Outline

• Quick Summary of the Course

• Final Exam, MP5 Demo, Grading

• Student Feedback (ICES)
What We Have Talked About

- Online Social Networks
- Machine Learning 1, 2
- Crypto Constructs
- De-Identification
- Trusted Computing 1, 2
- Information Flow
- Crypto Models 1, 2
- Health IT
- Bitcoin
- Smartphones 1, 2
- Web Privacy
- Automobiles
- Adversarial ML
- Code Stylometry
- Smart Grid
- Hardware Side Channel
- Insider Threats
- Cyber Warfare
Traditional Threat Model

- Asset
- Attacker
- Vector
Guiding Future Research

- New threats derive from changes in the nodes of this graph.
- The overall model is still good but there are changes in the nodes.
- Ideally research plans should cover as much of the model as possible, but
- Sometimes strong work can be done without all elements being present.
Threats

**Asset**
- Embedded devices
- Clouds
- Personal information
- Credentials
- Intellectual Property
- Radio spectrum
- Public opinion

**Attacker**
- Attackers for hire
- States
- “Hacktivists”
- Black market
- Insiders

**Vector**
- Exploits
- New side channels
- Social networks
- App stores
- Cell phone sensors
- ML frameworks
Established Threats

• Attacks on company databases to find financial information
• Exploits for login information
  – Phishing
  – Banking Trojans (Man in the Browser) attacks to obtain access to bank accounts
• Advanced Persistent Threats (APTs) for intellectual property (trade secrets)
• Attacks on cyber-infrastructure of energy systems
  – Stuxnet
• Theft of Bitcoins and the theft of cycles to mine bitcoins
• Integrity and DoS attacks on GPS
• Collecting cloud-based smart phone data of celebrities
Speculative Threats

• Attacks on medical devices
  – From Fitbits to defibrillators
  – Lab demonstrations and good play in the press
  – Some precedent: Tylenol and epilepsy

• Attacks on computerized automotive functions
  – Manipulating tire pressure readings by wireless, etc.
  – Take control of a self-driving car? Mislead its AI?

• Attacks on Electronic Health Records (EHRs)
Assessing Risk

• Cyber-security metrics are a key challenge
  – Practical people want to know how much they are getting for money spent on security.

• Early success with viruses like Code Red
  – Quantify costs based on lost work time, IT staff effort, new equipment and software.

• And there are some benchmarks
  – HIPAA and HITECH fines and the “Wall of Shame”

• But the problem remains mostly open
About The Final Two Weeks...
Final Exam (Take-home)

• Time: **May 8 Friday at 7pm CT**
  – Final exam paper will be released online
  – Watch out for announcement on Piazza

• Take-home for 48 hours, similar format to mid-term
  – 25% from first half of lectures + 75% from second half
  – You should be able to finish in 3 hours, use your time wisely

• Submit via **git** by **May 10 at 7pm CT**
  – A PDF document with your name, netID, and answers

• Open book, open notes, but finish it **independently**
  – You may not discuss any exam related questions with anyone
    (you have my trust 😊)
See https://piazza.com/class/k58g8mvvy1vf28e?cid=204

- Live demo in person → recorded video
- Upload the video to your Google drive and share the link with us via email (set permission correctly)
- Deadline for submission **May 11, 11:59 PM CT**
- Expected length 10 minutes
- Discuss about all questions asked in report to this demo presentation
### Common Assessment

<table>
<thead>
<tr>
<th>Assessment Element</th>
<th>% of Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP1</td>
<td>6</td>
</tr>
<tr>
<td>MP2</td>
<td>7</td>
</tr>
<tr>
<td>MP3</td>
<td>8</td>
</tr>
<tr>
<td>Midterm</td>
<td>15</td>
</tr>
<tr>
<td>MP4</td>
<td>9</td>
</tr>
<tr>
<td>MP5</td>
<td>10</td>
</tr>
<tr>
<td>Participation*</td>
<td>15</td>
</tr>
<tr>
<td>Final</td>
<td>30</td>
</tr>
</tbody>
</table>

This will be used for 100% of the grade for 3 credit students and 75% of the grade for 4 credit students.

**Participation: full score = done 70% of the quizzes**
Students Getting 4 Credits

Write a Survey Paper

• Four-credit students are expected to complete a survey paper.

• Grade will come 75% from common assessment and 25% from the Extra Credit Assessment

Steps

• Choose your topic (related to security and privacy).

• Select at least 10 papers on the topic.

• Proposal due on March 26 at 11:59PM

• Write an 8 page survey of the papers.

• Survey due on Sunday May 10 at 11:59 PM CT
Final Remarks

• This has been a very challenging semester
• Thanks everyone for working hard to overcome the difficulties
• Stay safe and healthy
• Contact us if you need any additional help

Big Thanks to HB!
Please Give us Feedback via ICES

• Instructor and Course Evaluation System (ICES)
  – Email will be sent to you with the evaluation link

• My first time teaching this course, looking for all kinds of feedback and suggestions

• *40 students will be randomly selected from the pool of students who complete ICES for $25 Amazon gift card