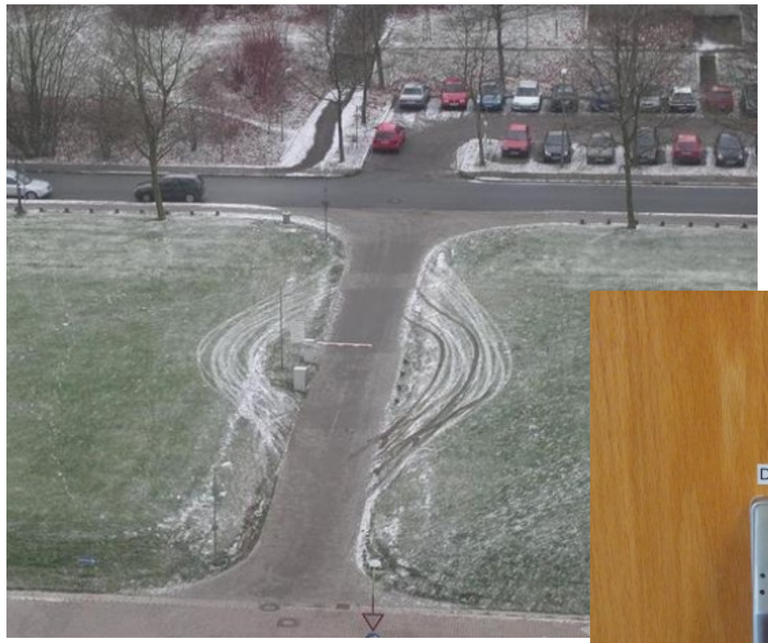
Introduction to Computer Security (Part I)

Professor Travis Peters
CSCI 476 Computer Security
Spring 2020

So what are we doing here?

- Learning to think about security!



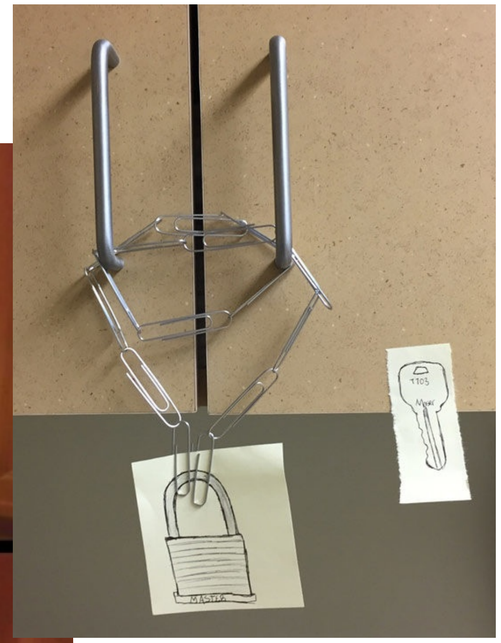


Photo credits: https://brightside.me/wonder-curiosities/20-ridiculous-security-fails-that-are-too-good-to-be-true-426810/

OK, OK, HA HA. So what *is* security?

Think-Pair-Share Activity:

You Tell Me!

What is security?

What is security ***not***?

Popular examples?

Examples you've encountered (recent or past)?

The Standard Rubric: C.I.A. *a.k.a The CIA Triad*

Confidentiality *> the system does not reveal data to the wrong parties*

Integrity *> data the system stores does not get changed in inappropriate/illicit ways*

Availability *> the right parties can always use the system when they need it*

- Is this definition sufficient?
  - Is each property equally important? (Examples?!)
  - Authenticity / Non-repudiation (CIAA) *> inability to deny a commitment to do something/having done something*
  - *There are many others…*

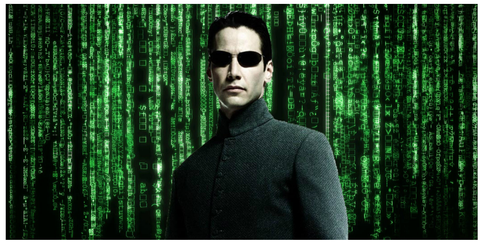
- Oft used to describe requirements for ***information security*** *(InfoSec) /* ***data security***

- What about other types of security?
  - Physical security?
  - Critical infrastructure security?

The Craft of System Security - 1st Edition. Sean Smith (2007).

The Matrix

- No, no… not *that* Matrix



- The Access Control Matrix

  The idea: *prevent the wrong people from doing the wrong things within a system*

  - specify what are the objects,

  - who are the subjects, and

  - what subjects can do to which objects

SYSTEM

SUBJECTS	OBJECTS: File 1	File 2	File 3	File 4
User A	Own Read Write		Own Read Write	
User B	Read	Own Read Write	Write	Read
User C	Read Write	Read		Own Read Write

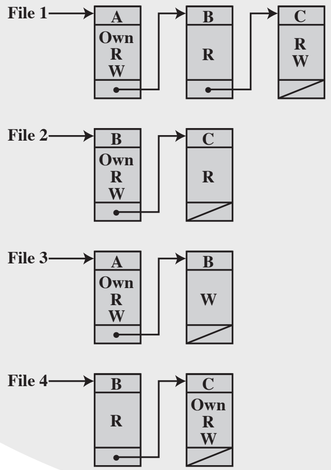
For each subject → easy to look up their capabilities

For each object → easy to look up authorized users

Simpler:

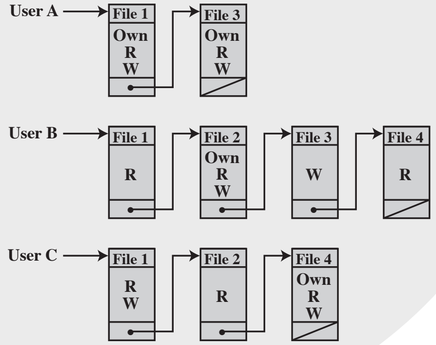
"Access Control List (ACL)"

objects → subjects



"Capabilities" List

subjects → objects



SYSTEM

So…

- Is our system secure?
  - CIA?
  - Access Control Matrix / Access Control Lists / Capabilities Lists?

- Maybe better questions are:

*Given a **model** of the threats to our system,*
how much of our resources should we expend
to mitigate the risk and impact of an attack?

*Who is the **adversary**? What **resources** do they have? What **capabilities** do they have?*

***Detect** or **Prevent**?*

*What's the **cost**?*

In general, define the adversary and see whether the system can remain in a good state despite the adversary

The Take-Home Message

*Learning to **think** about security!*

At the end of the day, security is hard to define!

The security & privacy field is always evolving:

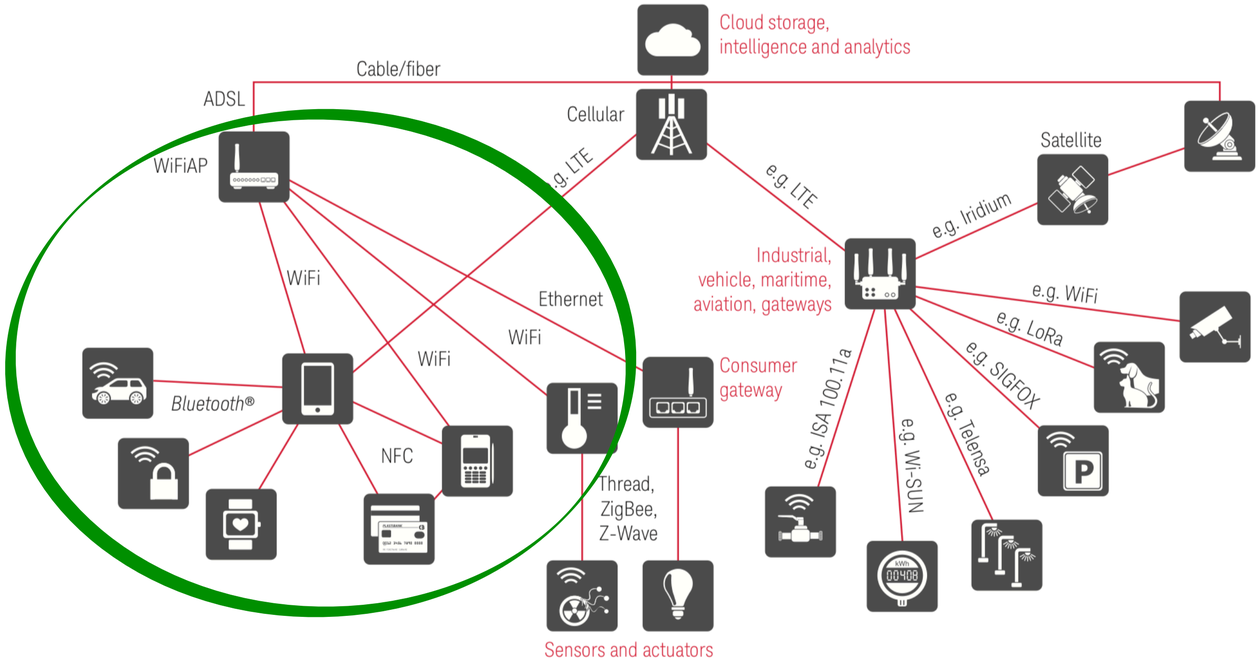
- new **assets**
- new **threats**
- new **capabilities**
- new **technologies**

You need to be ready to think through new situations that arise, leveraging what you've already learned (here, past experiences, case studies, reports, etc.) to find S&P solutions for those new situations.

Sounds intriguing! But uh… who *is* this guy?

- **Travis Peters (me)**
  - New prof @ MSU as of Fall 2019
  - Enthusiastic about helping other people learn about security!

- In my work, I mostly wear the hat of the "defender"
  - **wireless security** solutions for IoT, Wi-Fi, Bluetooth/BLE
  - **system security** solutions for mobile health devices, popular PCs
  - **data security** for sensitive user data



Key Insight Technologies, IoT Infogram - https://www.keysight.com/us/en/home.html

Also: The Age of Devastating Vulnerabilities

LILY HAY NEWMAN SECURITY 07.29.19 11:04 AM

AN OPERATING SYSTEM BUG EXPOSES 200 MILLION CRITICAL DEVICES

Think of how the WannaCry ransomware used the Eternal Blue Windows vulnerability to spread across networks and around the world. It's like that, but with firewalls, industrial equipment, and medical devices instead of Windows machines. The result could be anything from device malfunctions to full system takedowns.

MOTHERBOARD TECH BY VICE | By Kim Zetter | Mar 25 2019, 9:00am

Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers

The "solutions"…

TC

*"How do you stay safe? **Keep all of your devices updated** regularly and **be wary of older IoT devices**."*

THE VERGE

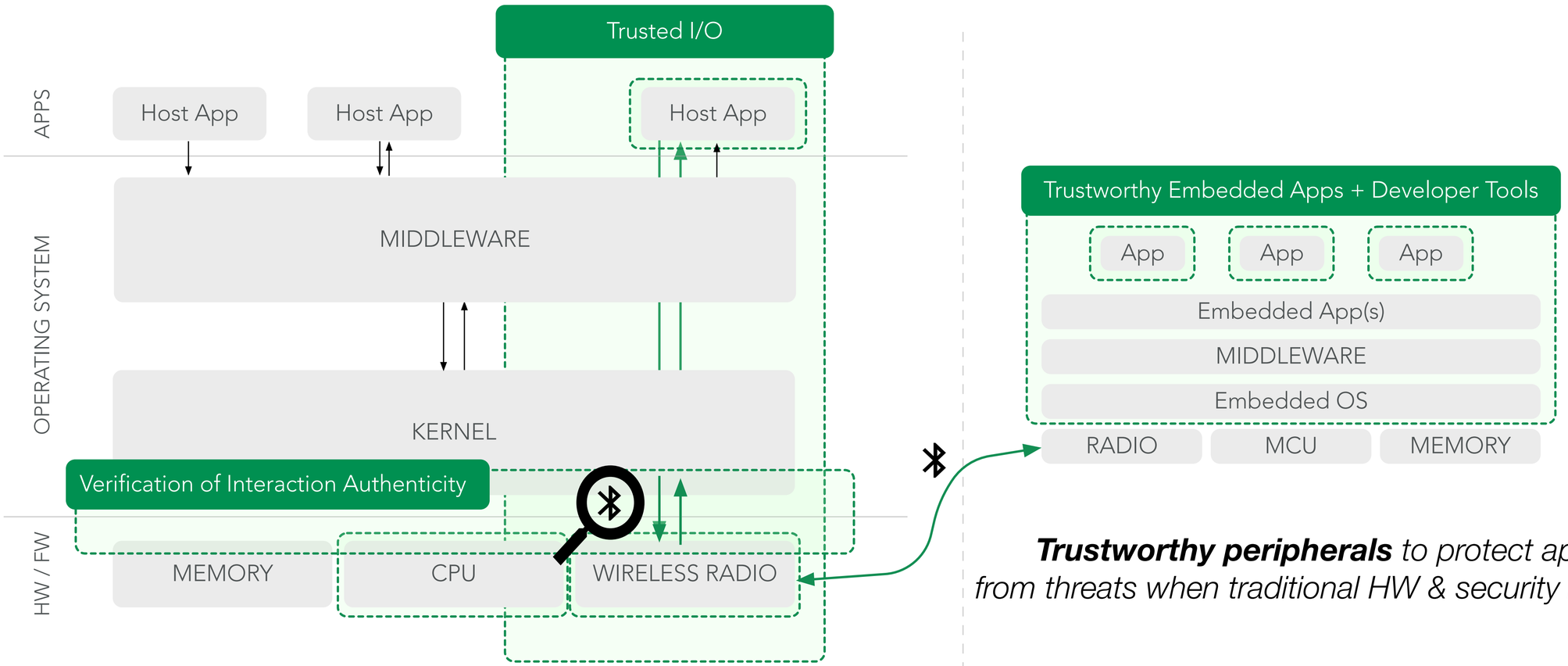
*"The simplest protection is to **leave Bluetooth off**, but since phones are still vulnerable when they're connected to a Bluetooth device, **the only recommendation is not to use Bluetooth at all**."*

There must be a better way….

My Research

Towards more trustworthy WPANs

Trustworthy I/O *to protect user data from privileged threats*



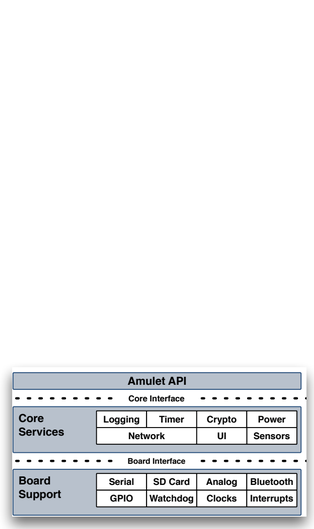
Trustworthy peripherals *to protect apps & data from threats when traditional HW & security is not available*

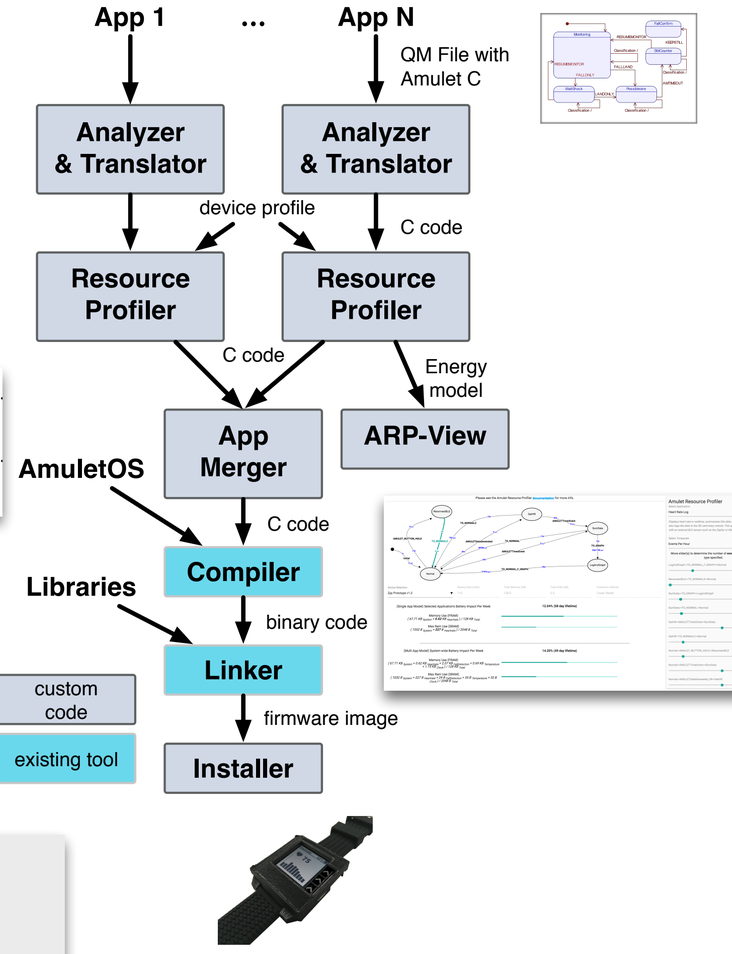
Verification of Trustworthy Interactions *to protect apps & devices over time*

Amulet

Better security for resource-constrained devices — "Security on a Budget"

- A secure & efficient mHealth platforms that
  - ***isolates apps*** through compile-time and run-time isolation mechanisms;
  - ***controls access*** to system resources through authorization policies;
  - ***profiles resource usage*** of apps through static analysis of code;
  - generates dynamic ***tool to aid applications developers***; *and*
  - merges applications & Amulet OS into a ***smaller, faster, more secure firmware image suitable for peripheral devices***.





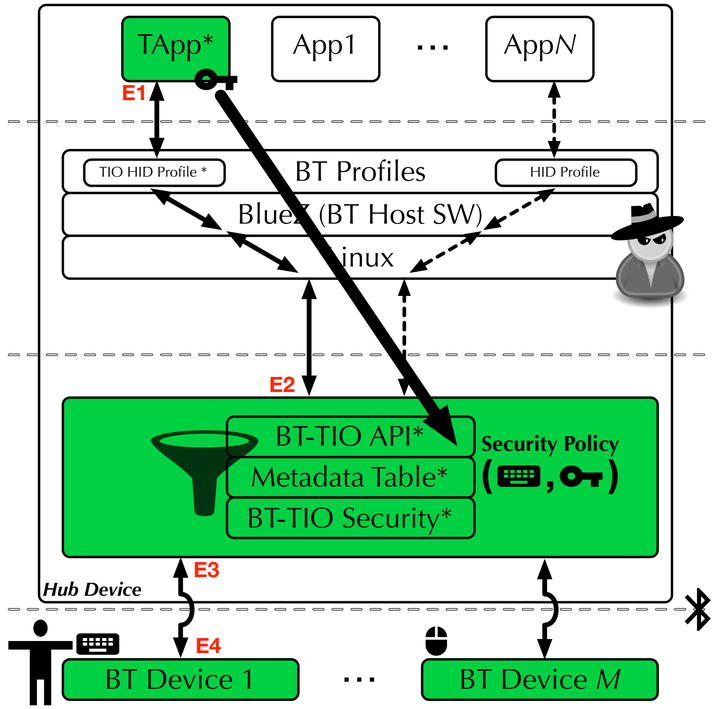
1. Josiah Hester, *Travis Peters*, Tianlong Yun, Ronald Peterson, Joseph Skinner, Bhargav Golla, Kevin Storer, Steven Hearndon, Kevin Freeman, Sarah Lord, Ryan Halter, David Kotz, Jacob Sorber. **Amulet: An Energy-Efficient, Multi-Application Wearable Platform**. Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys'16). November, 2016.

2. Andres Molina-Markham, Ronald Peterson, Joseph Skinner, Tianlong Yun, Bhargav Golla, Kevin Freeman, *Travis Peters*, Jacob Sorber, Ryan Halter, David Kotz. **Amulet: A secure architecture for mHealth applications for low-power wearable devices**. Proceedings of the Workshop on Mobile Medical Applications - Design and Development (WMMADD'14). November, 2014.

BASTION-SGX

Bluetooth and Architectural Support for Trusted I/O on SGX

- Achieved ***trustworthy app-device I/O*** through platform extensions rooted in Bluetooth Controller firmware that
  - unobtrusively collects per-channel metadata;
  - uses metadata to secure I/O data between app and Bluetooth Controller *without*…
    - relying on untrusted host software, or
    - requiring changes to SGX, Bluetooth device, or Bluetooth standard.
- Prototype and case study demonstrates effective mitigation of ***privileged keylogger,*** which cannot access user input data from connected Bluetooth device (keyboard).
- Analytical evaluation demonstrates acceptable impact to memory, latency, and throughput.



1. *Travis Peters*, Reshma Lal, Srikanth Varadarajan, Pradeep Pappachan, David Kotz. **BASTION-SGX: Bluetooth and Architectural Support for Trusted I/O on SGX**. Proceedings of the Workshop on Hardware and Architectural Support for Security and Privacy (HASP'18). June, 2018.

2. Srikanth Varadarajan, Reshma Lal, Steven B. McGowan, Hakan Magnus Eriksson, *Travis W. Peters*. **System, apparatus and method for providing trusted input/output communications**. U.S. Patent 10,372,656, August 2019.

3. *Travis Peters*. **A Survey of Trustworthy Computing on Mobile & Wearable Systems**. Dartmouth College Technical Report TR2017-823. May, 2017.

A few slides skipped here (unpublished work :-)

Sounds intriguing! But uh… who *is* this guy?

- **Travis Peters (me)**
  - New prof @ MSU as of Fall 2019
  - Enthusiastic about helping other people learn about security!

- In my work, I mostly wear the hat of the "defender"
  - **wireless security** solutions for IoT, Wi-Fi, Bluetooth/BLE
  - **system security** solutions for mobile health devices, popular PCs
  - **data security** for sensitive user data

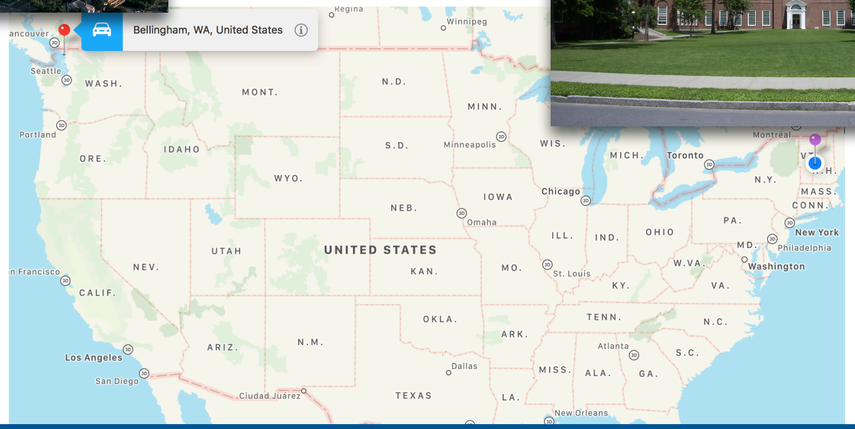
Check out my website for links to papers, etc. if you are interested :-)

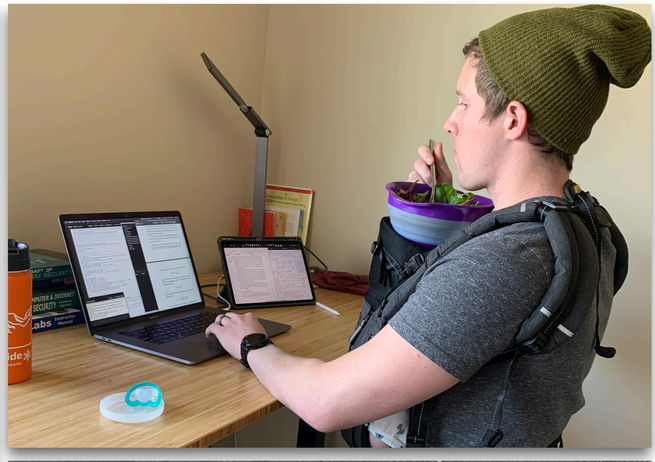
https://www.traviswpeters.com

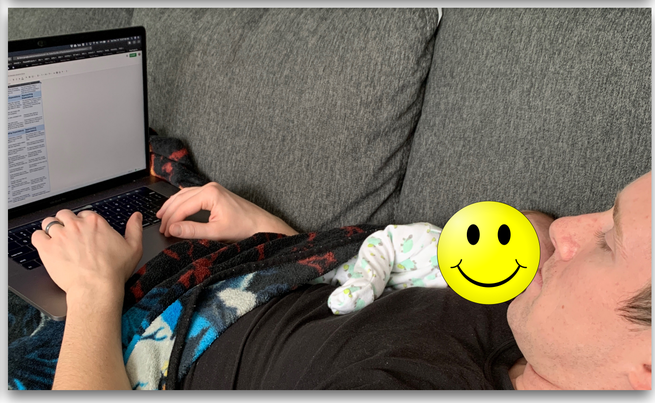
Key Insight Technologies, IoT Infogram - https://www.keysight.com/us/en/home.html

Sounds intriguing! But uh… who *is* this guy?

- Beyond the prof/researcher/security enthusiast…
  - A new dad! *(note: FMD this term…)*
  - I do other stuff too…
    - reading, running, biking, (amateur) woodworker, netflix, …
  - ugrad @ Western Washington University
  - grad @ Dartmouth







So what are we doing this semester? *The 30,000' View*

Introduction & Security Overview/Basics

- Basic concepts
- Linux security basics

Software Security

- Classics Attacks: : Set-UID attacks, env. variable attacks, buffer overflow attacks, format string attacks
- Recent Issues in SW: return-oriented programming, Shellshock attack

Network & Web Security

- SQL injection attacks
- sniffing & spoofing
- network attacks (e.g., TCP/IP)

Crypto

- symmetric & asymmetric cryptography
- Encryption & decryption
- digital signatures

System Security / Recent Topics

- Side-channel attacks

Admin Stuff

Course website:

https://www.traviswpeters.com/cs476/

Let's take a minute now to walk over a few important things…

- Office Hours
- Textbook
- Course Tools……..
- Grading
  - Labs (tentatively,
  - Final Exam
- Please bring laptops to class (at least on Thursdays). Please no using cellphones in class…
- Accommodations—talk to me and/or the appropriate office (notes, tests, etc.)
  - Note taking, anyone?!

Looking ahead…

Pro Tips

- Do the labs! AND START EARLY!
- Go to office hours — we aren't scary, and we are here to help! :-)
- Ask questions
- Try stuff!

For next time, think about…

- Note taking, anyone?
- Please be sure to fill out the **Questionnaire** (link on the website)
- Keep an eye out for **Lab 00** (setting up the work environment) — "due" next week
  https://www.traviswpeters.com/cs476/labs