

CSE 484 / CSE M 584: Computer Security and Privacy

Emerging Tech + Wrap-Up

Spring 2020

Franziska (Franzi) Roesner

franzi@cs.washington.edu

Thanks to 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

- **Last extra credit reading due tomorrow @ 11:59pm**
 - No late days
- **Lab 3 due Friday Saturday @ 11:59pm**
- **Final project due Mon, June 8 @ 11:59pm**
 - No late days
 - Make sure you address legal/ethical issues
 - Make sure you include references (at least in a dedicated slide)
- **No section tomorrow, no class Friday**
- Please let us know asap if your late days seem incorrect
- **If you are struggling, please reach out so we can make a plan**

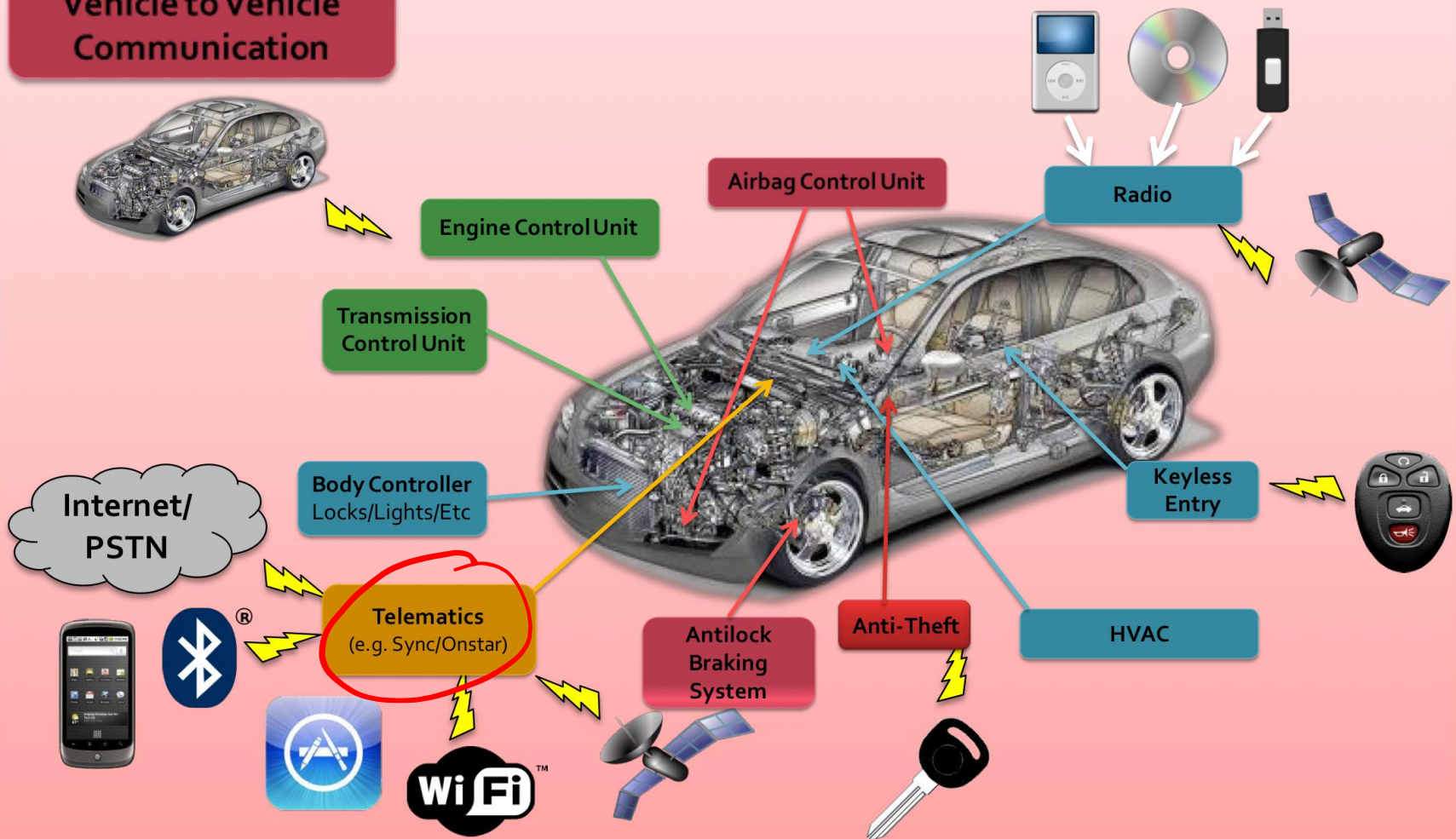
SECURITY AND PRIVACY FOR EMERGING TECHNOLOGIES

(1) Connected Automobiles

- Already emerged by now, but a fun story 😊
- Automobiles were only just being connected to the internet when we (UW+UCSD) studied them (~2009)
 - Had not faced significant adversarial pressure
 - Just won a “Test of Time” Award

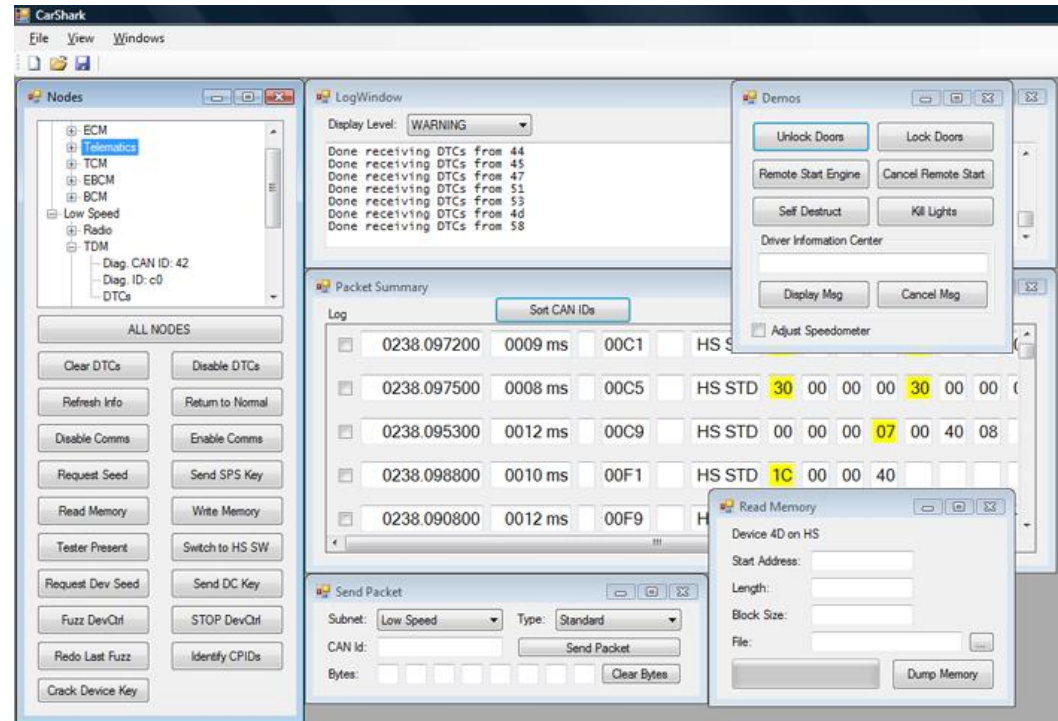
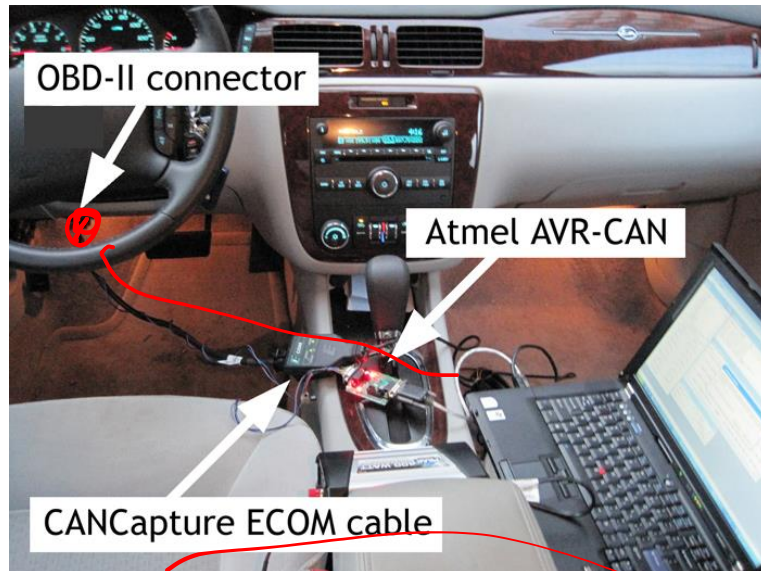
www.autosec.org

Vehicle to Vehicle Communication

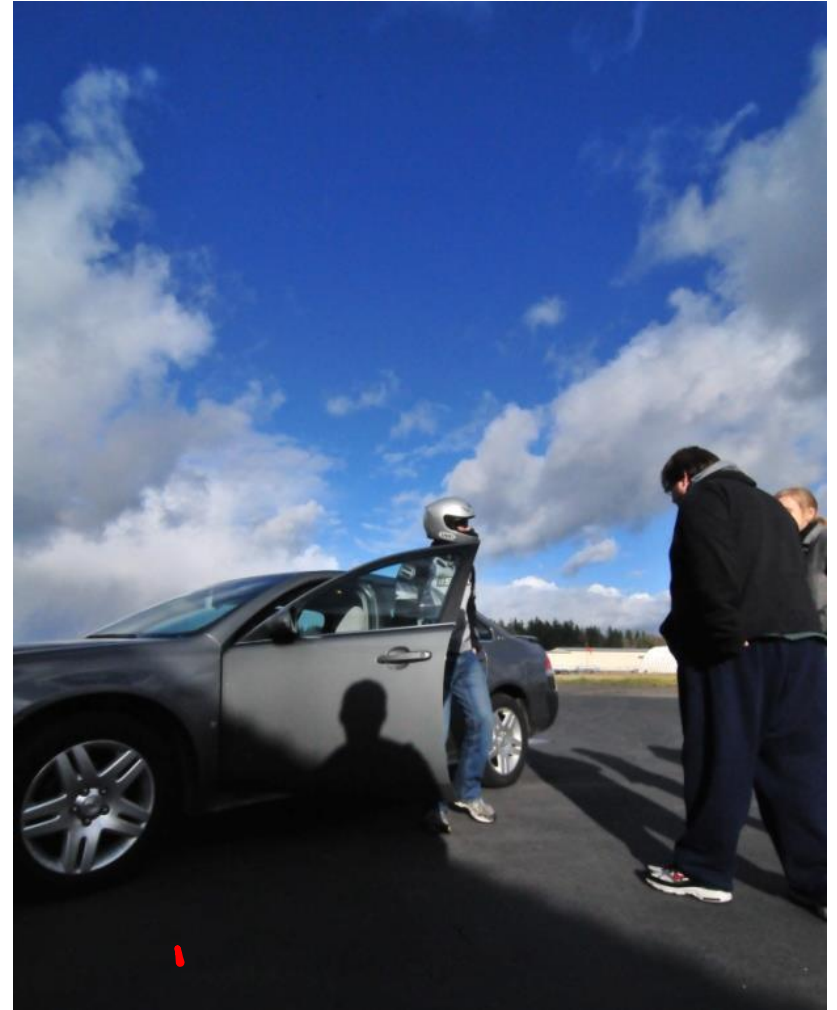


Computers in a modern automobile

Experiments with a Real Car



Experiments with a Real Car



Example: Force Brakes On/Off



<https://www.youtube.com/watch?v=H6oozuid1K4>

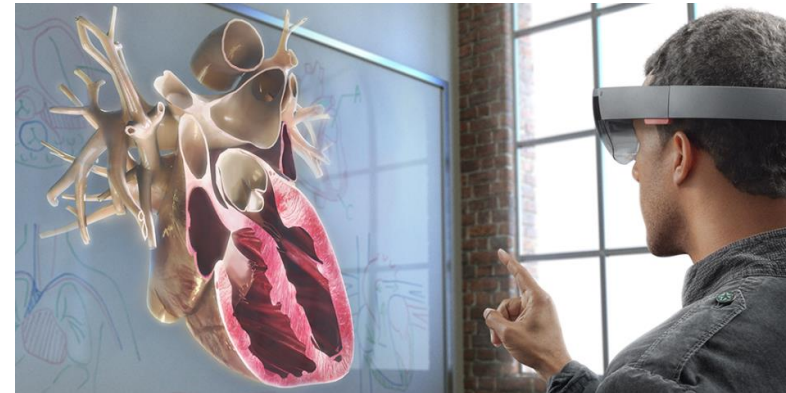


<https://www.youtube.com/watch?v=917VOx6tBKA>

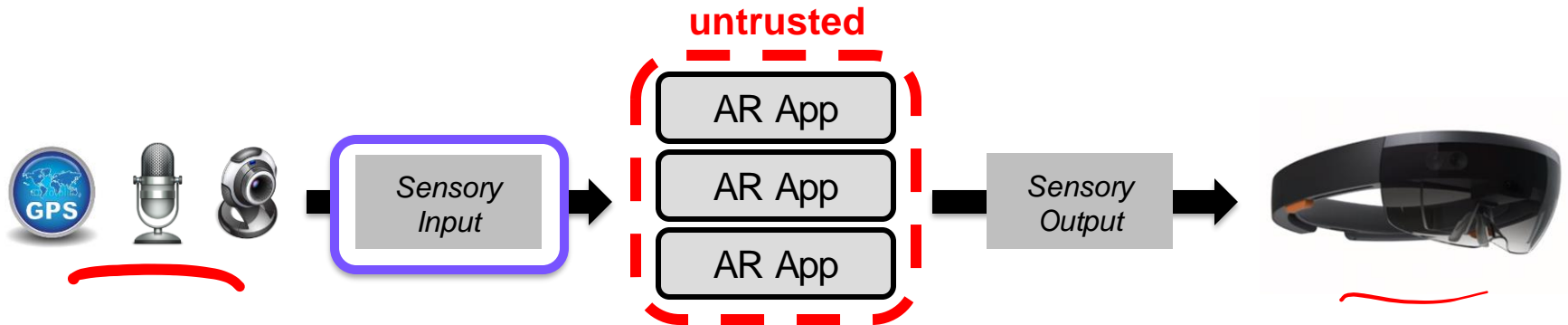
Impacts

- 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

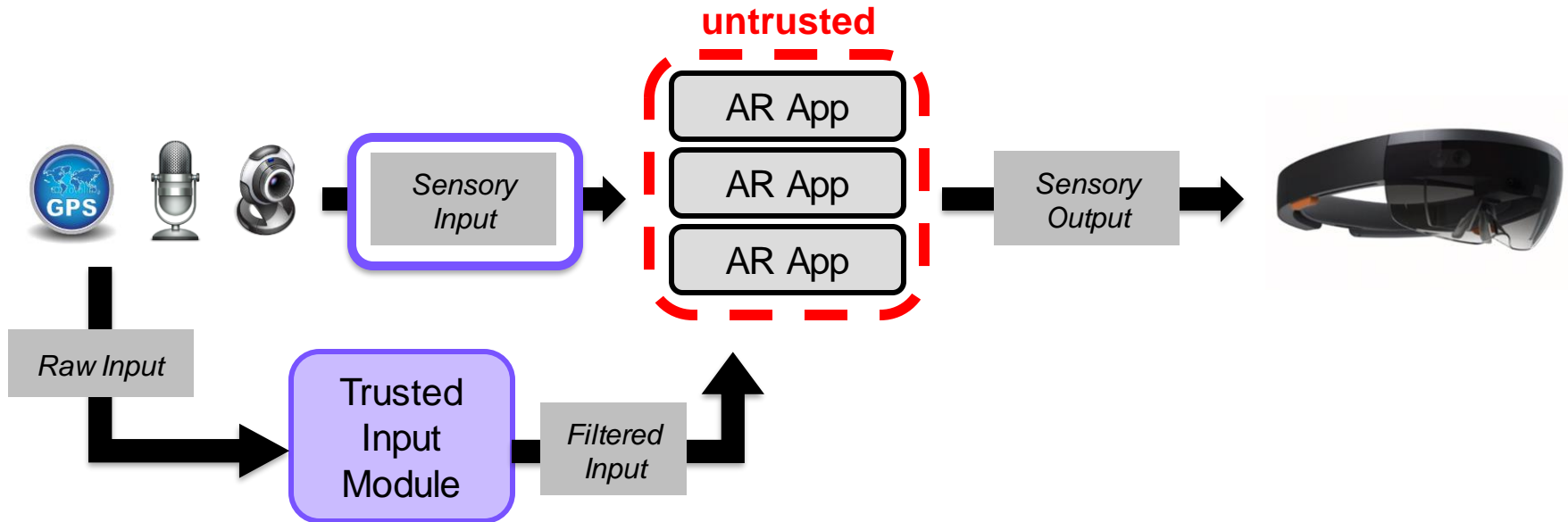


Seattle dive bar becomes first to ban Google Glasses over privacy fears

By NINA GOLGOWSKI

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

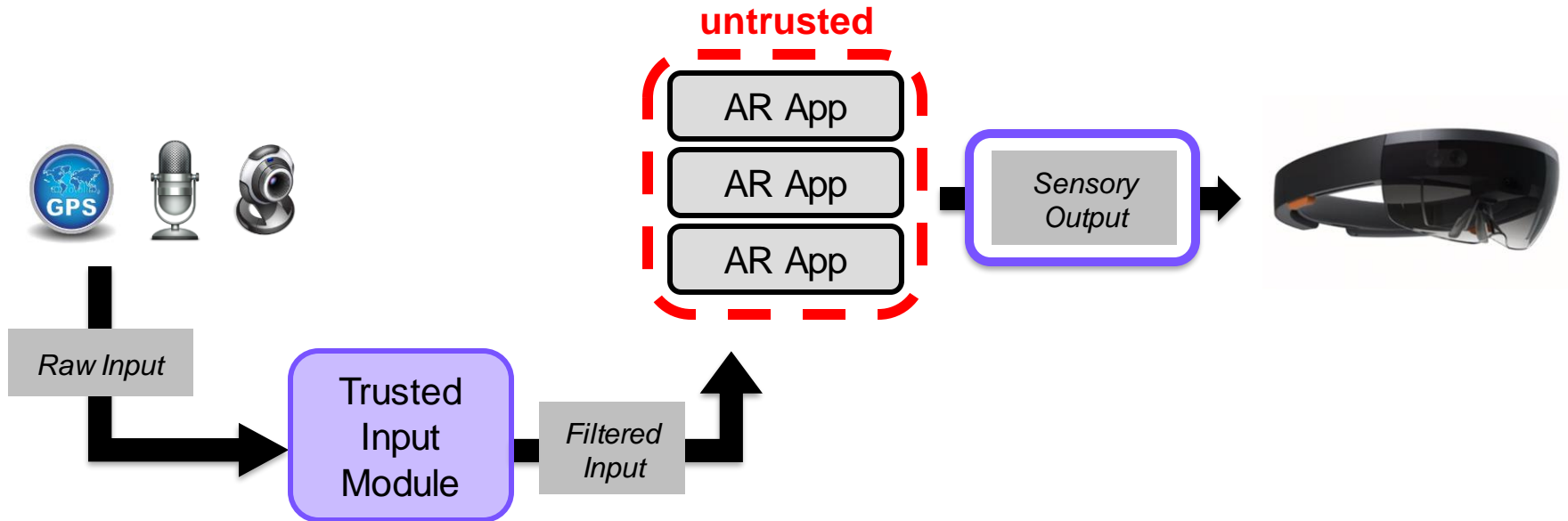
AR Input Privacy



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=YJg02ivYzSs>)

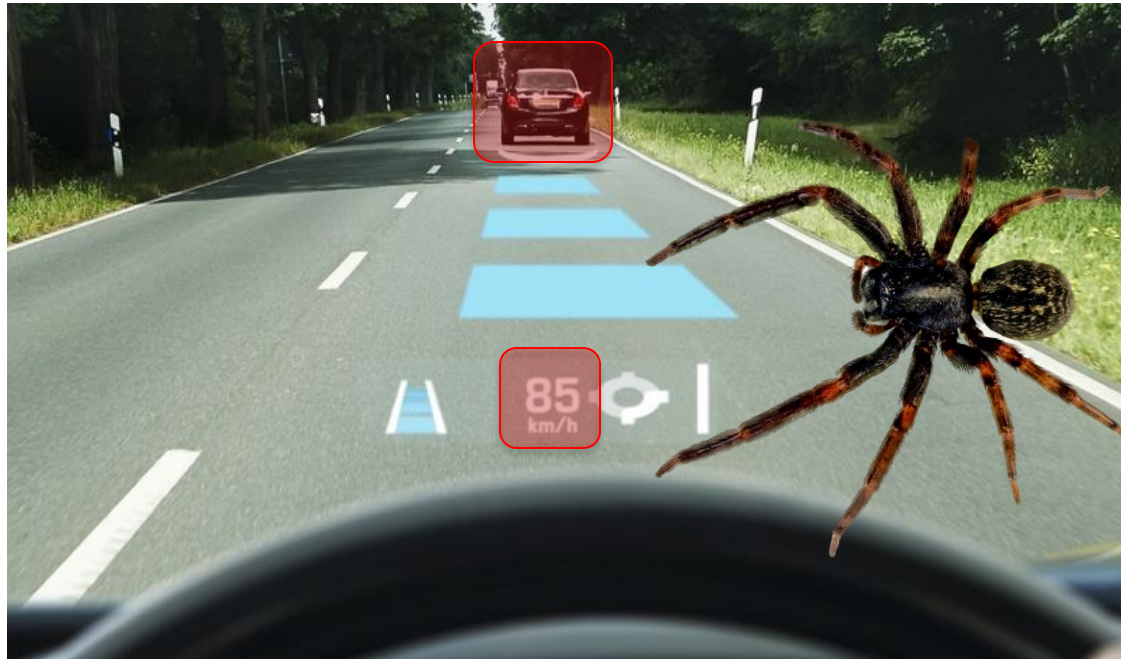
AR Output Security

A buggy or malicious app might...

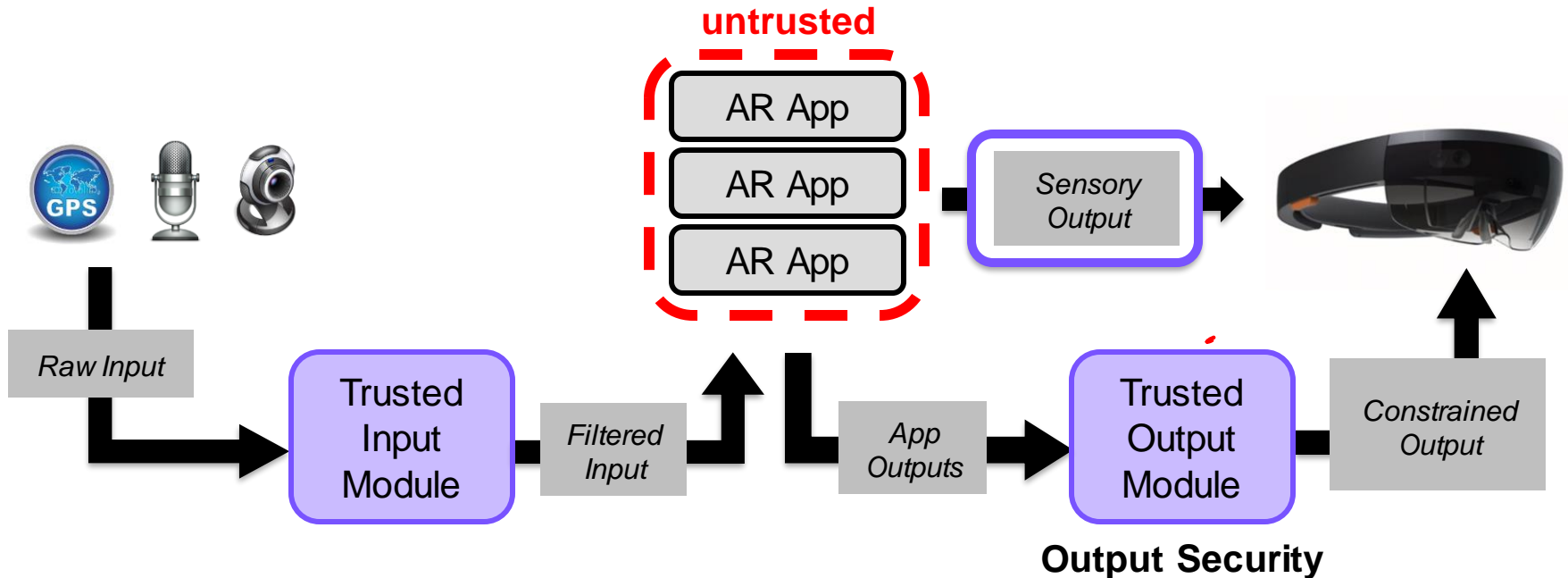
Obscure another app's virtual content to hide or modify its meaning

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

Disrupt the user physiologically, such as by startling them •



AR Output Security



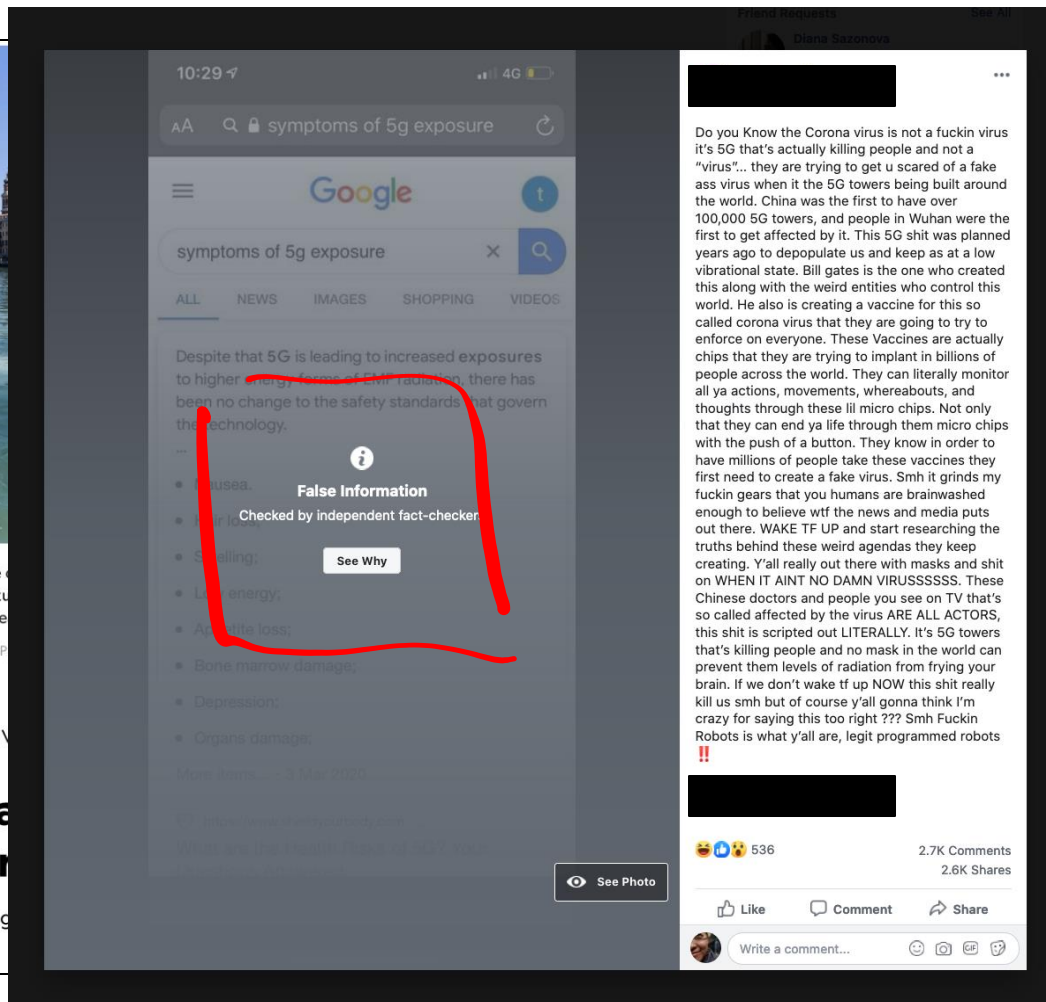
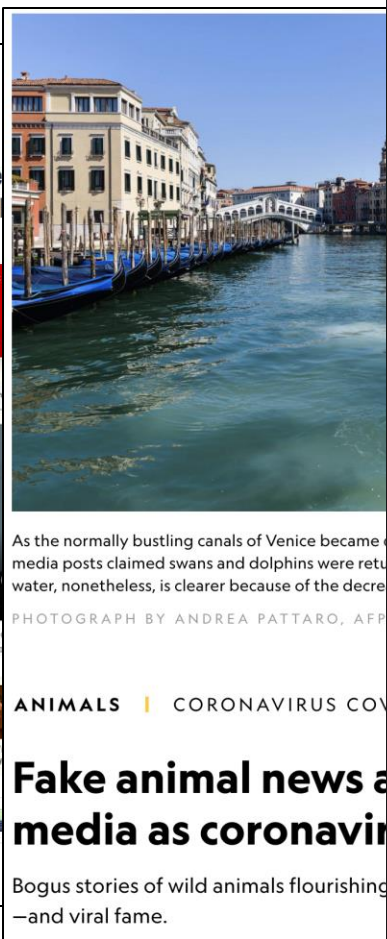
- Lebeck et al., HotMobile '16
- Lebeck et al., IEEE S&P '17
- Lebeck et al., HotMobile '19

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>

(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

Deep Fakes

- 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)

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 (even if strange) quarter! Hang in there.

- Please stay in touch
 - Extra office hours during lecture time on Friday
- Not ready to be done?
 - CSE 490 Cryptography in the fall
 - CSE 481S Security Capstone in the winter
 - TAing for 484
- Please fill out course evaluation:
<https://uw.iasystem.org/survey/225395>