! (Again)

‘Phishing’ hack at the University of Virginia compromises employee computer records

A | 16 | Save for Later | Reading List

By T. Rees Shapiro January 22 Follow @TReesShapiro

The campus of the University of Virginia, in Charlottesville, Va. (Photo by J. Lawler Duggan/For The Washington Post)

Hackers accessed numerous computer records containing personally identifiable information belonging to University of Virginia employees, part of a “phishing” scam that also included some bank records, school officials announced Friday.

Most Read

Cyber Espionage

Hacks of OPM databases compromised 22.1 million people, federal authorities say

A | 848 | Save for Later | Reading List

By Ellen Nakashima July 9, 2015 Follow @nakashimae

Hackers stole personal information about at least 22.1 million people, including addresses, mental health and criminal records, in two major breaches of U.S. government databases. (WUSA9)

Two major breaches last year of U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends, U.S. officials said Thursday.

Cyber Espionage

Home / USA /

United Airlines 'hacked' by group likely responsible for OPM breach – report

Published time: 30 Jul, 2015 23:57
Edited time: 31 Jul, 2015 00:45

Get short URL

© Eduardo Munoz / Reuters

Malware Costs: Conclusion

- Malware and other security attacks are very costly
- Computer security is a hot field today; many career and research opportunities for graduates from this course
- Knowledge of security issues is sensitive and carries an ethical responsibility with it

With Great Power Comes Great Responsibility

- Knowledge of security issues is sensitive and carries an ethical responsibility with it
- We must teach attacks upon computer systems in order to teach defenses against attacks
- Information about attacks must NEVER be used to attack any computer system in any way

Ethics Pledge

- Read and sign ethics pledge
- Should not be difficult to follow
- Ethics will be covered in more detail later
- You cannot continue in the course without signing the ethics pledge!

Ethics Pledge Points

- Unauthorized use of computer resources is forbidden
- Even a virus or worm that does nothing but copy itself uses resources
- Don't ever rationalize that a system owner won't object to your actions; ask permission
  - If you are afraid to ask permission, it must be forbidden!

Example: 1988 Morris Worm

- Creator rationalized that the worm did no damage; it only copied itself from system to system over the internet
- BUT: Copying monopolized system resources until they had to be shut down
- Worm reached 10% of entire internet
- Creator did not realize it would be that resource-intensive
- Creator was convicted of felonies!

Morris Worm Lessons

- Consequences of a virus or worm cannot always be foreseen
- Severe damage can be done without destroying data
- Excessive resource usage is destructive enough to be criminal

Criminal Prosecution

- Attackers have been prosecuted for:
  - Stealing passwords, even if never used
  - Copying copyrighted materials
  - Accessing confidential data, even if it was never used for harmful purposes
  - Entering a system without permission, causing sys admins to spend time tracking them and securing the system, even without otherwise causing harm
- Moral: Don't assume it is legally safe to do any of the above

Ethics Violations

- Violations by students endanger our ability to offer this course
- As a result, they will be treated severely
  - UJC (University Judiciary Committee)
  - Course grades
  - Criminal prosecution

ACM Code of Ethics

- ACM is the primary professional organization for computer scientists
- The entire code is available online
- Portions most applicable to students are excerpted in the handout
- See full statement here.

Ethics Questions

- Scenario: Jane Doe attempts to guess the password of a user of a system on which JaneDoe has no account. After a few guesses, she succeeds, but finds nothing of interest on the system and logs off.
- Q1: Has she committed a crime?
- Q2: Are heractions analogous to any common crime not involving computers?

Michele Co

- Research Scientist, UVA
- Lecturer, UVA
  - Intro to Computing
  - Data Structures
  - Computer Architecture
- Masters (2003) and Ph.D. (2006), C.S., UVA
  - Computer architecture – Energy-efficiency of branch predictor architectures (micro-architecture)
- B.A. (long time ago), C.S. (Chinese Studies), University of California, Berkeley

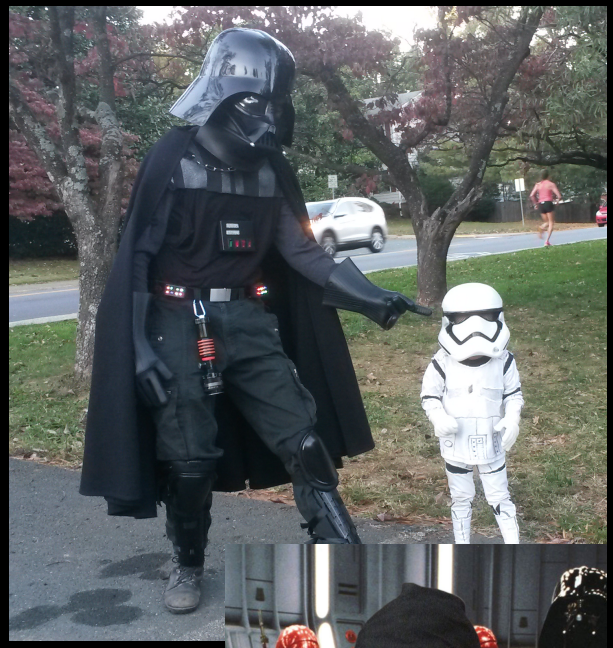
Michele Co: Recent and Current Projects

- Research projects
  - NICECAP
    - Software memory protection using software dynamic translation
  - IARPA STONESOUP
    - Preventing Exploits Against Software of Unknown Provenance (PEASOUP)
  - DARPA Cyber Grand Challenge
    - Autonomous system to analyze and protect unknown binary software
  - DARPA Cyber Fault-tolerant Attack Recovery (CFAR)
    - Double Helix

Michele Co – Research Interests

- Tradeoffs
  - Power vs. performance
  - Security vs. speed vs. memory consumption
  - Design space exploration
  - Secrecy of code vs. openness of code, data, information
- Impact of Technology on Society
  - Software security of systems we rely on
  - Workforce
  - Medical technology

Michele Co - Personal



- Interesting stuff
  - Family: 5 yr old son
  - Travelled during interesting times:
    - USSR (1987), PRC (1989-1990)
  - Sports:
    - Judo: 1st degree black belt
    - Mountain biking: completed SM 100
    - Running: Bay to Breakers and NYC Marathon
  - Chased the solar eclipse in Charleston, SC!!!

`whoami`

- Abbas Naderi
  online alias: abiusx
- Professional Hacker for 11+ years
- Security Researcher for 6+ years
  Presentations at all major security conferences
  Membership of all major security groups
- Founder of 2 successful startups
- 5th year PhD student under the supervision of Prof. Jack Davidson

`whoami`

- Research Activities
  - Web Application Security
  - Analysis of Dynamic Programs
  - Hybrid Taint Inference
- Professional Activities
  - Gamer
  - Open Source contributor
  - Full-time Husband
- What I did this summer
  - I had an internship at Google working on ChromeOS Kernel (containers secure file-system)

Me

- Professor of Computer Science, University of Virginia
  - Joined the faculty in 1982.
  - Spent time at Princeton University and Microsoft Research
- Ph.D., University of Arizona, 1981
- Research Activities
  - Two areas: compilers, security and computer architecture
  - Currently the PI of a large DARPA security project call CFAR (more about it later in the semester)
  - Also PI of an AFRL project, Trusted and Resilient Mission Operation

Me

- Research Activities (continued)
  - Current interests:
    - Iterative compilation
    - Software Dynamic Translation
    - Software Security

- Educational Activities
  - Wrote two introductory programming textbooks
  - Currently developing security curriculum sequence
    - Anti-virus course, network security, program analysis
    - Using Microsoft Phoenix infrastructure
    - Funded by NSF

Me

- Professional Activities
  - Past Chair of SIGPLAN Executive Committee
    - Sponsors major PL conferences: PLDI, OOPSLA, ICFP, POPL, ISMM, VEE
    - Provides funds for students to attend SIGPLAN-sponsored conferences
  - Member of ACM SIG Governing Board (SGB)
  - Co-chair of ACM Publications Board
  - Member of ACM Council
  - Serve on lots of Program Committees: LCTES, CASES, HiPEAC, PLDI, POPL, CGO

Me

- Fun stuff
  - Avid mountain biker
  - Hiking, backpacking, canoeing
- What I did this summer
  - I taught a summer school in Paris! Oo la la!

Paris

Roll Film!

- Hollywood's View
- DARPA Cyber Grand Challenge

You

- Tell us about yourself
  - Where you are from
  - Your interests (e.g., major, career goals, etc.)
  - What you hope to get out of this course
  - One fun or interesting thing about yourself