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
Computers in a modern automobile
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

untrusted

GPS
Microphone
Camera
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
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
(3) Technology-Enabled Disinformation

The explosion occurred at the Columbia Chemicals Co. plant located in Centerville, St. Mary. The company is situated near the site where a recent chemical accident occurred. The explosion caused significant damage to the surrounding area and prompted a large-scale response from emergency personnel.

As the normally bustling canals of Venice became inaccessible due to the flooding, media posts claimed swans and dolphins were returning to the lagoon. Although tourism in Venice is lower than usual, the area remains popular with tourists.

Fake animal news and media as coronavirus. Bogus stories of wild animals flourishing—and viral fame.

Do you know the Coronavirus virus is not a fusion virus? It’s 5G that’s actually killing people and not a “virus”. They are trying to get a scared of a fake virus when it’s the 5G towers being built around the world. China was the first to have over 100,000 5G towers, and people in Wuhan were the first to get affected by it. This 5G tech was planned years ago to depopulate us and keep us at a low vibrational state. 5G gates are the ones who created this along with the weird entities who control this world. He also created a vaccine for this so-called corona virus that they are going to try to enforce on everyone. These vaccines are actually chips that they are trying to implant in billions of people across the world. They can literally monitor all your actions, movements, whereabouts, and thoughts through these micro chips. Not only that, they can and will force people to take these vaccines. They will force millions of people to take these vaccines they first need to create a fake virus. Once it gains my f-cking gears that you humans are brainwashed enough to believe all the news and media stuff out there. WAKE TF UP and start researching the truths behind these weird agents they keep creating. Y’all are really out there with masks and shit on. MOVE IT AND SHINE VIRUS2022. These Chinese doctors and people you see on TV that’s so-called affected by the virus ARE ALL ACTORS. This shit is all set out LITERALLY. It’s 5G towers that’s killing people and no mask in the world can protect them from radiation of firing your brain. If we don’t make it up NOPE this shit really kill us but of course I’ll gonna think I’m crazy for saying this. Take it from a truther, robots is what y’all are, legit programmed robots
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></th>
<th>Satire</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>Poor journalism</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To Parody</td>
<td>✔</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>
<td></td>
</tr>
<tr>
<td>Passion</td>
<td></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>
<td></td>
</tr>
<tr>
<td>Profit</td>
<td>✔</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>
<td></td>
</tr>
<tr>
<td>Propaganda</td>
<td></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)
(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](https://uw.iasystem.org/survey/249000)