EECS 588
Computer & Network Security

Instructors: Earlence Fernandes and Amir Rahmati
GSI: Kevin Eykholt

Jan 5, 2017
Introduction
(material adapted from
J. Alex Halderman's slides)

#whoami

- Earlence Fernandes (Instructor), PhD Student, Graduating in April 2017
- Interviewing for Faculty Jobs!
- Systems Security Researcher (IoT)
- earlence@umich.edu
- 4945 Beyster; Office Hours: 4901 BBB Tu 3.30-4.30 or by appt.
- https://web.eecs.umich.edu/~earlence

#whoarewe

- Amir Rahmati (Instructor), PhD Student, Graduating in April 2017
- Interviewing for Faculty Jobs!
- Systems/Hardware/Network Security Researcher
- rahmati@umich.edu
- 4945 Beyster; Office Hours: 4901 BBB Tu 3.30-4.30 or by appt.
- amir.rahmati.com

#whoarewe

- Kevin Eykholt (GSI), PhD Student
- Machine Learning Security (past: DB security)
- keykholt@umich.edu
- 4945 Beyster; Office Hours: by appt.

Today's Class

- Welcome, Introductions, Course Overview
- Areas of Security Research: Systems, Networks, Privacy, …
- Current Events: IoT Security, Machine Learning Security, Data Breaches
- How to read research papers, How to write reviews, How to present a paper

Goals for This Course

- Gain hands-on experience
  - Building secure systems
  - Evaluating system security
- Prepare for research
  - Computer security subfield
  - Security-related issues in other areas
- Generally, improve research, writing, and presentation skills
- Learn to be a 1337 hax0r, but an ethical one!

Getting In, Getting an A

- Waitlist?
- Prereqs: EECS482 or EECS489 or grad standing
- We'll TRY to grant everybody overrides*, but can't guarantee hard work will bring success, unless you have the prerequisites.

* = Depending on class room space

https://eecs.umich.edu/courses/eecs588/

Computer & Network Security

EECS 588 – Winter 2017

Instructor: Amir Rahmati

Office hours: Tu 3:30–4:30, 4901 Beyster, or by appointment (Jan 17 and 24 have no fixed office hours yet)

Instructor: Earlence Fernandes

Office hours: Tu 3:30–4:30, 4901 Beyster, or by appointment (Jan 17 and 24 have no fixed office hours yet)

Credits: 4. This course counts towards meeting software quals requirements.

Prerequisites: EECS 482 Operating Systems, EECS 489 Networking (recommended), or grad standing. Success in this course requires a mature understanding of software systems.

Lectures: TuTh 1:30–3:30, 1690 Beyster

GSI: **Kevin Eykholt** (4945 Beyster, meetings by appointment)

Forum: We'll use Piazza for online discussion and announcements. For administrative issues, email eecs588.w17@umich.edu.

Resources

Security Research at Michigan
Security Reading Group
CSE CTF Club

This intensive research seminar covers foundational work and current topics in computer systems security. We will read research papers and discuss attacks and defenses against operating systems, client-side software, web applications, and IP networks. Students will be prepared for research in computer security and for security-related research in other subareas, and they will gain hands-on experience designing and evaluating secure systems.

- Building Blocks
  - Security Mindset, thinking like an attacker, reasoning about risk, research ethics, basic crypto (hash, MAC, PRNG, KeyEx, PKI, SSL/TLS)
- Software Security
  - Exploitable bugs: buffer overflow, ROP
  - Malware: viruses, spyware, rootkits
  - Automated security testing and tools for writing secure code
  - Virt, Sandboxes, OS-level defenses
- Web Security
  - Browser security model
  - Website attacks and defenses: XSS, SQL Inj, CSRF, Oauth hacks
  - Internet crime: spam, phishing, botnets – technical and non-tech responses
- Network Security
  - Protocol Security: TCP and DNS
  - Policing Packets: Firewalls, VPNs, Intrusion Detection
  - Denial of Service Attacks and Defenses
  - Data privacy, anonymity, surveillance, censorship
- Special/Emerging Topics
  - IoT (covering some aspects today and next week!)
  - Hardware security
  - Security for Machine Learning and Machine Learning for Security
  - Electronic Voting

NOT A CRYPTO COURSE

Getting to know you

- Fill up this Google form now (5 minutes):

http://bit.ly/2jbqpNf

Meet the Adversary

"Computer security studies how systems behave in the presence of an *adversary.*"

An intelligence that actively tries to cause the system to misbehave.

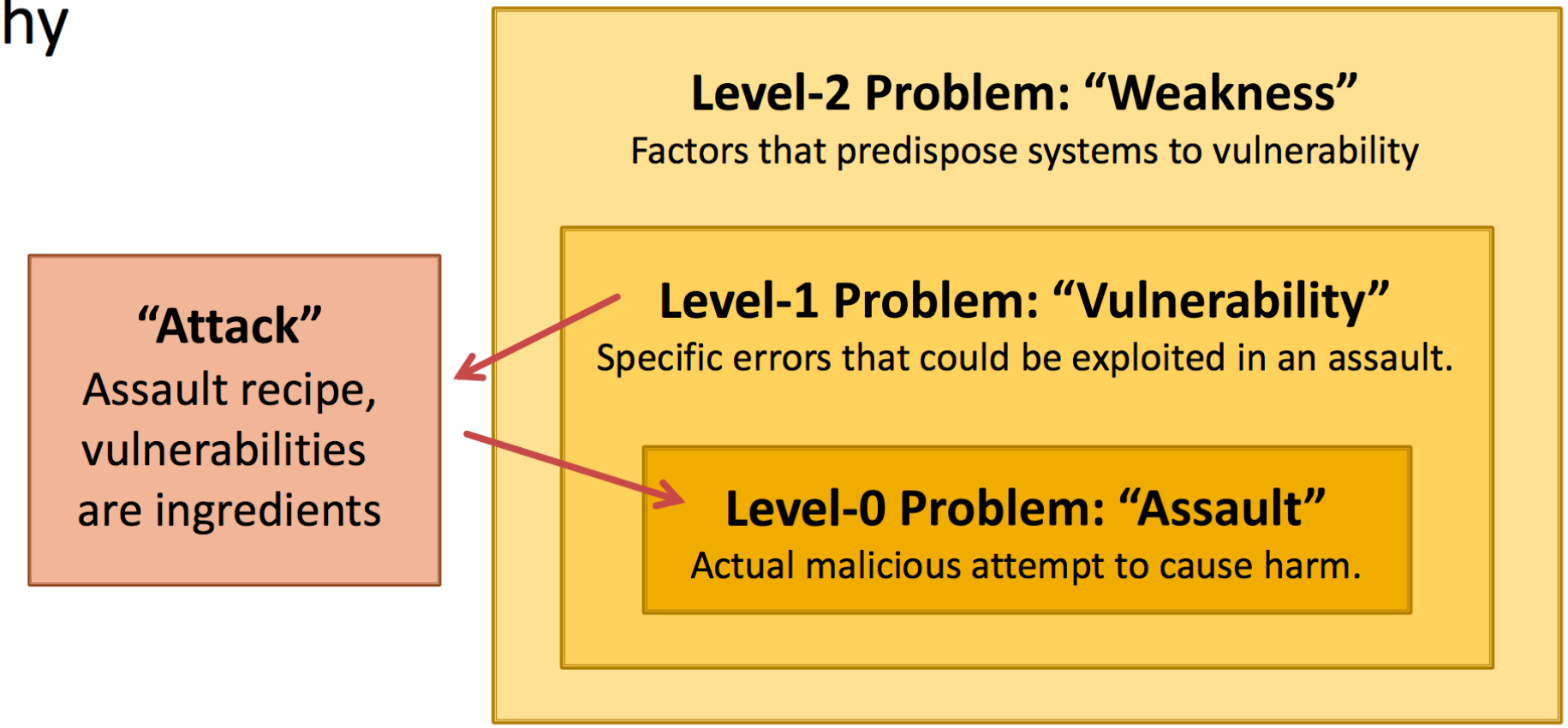
Why is Security its own Area of CS?

Who does Security Research?

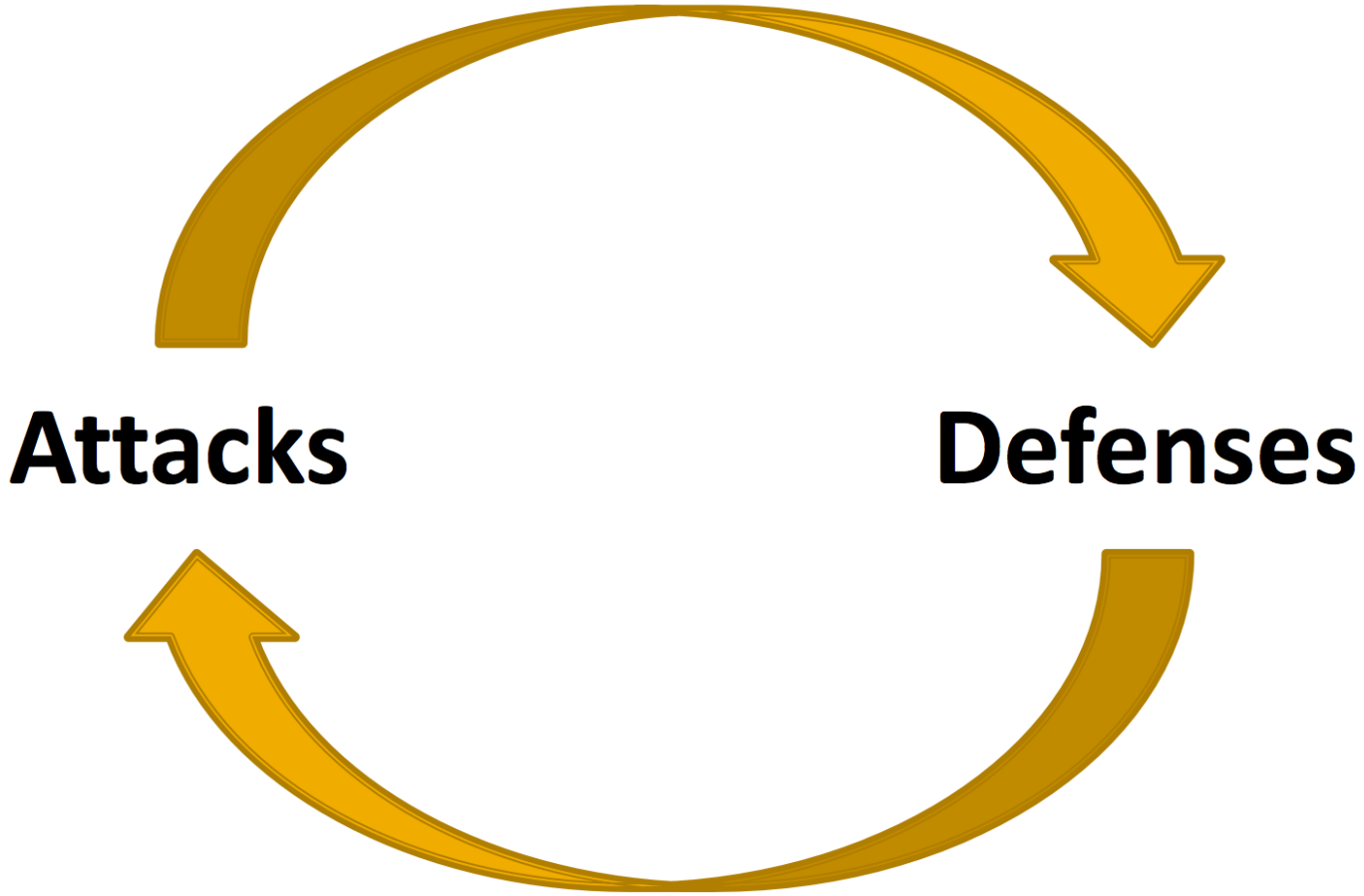
- Academia
- Industry
- Military
- Hobbyists
- Bad guys…

“Insecurity”?

Hierarchy



High Level Approach



Why Study Attacks?

- Identify vulnerabilities so they can be fixed.
- Create incentives for vendors to be careful.
- Learn about new classes of threats.
- Determine what we need to defend against.
- Help designers build stronger systems.
- Help users more accurately evaluate risk.

Thinking Like an Attacker

- Look for weakest links – easiest to attack.
- Identify assumptions that security depends on. Are they false?
- Think outside the box: Not constrained by system designer's worldview. Practice thinking like an attacker:
  - For every system you interact with, think about what it means for it to be secure, and image how it could be exploited by an attacker.

RATIONAL PARANOIA

Think Like an Attacker

- Breaking into the CSE building?
- Stealing my password
- What are some security systems that you interact with in everyday life?

Thinking as a Defender

- Security policy
  - What are we trying to protect?
  - What properties are we trying to enforce?
- Threat model
  - Who are the attackers? Capabilities? Motivations?
  - What kind of attack are we trying to prevent?
- Risk assessment
  - What are the weaknesses of the system?
  - What will successful attacks cost us?
  - How likely?
- Countermeasures
  - Costs vs. Benefits?
  - Technical vs. nontechnical? Challenge is to think rationally and rigorously about risk. Rational paranoia.

Thinking As a Defender

- Should you lock your door?
  - Assets?
  - Adversaries?
  - Risk assessment?
  - Countermeasures?
  - Costs/benefits?
- Using a credit card safely?

Secure Design

- Common mistake:
  - Trying to convince yourself that the system is secure
- Better approach:
  - Identify the weaknesses of your design and focus on correcting them
- Secure design is a process
  - Must be practiced continuously; can’t be retrofitted

Where to Focus Defenses

- Trusted components
  - Parts that must function correctly for the system to be secure.
- Attack surface
  - Parts of the system exposed to the attacker
- Complexity vs. security?

Current Security Events and Upcoming Research Areas

theguardian

opinion sports soccer tech arts lifestyle fashion business travel environment ≡ browse all sections

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

● Major cyber attack disrupts internet service across Europe and US

Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

WIRED Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

BUSINESS CULTURE DESIGN GEAR SCIENCE

SHARE

SHARE 604

TWEET

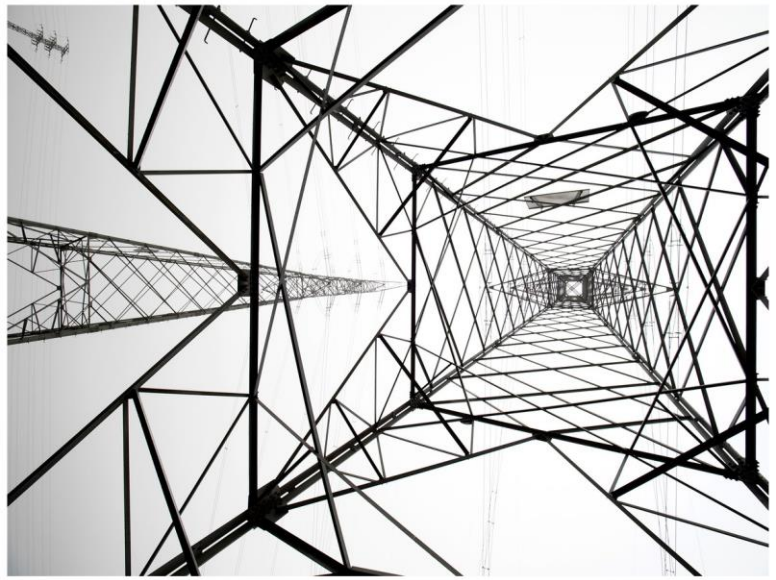
PIN 2

COMMENT 96

EMAIL

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



Security for ML

- Adversarial Perturbation
- Robust Model Design

Reading a research paper

- What to do
  - Read Critically
  - Read Creatively
  - Make Notes
  - Get the Main Idea
  - Compare to Other Works
- What not to do
  - Trash the paper

http://www.eecs.harvard.edu/~michaelm/postscripts/ReadPaper.pdf

The Three Pass Approach

- First Pass
  - Carefully read title, abstract, Intro
  - Read headings, conclusion
  - Glance at maths & references
  - Answer the 5 C’s
    - Category
    - Context
    - Correctness
    - Contributions
    - Clarity

http://blizzard.cs.uwaterloo.ca/keshav/home/Papers/data/07/paper-reading.pdf

The Three Pass Approach

- Second Pass
  - Read with greater care
  - Ignore proofs
  - Write down key points/questions
  - Look carefully at figures/diagrams
  - Mark relevant references you may want to read
  - Takes a couple of hours in the beginning; will become faster as you become more experienced
  - Should be enough to review the paper

The Three Pass Approach

- Third Pass
  - Virtually reimplement the paper
  - Identify strong and weak points
  - Identify and challenge every assumption
  - How would you present it differently?
  - Write down ideas for future work

Presenting a Research Paper

- Look for presentation video/slides online; cold-email authors!
- Communicate the key ideas
- Don’t get bogged down in details
- Structure your talk
- Know your audience
- Do the full three pass so you can answer any question

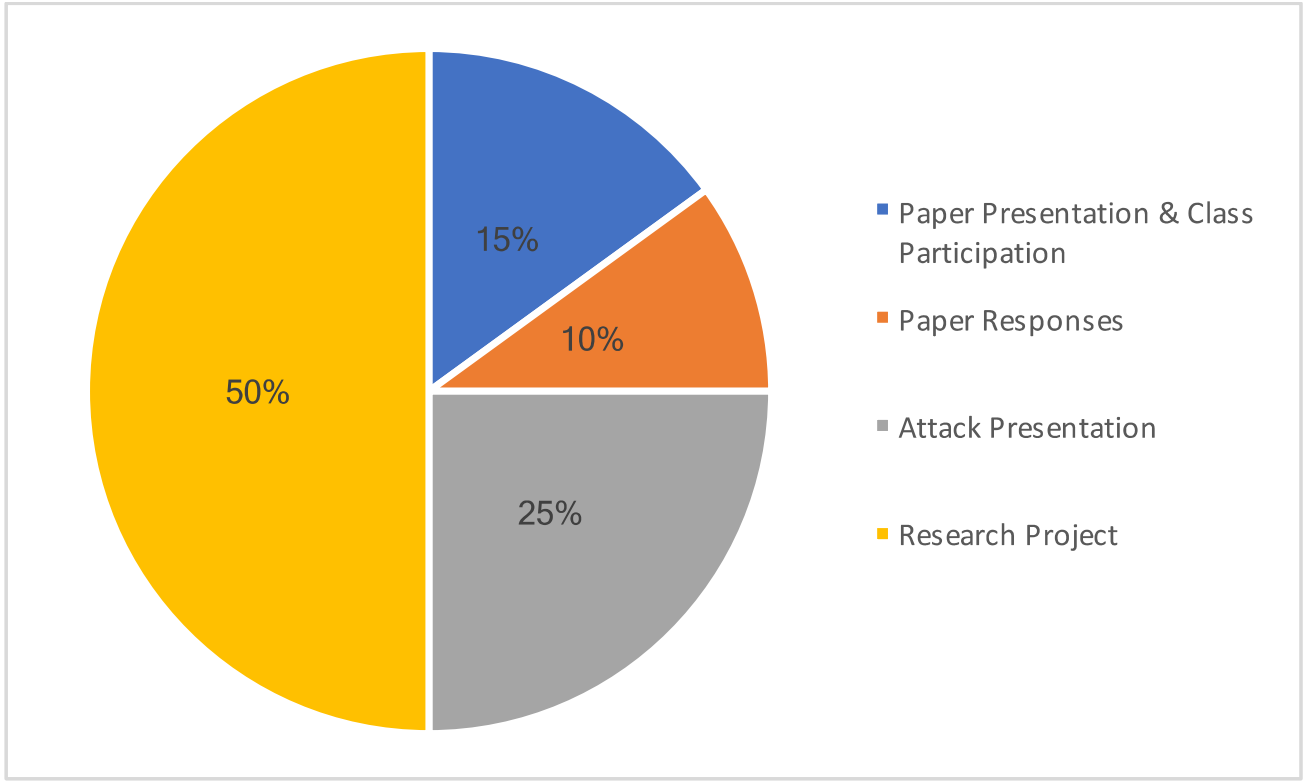
https://www.sfu.ca/~jeffpell/Ling480/ParberryMembrane.pdf

Recall Goals for This Course

- Gain hands-on experience
  - Building secure systems
  - Evaluating system security
- Prepare for research
  - Computer security subfield
  - Security-related issues in other areas
- Generally, improve research, writing, and presentation skills
- Learn to be a 1337 hax0r, but an ethical one!

Grading

- Paper presentation & class participation (15%)
- Paper Responses (10%)
- Attack Presentation (25%)
- Research Project (50%)



Paper Presentation & Class Participation (15%)

- Every student must present a paper during the semester
  - 30 minutes time slot (including Q&A)

- ~2 required papers for discussion in each session (other readings optional but recommended)
  - Everyone should come prepared to contribute!
  - Full points for speaking up and contributing substantial ideas
  - Lose points for being silent, missing class, Facebook, etc.

Paper Responses (10%)

- Brief written response to each paper (~400 words)
- In the first paragraph
  - State the problem that the paper tries to solve; and Summarize the main contributions.
- In one or more additional paragraphs
  - Evaluate the paper's strengths and weaknesses
  - Discuss something you would have done differently if you had written the paper
  - Suggest interesting open problems on related topics.
- You will be grading each other’s review

Attack Presentation (25%)

- With a partner, choose a specific attack from recent research and implement a demonstration

- Give a 15 minute presentation
  - describe the attack
  - talk about how you implemented it, give a demo
  - discuss possible defenses
  - Course website contains list of topics
  - Each group send me ratings for each choice by Monday the 16th

Research Project (50%)

- In groups, investigate new attack/defense/tool
  - Aim for a publishable workshop paper.
- Components (more detail on website):
  - Preproposal presentation
  - Project proposal
  - Project checkpoint
  - Workshop-style presentation in class
  - Final workshop-style report

Target a USENIX Security Workshops

Deadline typically in May

IoT Home Inspector Challenge

- Criteria
- Judges
- Rules
- FAQ's
- Registration and Submission

IoT Criteria

CRITERIA SUMMARY

See the Rules for complete details of what is required, what is prohibited, and the full Judging Criteria.

Threshold Solution Criteria – in order to be considered.

- Submissions must provide a technical solution, rather than a policy or legal solution.
- The tool must work on home IoT devices that currently exist on the market.
- The tool must protect information it collects both in transit and at rest.
- The Submission must address how the tool will avoid or mitigate any additional security risks that the tool itself might introduce into the consumer's home by, for example, probing the home network or facilitating software upgrades.

a. The Abstract. The abstract should include a title for the Submission and a brief explanation of how the tool functions.

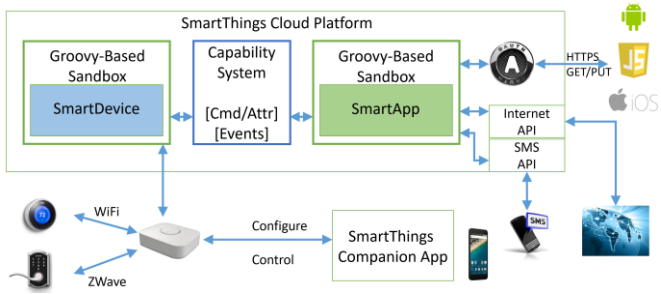
b. The Video. The video need only demonstrate how the tool would be used with one (1) IoT device that is likely to be found in consumers' homes.

FTC IoT Challenge

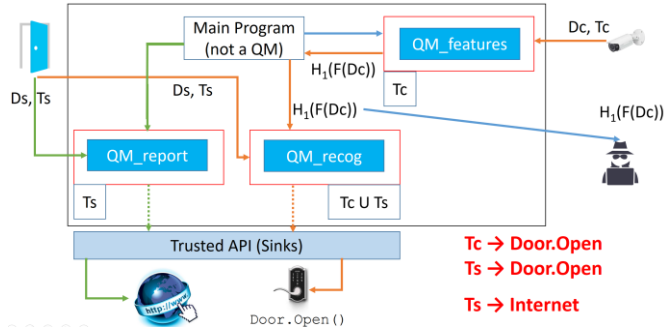
- Your course project can be an entry for this competition!
- 25K prize! (3K for runners ups)
- Deadline for project submission is May 22, 2017

https://www.ftc.gov/node/1010523

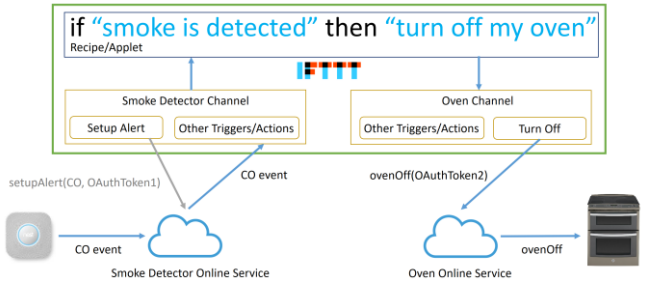
Our Research



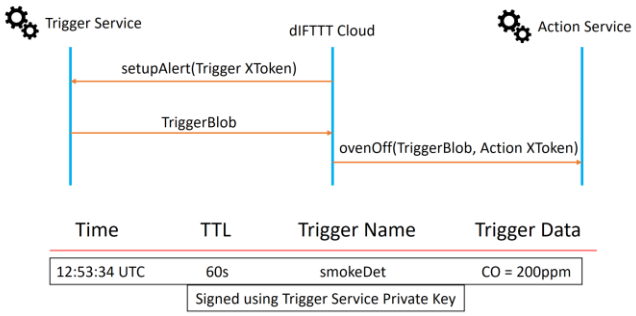
SmartThings Analysis



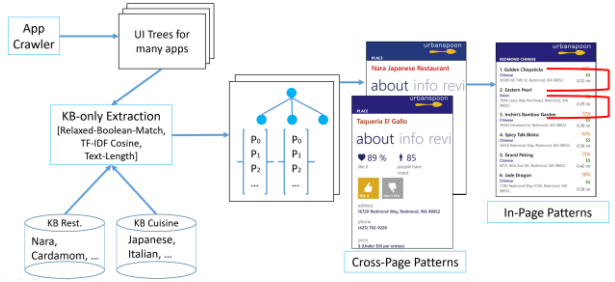
FlowFence



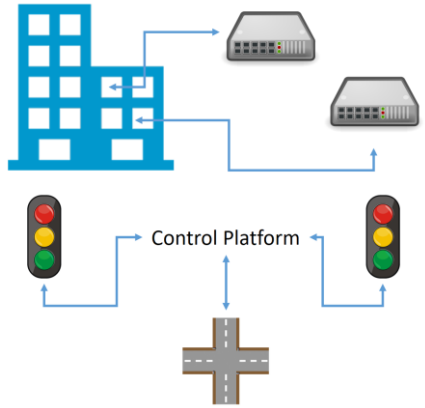
IFTTT Analysis



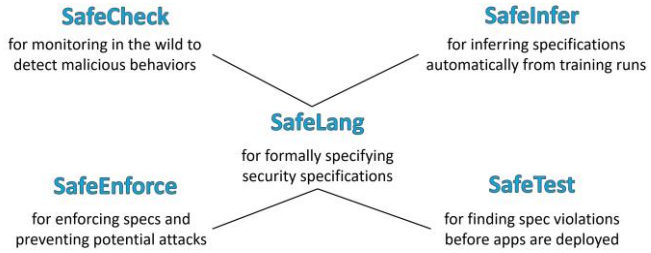
Decoupled-IFTTT



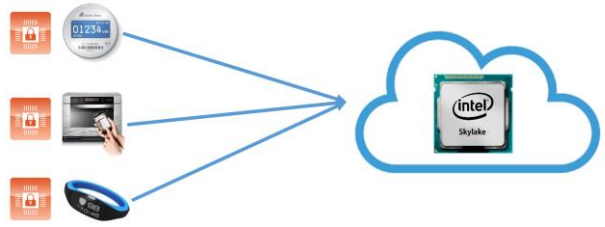
Appstract



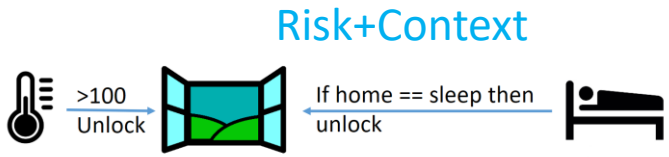
Large-Scale IoT Platform Security



Fail-Safe Security



Tamper-Proof Audit



IoT Permission System Improvements

Communication

- Course Web Site https://eecs.umich.edu/courses/eecs588/
  - schedule, reading list, reading response submission
- Piazza
  - announcements, discussion, find a partner or group
- Email Us
  - eecs588.w17@umich.edu administrativia, suggestions, questions, concerns

Law & Ethics

- Don’t be evil!
  - Ethics requires you to refrain from doing harm
  - Always respect privacy and property rights
  - Otherwise **you will fail the course**
- Federal/state laws criminalize computer intrusion, wiretapping
  - e.g. Computer Fraud and Abuse Act (CFAA)
  - You can be sued or go to jail
- University policies prohibit tampering with campus systems
  - You can be disciplined, even expelled
- Talk to us if you have any questions

Your Assignments

- First paper Review due Tuesday (2 IoT papers)
  - See course site for required reading (under construction)
  - Submit written responses by start of class!
- Full paper schedule available by Friday
  - email topic ratings by 5pm on Tuesday
- Find a partner and rate the topics for attack presentation
  - email topic ratings by 5pm on Monday the 16th
- Start thinking about your course project
  - Form a group, present topic idea February 16 in class