CSE 484: Computer Security and Privacy

Emerging Tech + Wrap-Up

Fall 2021

David Kohlbrenner

dkohlbre@cs.washington.edu

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Admin

- **Lab 3** was due Wed
  - There were some unexpected issues with sploit1 no longer causing crashes for everyone
    - Only on attu
    - If this was a problem for you, let us know

- Final **project due** Mon, Dec 13 @ 11:59pm
  - No late days
  - Please let us know ASAP if there are any group, submission, etc. problems

Security Research

Its an odd field to work in!

- Covers everything:
  - How different groups of people use their smartphones
  - The effectiveness of airport bodyscanners at detecting firearms
  - Electromagnetic emanations from electronics
  - XSS on webpages
  - The spread of misinformation online
  - Adversarial attacks on computer vision

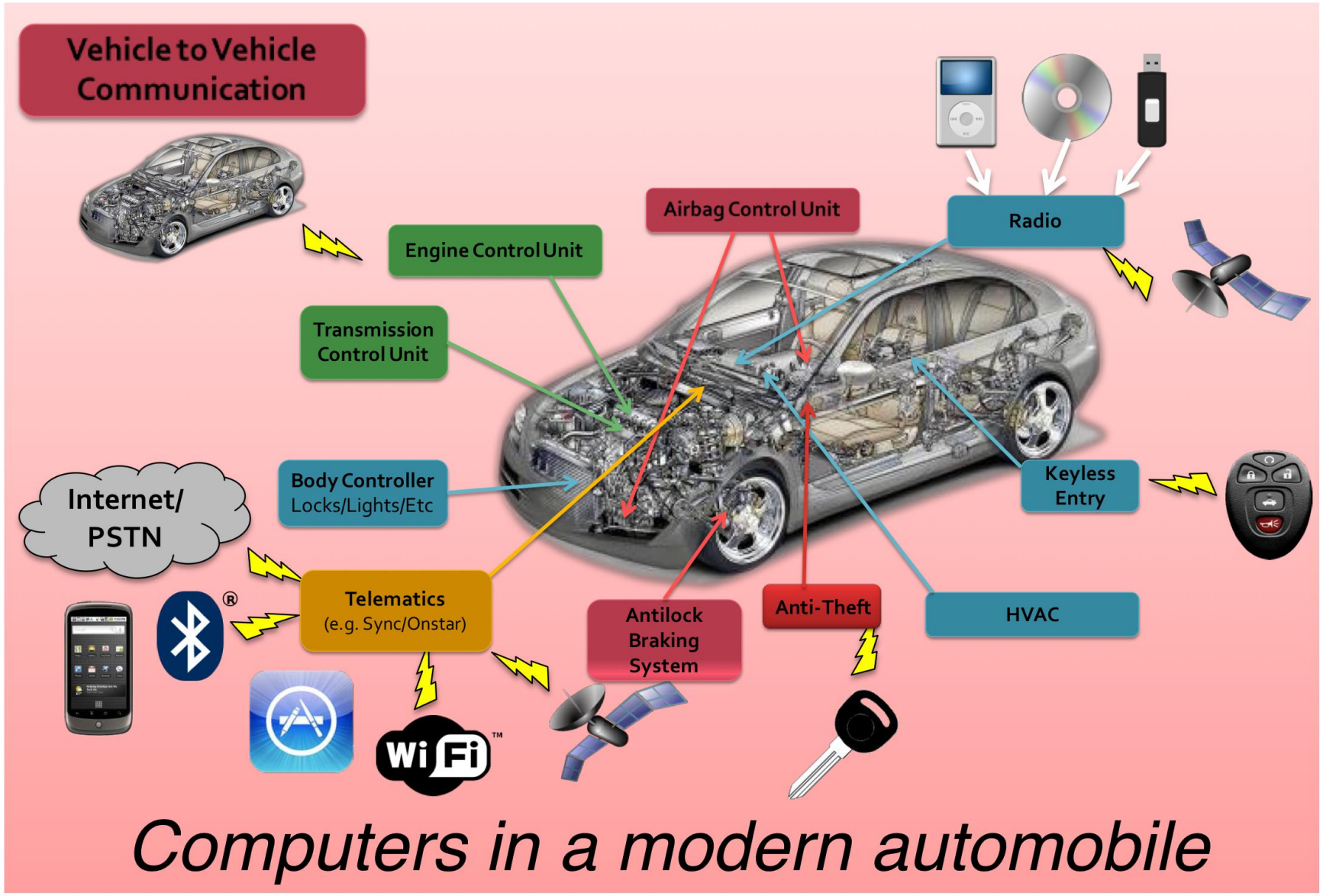
Security and Privacy For Emerging Technologies

(1) Connected Automobiles

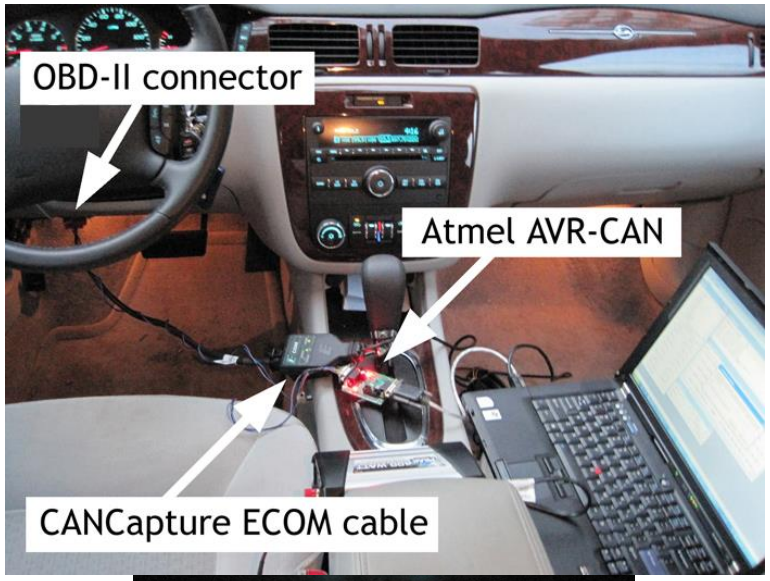
- Already emerged by now, but a fun story ☺

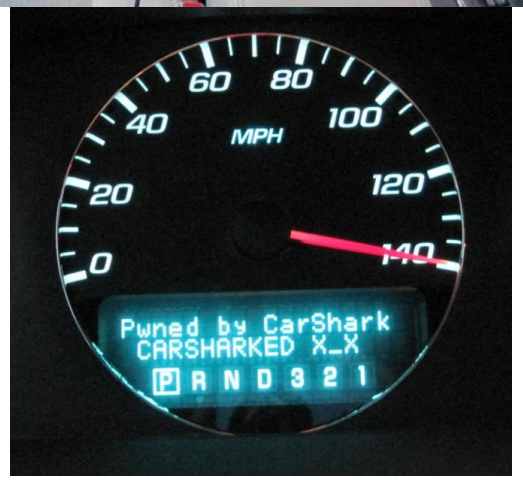
- Automobiles were only just being connected to the internet when UW+UCSD studied them (~2009)
  - Had not faced significant adversarial pressure
  - Won a "Test of Time" Award last year

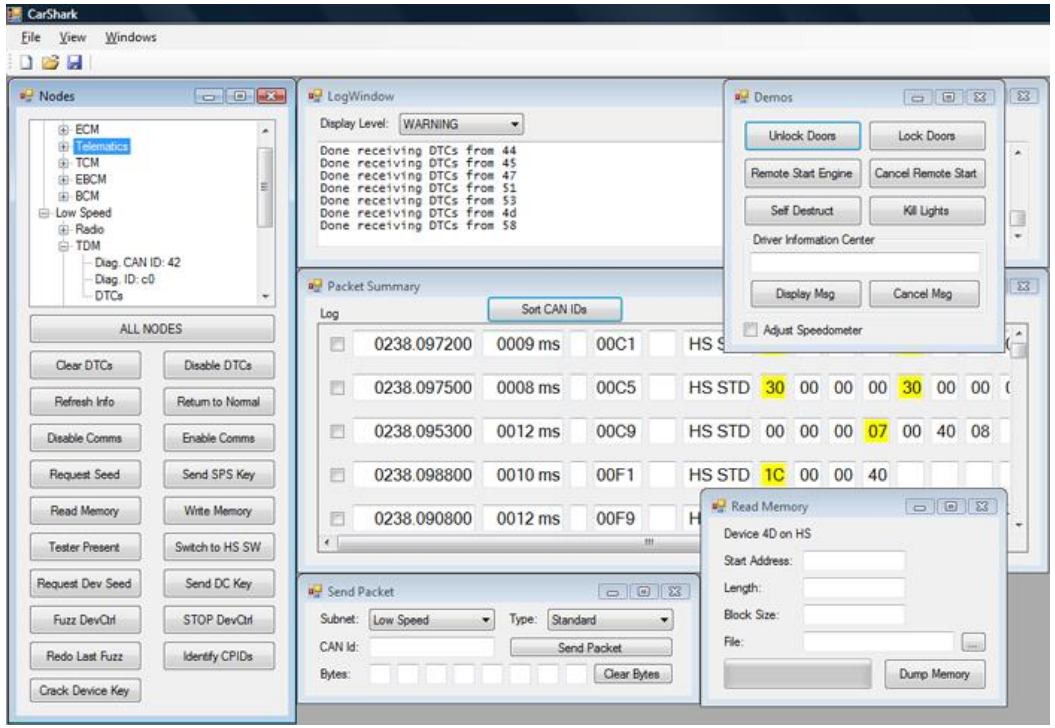
www.autosec.org


Vehicle to Vehicle Communication
Engine Control Unit
Airbag Control Unit
Radio
Transmission Control Unit
Body Controller
Locks/Lights/Etc
Keyless Entry
Internet/
PSTN
Telematics
(e.g. Sync/Onstar)
Antilock Braking System
Anti-Theft
HVAC
Wi Fi
Computers in a modern automobile

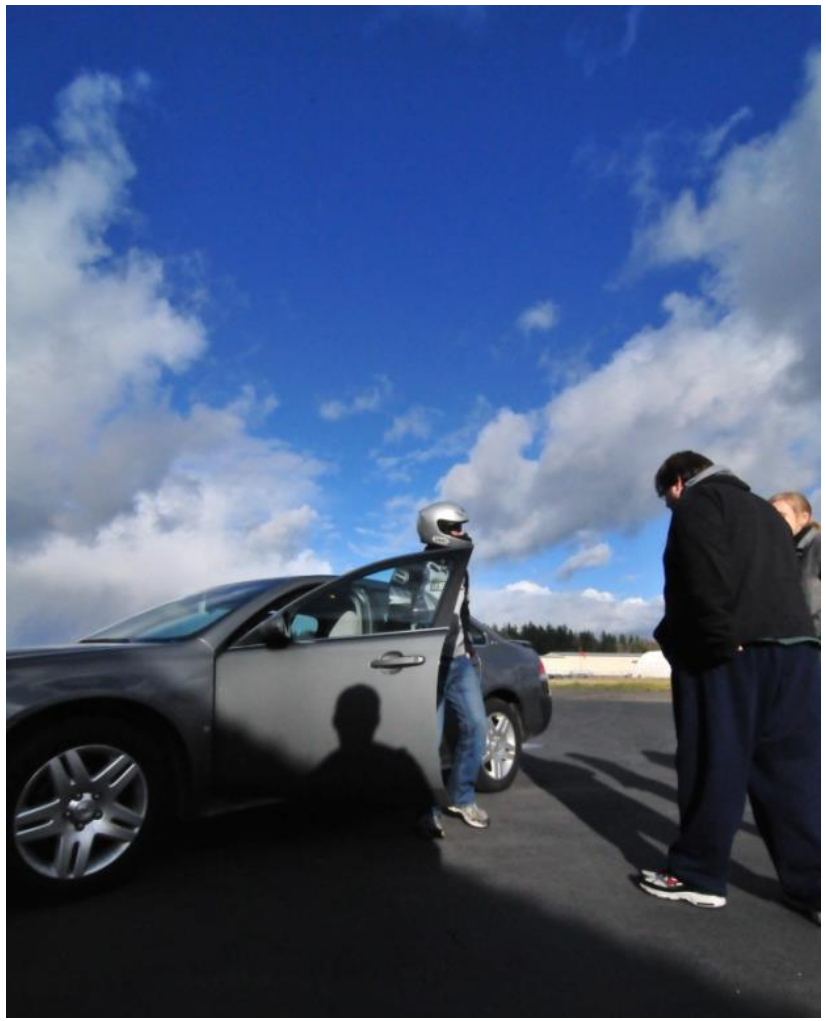
Experiments with a Real Car







Experiments with a Real Car



Example: Force Brakes On/Off

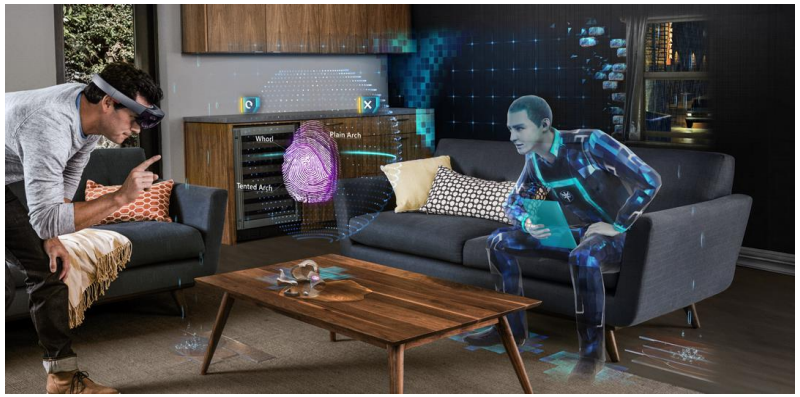
https://www.youtube.com/watch?v=H6o0zuid1K4

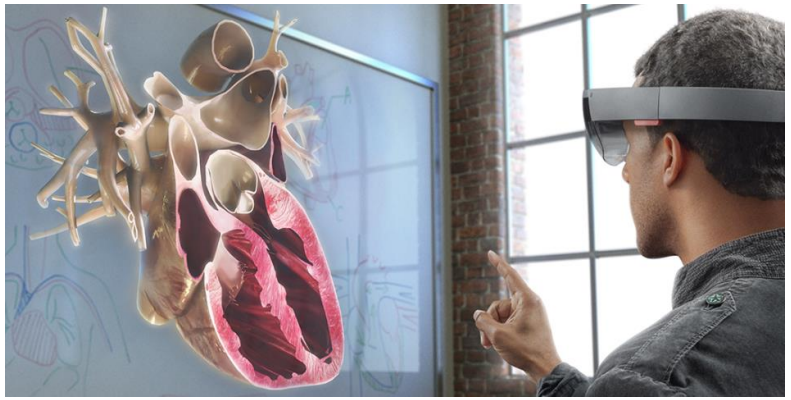
https://www.youtube.com/watch?v=917VOx6tBKA

Impacts

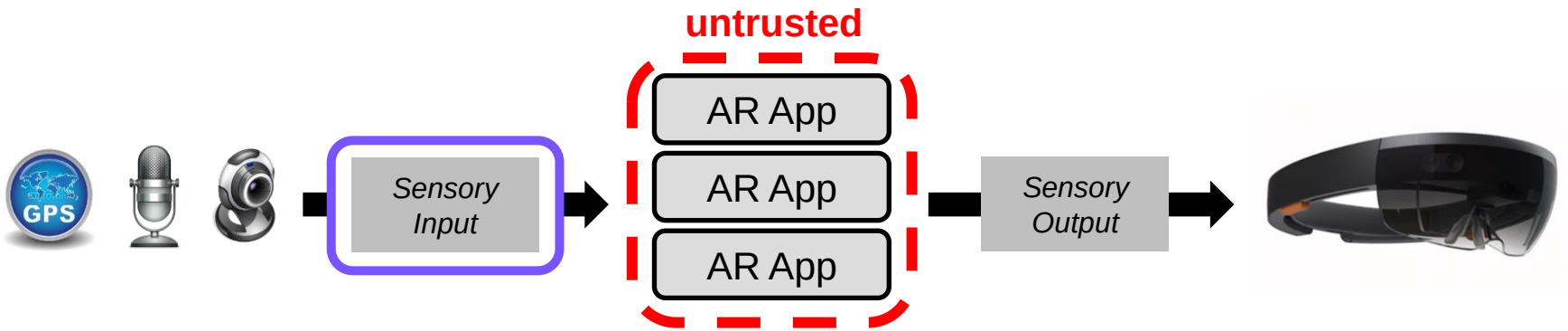
- Impact on automotive industry
  - Significant investment by automotive companies
  - Spurred vendor industry around automotive security
- Impact on standards, regulation, and legislation
  - SAE International (de facto standards body for the U.S. automotive industry) created committee and standards
  - Resources committed by NHTSA
  - U.S. bills on automotive cybersecurity
- Impact on research
  - New subfield of automotive security and significant DARPA and other funding efforts

(2) Security and Privacy for Augmented Reality





AR Input Privacy

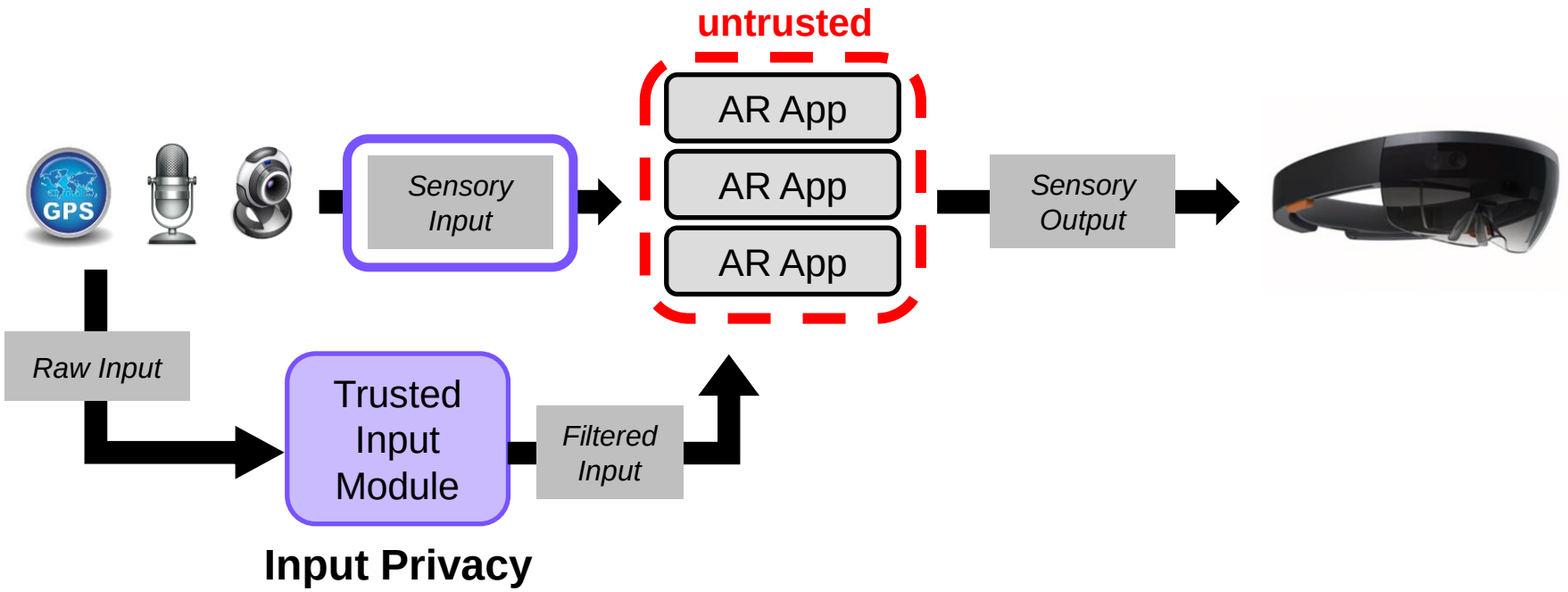


Seattle dive bar becomes first to ban Google Glasses over privacy fears

By NINA GOLGOWSKI

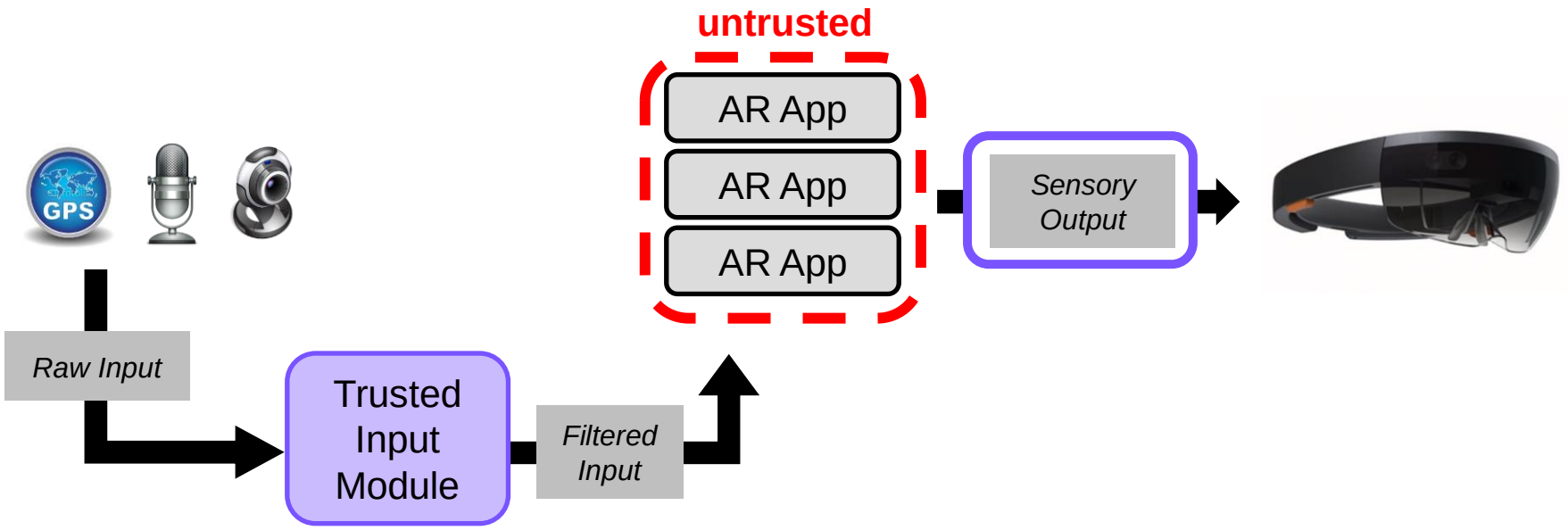
PUBLISHED: 00:43 EST, 10 March 2013 | **UPDATED:** 02:16 EST, 10 March 2013

AR Input Privacy



- Jana et al., USENIX Security ’13
- **Roesner et al., CCS ’14**
- Templeman et al., NDSS ’14
- Raval et al., MobiSys ’16

AR Output Security



Hyper Reality (https://www.youtube.com/watch?v=YJgo2ivYzSs)

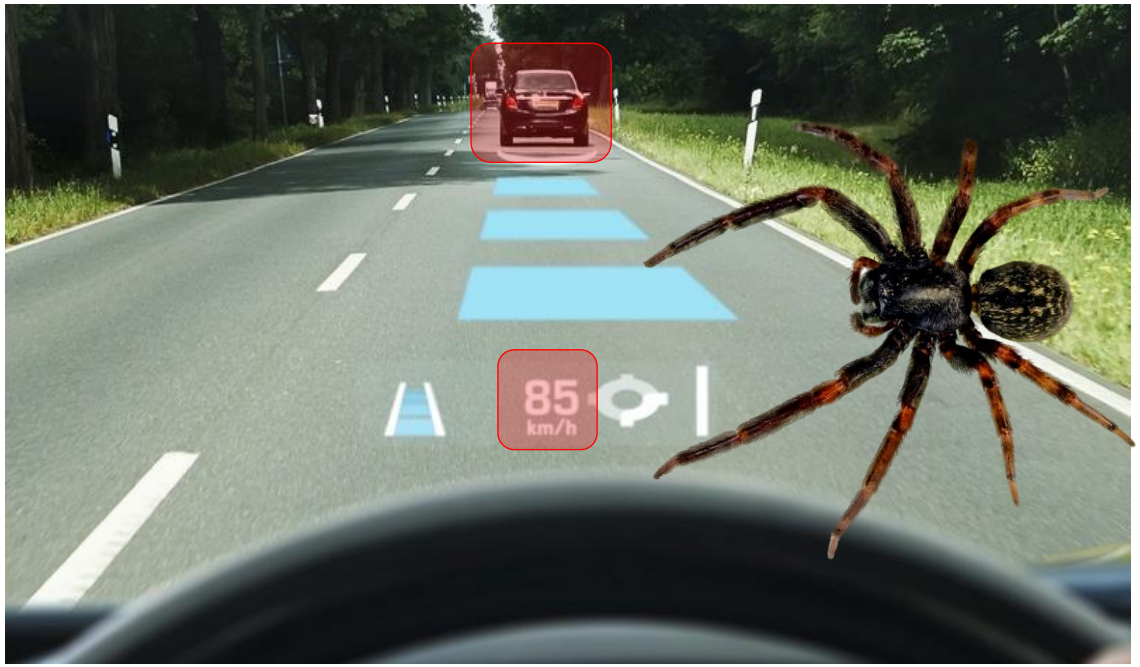
AR Output Security

A buggy or malicious app might…

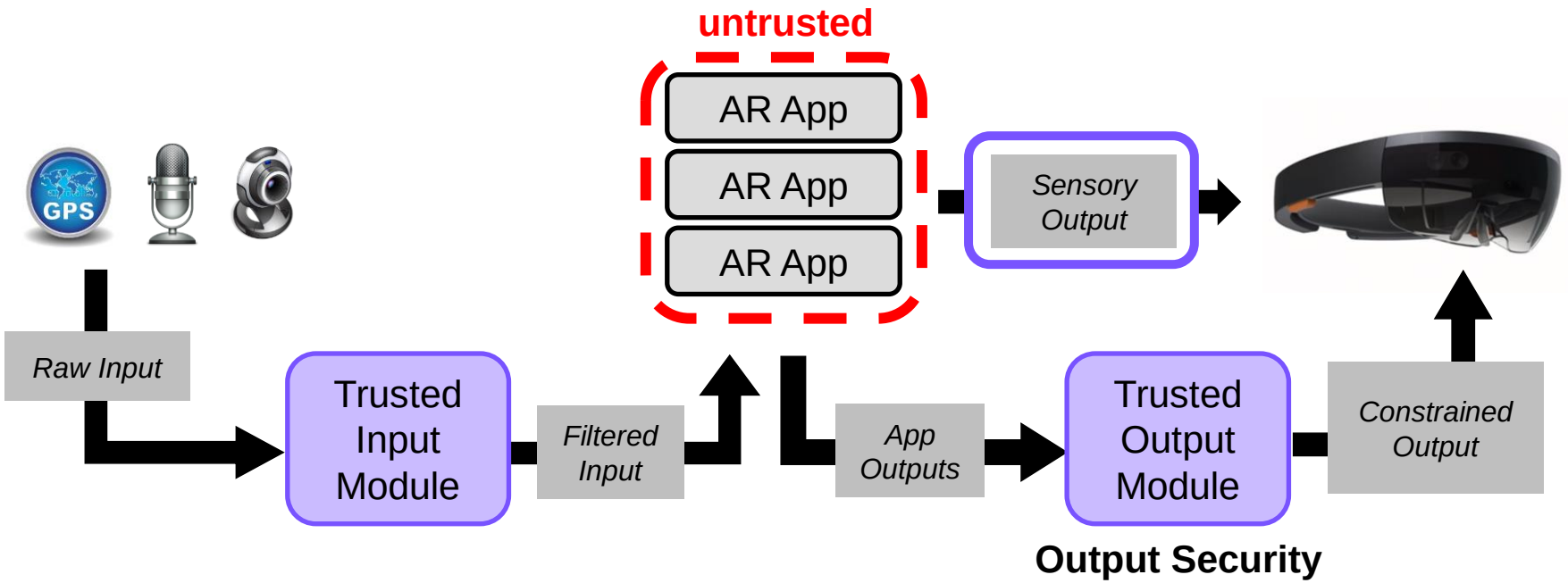
Obscure another app's virtual content to hide or modify its meaning

Obscure important real-world content, such as traffic signs or cars

Disrupt the user physiologically, such as by startling them



AR Output Security



Output Security

- **Lebeck et al., HotMobile '16**
- **Lebeck et al., IEEE S&P '17**
- **Lebeck et al., HotMobile '19**

Many Other Questions

- How to handle multiple apps augmenting reality at the same time?
  - **Lebeck et al., HotMobile '19**
- How to handle interactions between multiple users who may see different realities?
  - **Ruth et al., USENIX Security '19**

https://ar-sec.cs.washington.edu

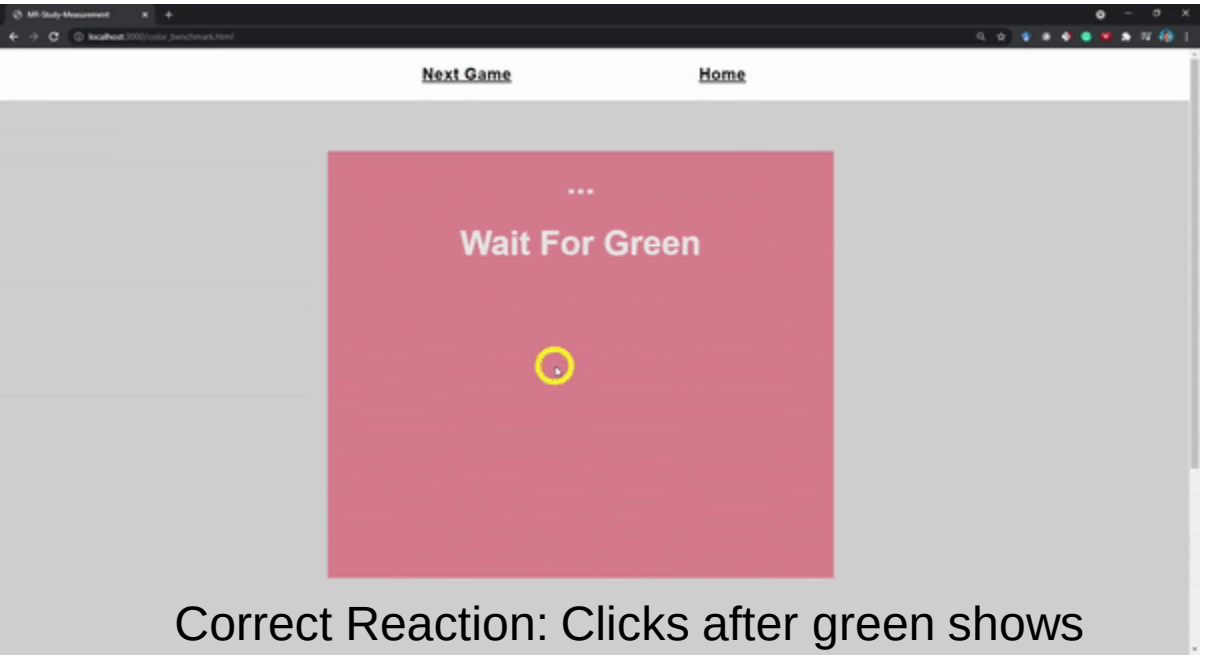
Recent developments in MR Security:

Researchers presented the microbenchmarks **(real-world stimuli)** on a computer monitor.

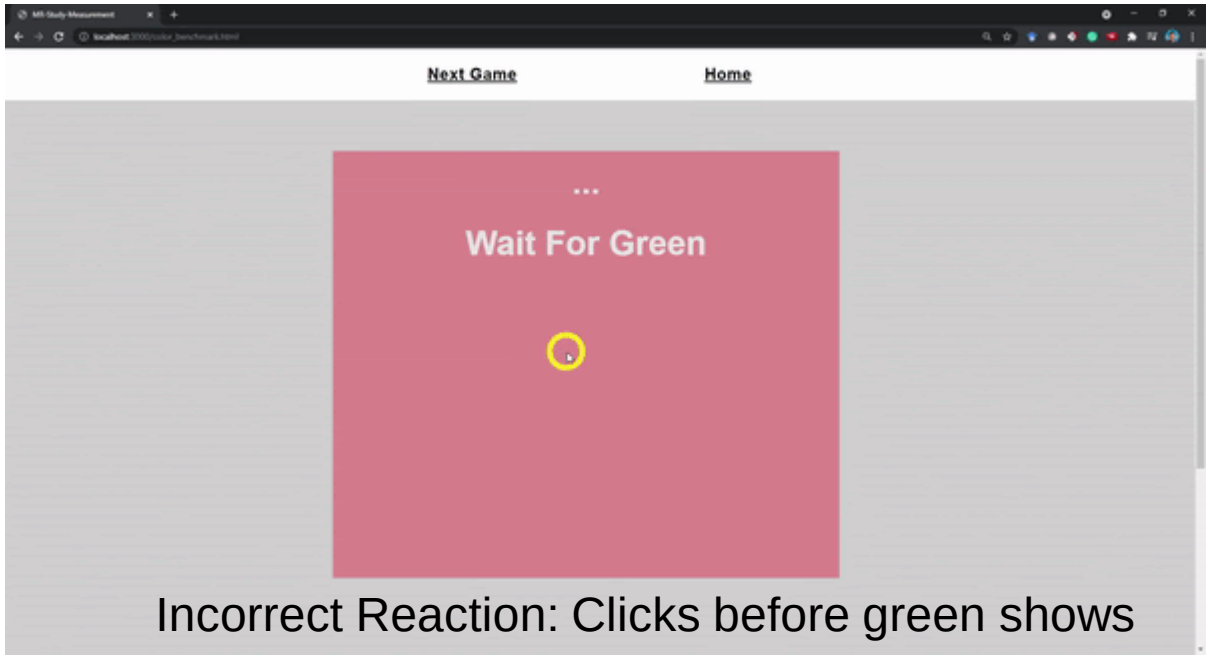
To allow for safe & controllable experiments where things were the same between all participants

Slides from Kaiming Chen (UW S&P Lab)

Reaction Time Task & MR Attacks



Correct Reaction: Clicks after green shows



Incorrect Reaction: Clicks before green shows

Goals for MR Attack:
Delay a correct reaction significantly or *induce an incorrect reaction*

Slides from Kaiming Chen (UW S&P Lab)

Key Lessons

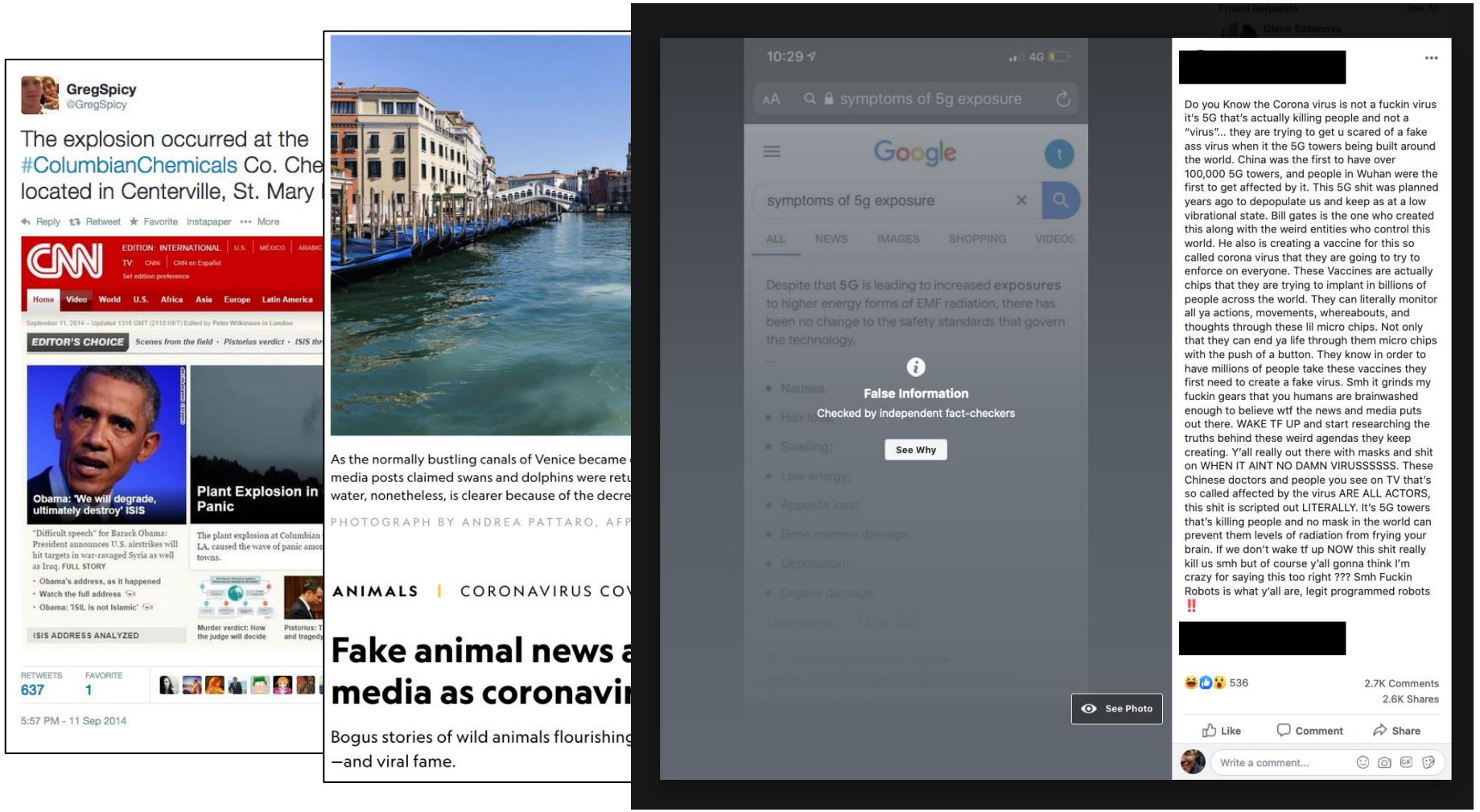
1. MR output attacks **can** have significant impacts on users.

2. In addition to **direct impacts** from attacks (e.g., inducing incorrect reactions on a task), we also documented **secondary impacts** from attacks that manifested on subsequent tasks.

3. **Dynamic**: Examples of participants' defensive strategies succeeding or backfiring

Slides from Kaiming Chen (UW S&P Lab)

(3) Technology-Enabled Disinformation



Serious Potential Consequences

Facebook uncovers disinformation campaign to influence US midterms

Social network removes 32 pages and accounts for 'co-ordinated inauthentic behaviour'

Hannah Kuchler in San Francisco and **Demetri Sevastopulo** in Washington JULY 31, 2018

How WhatsApp Destroyed A Village

In July, residents of a rural Indian town saw rumors of child kidnappers on WhatsApp. Then they beat five strangers to death.

Pranav Dixit
BuzzFeed News Reporter

Ryan Mac
BuzzFeed News Reporter

Reporting From
New Delhi

Posted on September 9, 2018, at 9:00 p.m. ET

Many Types of “False News”

	Satire	False Connection	Misleading Content	False Context	Imposter Content	Manipulated Content	Fabricated Content
Poor journalism		✔	✔	✔			
To Parody	✔				✔		✔
To Provoke or to ‘punk’					✔	✔	✔
Passion				✔			
Partisanship			✔	✔			
Profit		✔			✔		✔
Political Influence			✔	✔		✔	✔
Propaganda			✔	✔	✔	✔	✔

From Claire Wardle, https://medium.com/1st-draft/fake-news-its-complicated-d0f773766c79

What's New?

The Technology, Not the Incentives

- How content is created
  - Scale and democratization
  - Automated fake content creation
    - Video: https://grail.cs.washington.edu/projects/AudioToObama/
    - Text: https://rowanzellers.com/grover/
- How content is disseminated
  - Scale and democratization
  - Tracking and targeting
  - Algorithmic curation
  - Anonymity and bots
  - Immediate reach and feedback
- How content is consumed
  - Attention economy
  - Filter bubbles

Not Just a Technical Problem: Human Cognitive Vulnerabilities

(e.g., confirmation bias, backfire effect)

(4) Cryptocurrency/NFTs/etc

…Actually pretty little to do with S&P!

- Cryptocurrency has some neat math
  - But is mostly an economics and regulatory question
- NFTs
  - Are mostly a FOMO question
- That's about it!

The *usability* of these is interesting

- System compromise now == $$$

WRAP-UP

This Quarter

- Overview of:
  - Security mindset
  - Software security
  - Cryptography
  - Web security
  - Web privacy
  - Authentication
  - Mobile platform security
  - Usable security
  - Physical security
  - Anonymity
  - Smart home security
  - Side channels
  - Adversarial ML
  - Security for emerging tech

Lots We Didn't Cover…

- Really deep dive into any of the above topics
- (Most) Network security
- (Most) Traditional OS security
- (Most) Recent attacks/vulnerabilities
- (Most) Specific protocols (e.g., SSL/TLS, Kerberos)
- Access control
- Spam
- Malware / Bots / Worms
- Social engineering
- Cryptocurrencies (e.g., Bitcoin)
- Other emerging technologies
- …

Thanks for a great quarter! Hang in there.

- Stay in touch

  I'm always happy to answer questions or point you in directions on S&P ☺

- Not ready to be done?
  - CSE 490 Cryptography
  - CSE 481S Security Capstone
  - CSE 564 Graduate Computer Security

- Please fill out course evaluation:
  - https://uw.iasystem.org/survey/249000