Instructor: Laurin Weissinger, laurin.weissinger@tufts.edu

Office Hours: Monday, 11:00am–13:00 noon, Zoom

Description and Objectives: This part of “How systems fail” will focus on complex (socio) technical systems, analyzing why real-world systems fail and what can be done to build resilient systems.

Course Requirements:

- **Attendance and Reading** – It is very important to attend each class and read the required reading. Attendance is mandatory.

- **Homework** – Most classes will have required reading; summarize your findings, thoughts, and ideas by Wednesday 12 midnight Eastern Time. Try to speak to two of the “Reflection Questions” but you are welcome to add your personal thoughts, ideas, and questions as well. Expected length: 400-800 words. It will be graded as ✓+, ✓, ✓–, ✗ (A, A-, B+, I)

- **Briefing Paper** – 1000-1200 word briefing paper about a cybersecurity issue.

- **Final Group Project** – Concept document for a COVID-19 vaccination tracking application and its backbone.

- **Grading** – Homework (25%); Briefing Paper (30%); Final Project (45%). The Policy Grade will be 1/3 of the overall class grade.

Course Overview:

1. Week 1: What is a system?
2. Week 2: How do you build a system?
3. Week 3: Threat Modeling in complexity
4. Week 4: Privacy and Data – do they matter to system architecture?
5. Week 5: Complex infrastructures: IoT and self-driving vehicles
6. Week 6: Social Media and Content Moderation – where are the system boundaries?
7. Week 7: If something goes wrong: who has visibility, who can fix things, who is responsible?
8. Week 8: Global Systems: DNS root key rollover
9. Week 9: National Security and "national systems" – what is critical infrastructure?
10. Week 10: The EINSTEIN Program
11. Week 11: The Solar Winds breach

12. Week 12: How do we build for success?

13. Week 13: Reflections on systems and system failures

Schedule

Themes:

**Week 1: What is a system?**

1. Reflection Questions
   - How can we conceptualize what a system is and what it does?
   - Based on your work experience, studies, etc: How does your (previous) discipline or niche understand systems?
   - How can we visualize a system?
   - Why think in/from a ‘systems perspective’?

2. Reading:

**Week 2: How do you build a system?**

1. Reflection Questions
   - Consider for one example or compare: hospital, bank, university:
   - What are the key (security) issues to keep in mind when building a system?
   - How can we analyze what to build; how, and when to build a system?
   - What resources and types of expertise need to be included?

2. Reading:

**Week 3: Threat Modeling in complexity**

1. Reflection Questions
   - How should we analyze and conceptualize threats and risks to (complex) systems?
   - What controls best address key threats / threat actors (choose an example); why?
   - What is the difference between risk, threat, threat actor? Can we assign numbers to this issue?
2. Reading:
   Adam Shostack (n.d.) Experiences Threat Modeling at Microsoft

3. Further Reading:

Week 4: Privacy and Data – do they matter to system architecture?

1. Reflection Questions
   - Are data information part of the system or something that the system processes?
   - How to design a system around protecting privacy?
   - Are data a toxic asset; should their possession and processing be more regulated?

2. Reading:

Week 5: Complex infrastructures: IoT and self-driving vehicles

1. Reflection Questions
   - How can we define system boundaries; are they the same for everyone; do they always make sense?
   - What constitutes a system failure for IoT or SDVs?
   - Is the complexity of these systems too high to deal with? How would we address that complexity?
   - What solutions can actually be implemented?

2. Reading:
Week 6: Social Media and Content Moderation – where are the system boundaries?

1. Reflection Questions
   - How can we design a system and respond to issues in systems that include unpredictable users?
   - Is Section 230 the right approach to content moderation?
   - Is dealing with malicious content even possible considering system size, complexity, and (different) regulation(s)?

2. Reading:

3. Further Reading:

Week 7: If something goes wrong: who has visibility, who can fix things, who is responsible?

1. Reflection Questions
   - How to address systemic threats; who can do it; who should do it?
   - How would we identify the culprit; is there always one?
   - Who is responsible for the internet, for the DNS?

2. Reading:

Week 8: Global Systems: DNS root key rollover

1. Reflection Questions
   - Why does the DNS root zone signing key matter?
   - What are the issues that are being considered here?
   - How could the concept fail?
2. Reading:

*ICANN Implementation Plans*
2017 & 2018 KSK Rollover Operational Implementation Plans
2017 & 2018 KSK Rollover Back Out Plans


**Week 9: National Security and “national systems” – what is critical infrastructure?**

1. Reflection Questions

- What is a national computer network? How does it fit into the ‘national system’?
- What is critical infrastructure, what isn’t? How do we tell?
- Is national cyber defense possible?

2. Reading:


Skim: Fireeye Report: APT37 (REAPER) The Overlooked North Korean Actor

**Week 10: The EINSTEIN3 Program**

1. Reflection Questions

- How does system architecture matter to how we build solutions?
- Why do the authors think that EINSTEIN3 cannot work?
- What could be done to make something like EINSTEIN3 work?
- Can a distributed infrastructure ever be controlled; can it be secure?
- Can a centralized infrastructure ever be controlled; can it be secure?

2. Reading:


**Week 11: The Solar Winds breach**

1. Reflection Questions

- What happened?
- Who is to blame?
- Could be avoided, realistically?

2. Reading:

This is a developing case, reading will be made available closer to the class date.
Week 12: How do we build for success?

1. Reflection Questions
   - What have we learned about systems?
   - What are the key things we should and shouldn’t do?
   - Is there a political economy of security?

2. Reading:

Week 13: Reflection Class: On systems and system failures

1. Reflection Questions
   - Why do systems fail; what are the recurring issues – are they ‘internal’ or ‘external’?
   - Can policy fix these issues?
   - Can these issues be fixed outside policy, theoretically and practically?

2. Short Reading based on prior discussions might be assigned.