Admin

• **Lab 3** due today
  – OK to use late days

• **Final project due** Mon, Dec 14 @ 11:59pm
  – No late days

• Please let us know asap if your late days seem incorrect
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
  – Won a “Test of Time” Award this year

www.autosec.org
Computers in a modern automobile
Experiments with a Real Car

OBD-II connector

Atmel AVR-CAN

CANCapture ECOM cable

12/4/20

CSE 484 / CSE M 584 - Autumn 2020
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

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

Raw Input

Trusted Input Module

Filtered Input

untrusted

AR App

AR App

AR App

Sensory Output

AR App

CSE 484 / CSE M 584 - Autumn 2020
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
As the normally bustling canals of Venice became eerily quiet, social media posts claimed swans and dolphins were returning. But the water, nonetheless, is clearer because of the decrease in traffic from the usually bustling canals.

Fake animal news and media as coronavirus.

Bogus stories of wild animals flourishing— and viral fame.
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”

<table>
<thead>
<tr>
<th>Poor journalism</th>
<th>False Connection</th>
<th>Misleading Content</th>
<th>False Context</th>
<th>Imposter Content</th>
<th>Manipulated Content</th>
<th>Fabricated Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Parody</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>To Provoke or to ‘punk’</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partisanship</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Profit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Political Influence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Propaganda</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

• Stay in touch
  – Come say hi when we are back on campus 😊

• Not ready to be done?
  – CSE 490 Cryptography
  – CSE 481S Security Capstone in the winter
  – CSE 564 Graduate Computer Security
  – TAing for 484

• Please fill out course evaluation: https://uw.iasystem.org/survey/232765