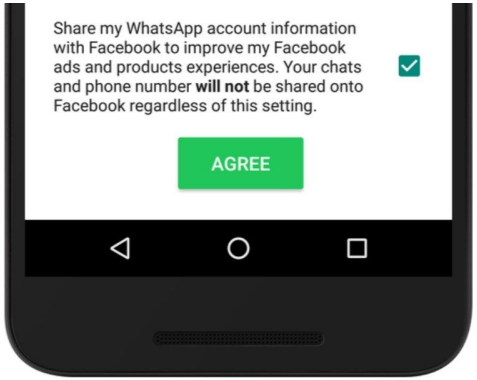
Future Crimes

Regina Lin, Sierra Mills, Kenan Saleh,
Saranya Sampath, Vignesh Valliyur,
Robert Zajac

A Gathering Storm

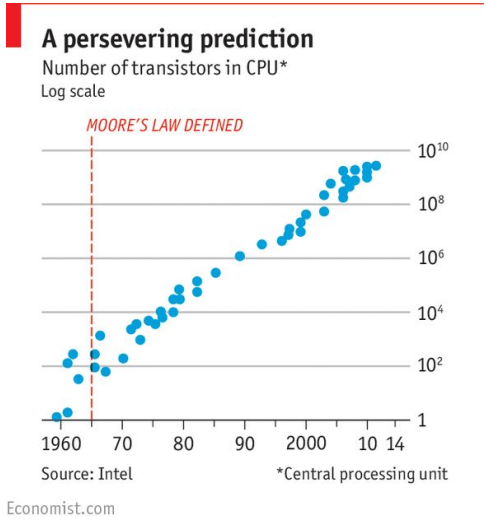
Dependency on technology makes us vulnerable to crime

- Increasing number of “blind” consumers who don’t even know what precautions to take
  - Facebook data sharing
  - Anti-virus services
- As technology takes over more roles of our life, we only become more exposed to potential crimes



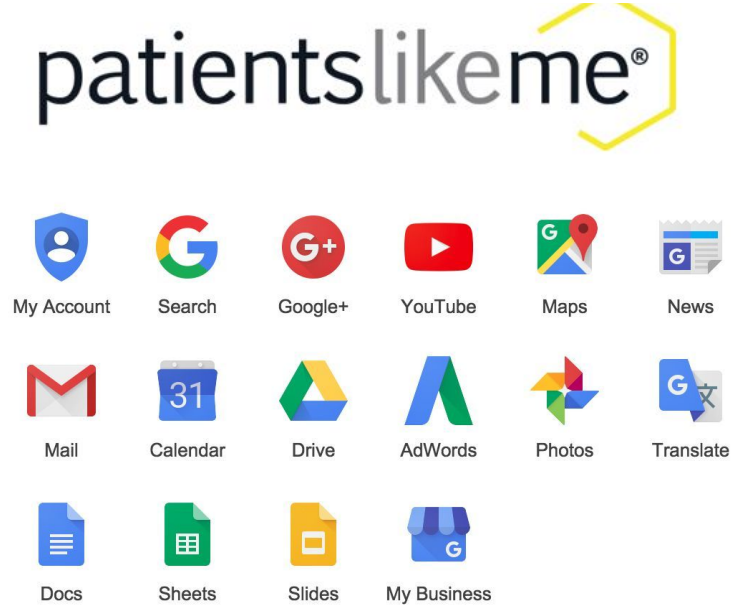
Moore’s Law Benefits Hackers More than Developers

- Advancing technology only augments the asymmetric problem of computer security
  - A hacker only has to find one flaw, a developer has to protect against all possible weaknesses
- As the world runs more and more on code, controlling the code means controlling the world
  - AI crime singularity



You're not the customer, you're the product

- Case Study: Bilal Ahmed
  - Suffered from anxiety, depression, after death of mother
  - PatientsLikeMe.com
- Privacy Policy:
  - "You should expect that every piece of information you submit (even if it is not currently displayed) may be shared"
- Google
  - **"You are not Google's customer; you are its product. That's why you don't get a bill."**

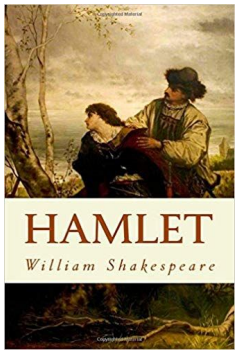


You're not the customer, you're the product

- Terms of Services: purposefully long, you may be agreeing to things you didn't mean to.
- How long are they?

9300

36,275



30,066

You're not the customer, you're the product

- **LinkedIn:** "You grant LinkedIn a nonexclusive, irrevocable, worldwide, perpetual, [...] right to us to copy, prepare derivative works of, improve, distribute, publish, [...] any information you provide, directly or indirectly to LinkedIn. [...] Any information you submit to us is at your own risk of loss"

- **GameStation UK:**

  "By placing an order via this GameStation Web site on the first day of the fourth month of the year 2019 Anno Domini, you agree to grant us a non transferable option to claim, for now and for ever more, your immortal soul, should we wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (give) working days of receiving written notification from gamestation.co.uk or one of its duly authorised minions"

The Surveillance Economy

- Data Brokers
  - Acxiom, Epsilon, Datalogix
  - Acxiom collects > 50 trillion unique data transactions yearly
  - Goal: “behavioral targeting”, sell data to marketers
- Target Case Study
  - Target sent teenager coupons for pregnancy-related items
  - “Pregnancy Prediction Score”
  - Great for Target/marketers, not necessarily great for consumers
- **“The more data you produce and store, the more organized crime is happy to consume”**
- Organized crime
  - Posting where you’re going for vacation on Facebook, Twitter
  - Google’s Street View

Who’s Watching You?

- Mobile phones and personal devices
  - Operating systems and app stores
    - Android updates vs. iOS
    - App security screening
    - Flashlight app and permissions
  - BYOD in workplaces
- Locations
  - Photo embeddings and family-tracking
  - Automatic license plate reader (ALPR)
  - Retail tracking
- Big Data and the Cloud
  - Edward Snowden and the NSA
  - Where does our data go?

Screen Dependency, A Fake Reality

- Blind trust in a black-box society
  - Stuxnet and Iran's nuclear power plant, Natanz
  - Internet censorship and collaborative filtering
    - Government bans
    - Sock puppetry
  - Robin Sage experiment
- Man-in-the-middle attacks
  - Data alteration
    - Credit, medical, criminal
    - TSA checks
  - GPS jamming and spoofing
    - Traffic rerouting
  - Phishing
    - Deputy President of Coca-Cola

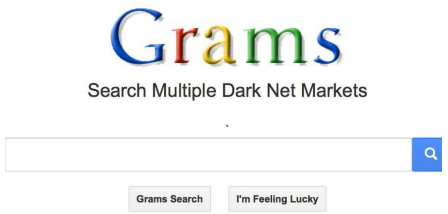
The Modern Criminal

Crime, Inc.

- **Why is cybercrime so pervasive? Low risk, high reward.**
  - Borderless
  - Anonymous
  - Rare prosecutions (less than 1/1000th of 1 percent of all cases)
- Cybercrime enterprises are sophisticated
  - Case Study: Innovative Marketing
    - $180 million in revenue in 2009 (vs. $106 million earned by Twitter in 2011)
- Cybercrime infrastructure is extensive and organized

Inside the Digital Underground

- TOR (The Onion Router)
- Deep Web
  - Google searches give you 0.03% of information actually in existence
  - Search engines cannot index into password / paywall protected information
- Dark Web
  - Silk Road (“ebay of drugs and vice”)
  - Grams (distributed search engine modeled after Google)
- Virtual currencies (Bitcoin, Darkcoin)
- **Crime as a Service (CaaS)**
  - Web hosting
  - Cloud computing
  - Software developers
  - Hacking toolkits (phishing, spam, DDoS, data theft), zero-day exploits
  - Botnets
- **Cybercrime imperils a world that is increasingly connected**



When All Things Are Hackable

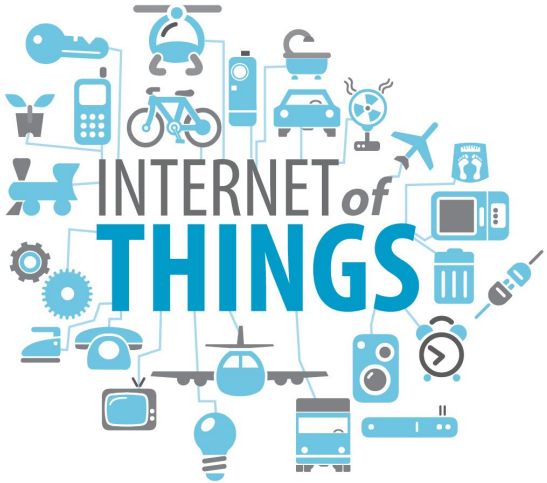
- **What is IoT (Internet of Things)?**

  Pew Research Center: "global, immersive, invisible, ambient networked computing environment built through the continued proliferation of smart sensors, cameras, software, databases, and massive data centers in a world-spanning information fabric"

- **Modern networked homes**

Implications of IoT

- Quality of life
- Privacy / Data
  - When / what data is being collected?
  - Who owns the data?
- Tracking objects AND people
  - Real space = cyberspace
  - “Perfect enforcement”
- Looking to the future:
  - Smart cities
  - More connections = more vulnerabilities (IPv6)
- **Internet of Things = Internet of Things to be hacked**



The Future of Crime

What happens when Black Mirror becomes reality?

Hacking you

The internet of things will change everything - including ourselves

- The thesis is simple - with the expansion of technology, the number of things that can go wrong increases dramatically. Basically Moore's law on steroids
- **Technology becomes one with the body -**
  - IMD - implanted medical devices, wearables (fitbit, apple watches), ICD - implanted cardioverter defibrillator
- **Biometric Systems -**
  - Fingerprint systems and databases - Aadhar in India
  - Facial recognition software
  - Voice recognition and patterns

Rise of the Machines

- **The propagation of Robots**
  - It’s not just going to be your Roomba
  - They are going to pop up everywhere - surgery bots, self driving cars, military bots
- **Drones everywhere**
  - Terrorism may get a facelift
  - How does this change notions of privacy?
  - Significant ethical and legal questions? Who do we sue if a driverless car causes an accident?
- **3-D printing**
  - Massive loss of intellectual property
  - People can make their own guns

Next Generation Security Concerns

- AI
- Bio Computing
- Nanotechnology and Quantum Computing

Surviving Progress

How can we protect users within our current systems?

Problems thus far

The picture is bleak

Technology can be used for good...

ebay

Until it's not...

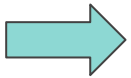
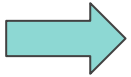
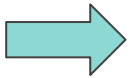
Bad actors need only find ***one*** vulnerability

We need to protect against ***all*** vulnerabilities

Complexity is increasing ***rapidly***

What can we do?

Methodological Approaches

“Move fast and break things.” *Facebook*	 *Reducing complexity*	Move as fast as you can while retaining good practices.
“We’re only human, there is no such thing as perfect software.” *Developers*	 *Managing expectations*	We’re only human, but we’re not even 50% of the way to perfect software, and we can do better.
“We do not guarantee that our product will always be safe, secure, or error-free.” *ToS*	 *Aligning incentives*	Guaranteeing the safety of our products is in the best interest of our bottom line.

What can we do?

Technical Approaches

Data privacy

a. Better practices around data collection
    i. Reduce data collection -> reduce value of breaches
    ii. Enforcing standards around data rights (e.g. GDPR)
b. (In-class) Extract insights from data while preserving privacy
    i. Differential privacy!

Better “passwords” - our key to the online world

a. Multi-factor authentication
b. Biometrics

More encryption - “locking” data

a. Many corporations still store data in plaintext
b. HTTPS Everywhere
    i. Securing the web

What can we do?

Institutional Approaches

More cybersecurity education

a. Human factor is biggest weakness in securing systems
    i. Using infected USBs, clicking on phishing links, etc.

Better electronic policing

a. Hackers easily move ***between countries***, but police forces cannot
b. Global forces like Interpol are dramatically underfunded
    i. Operating budget of $90 million to fight all international crime
    ii. El Chapo, upon arrest, had $200 million of cash in his home

Solution: “Cyber CDC”

a. One organization owns: education, networking monitoring, threat “immunization”, incident response
b. Recruit technologists

The Way Forward

How will we build safe systems in the future?

Rethinking organizations

Building secure groups for the 21st Century

Shift focus from prevention -> detection

a. Breaches will happen inevitably
b. Current detection time > 200 days
c. Disassociate stigma with data breaches -> encourage disclosure

Building resilient products and organizations

a. Should not have central points of failure
    i. E.g. Target HVAC

Government, and private-sector collaboration

a. Stimulate innovation in government before criminals (and foreign states) outpace us
b. 85% of U.S. critical infrastructure owned privately
c. Better information sharing, aligned incentives -> stronger security effort

Rethinking individuals

The power of crowdsourcing

Leverage the joint efforts of millions of citizens.

Gamification

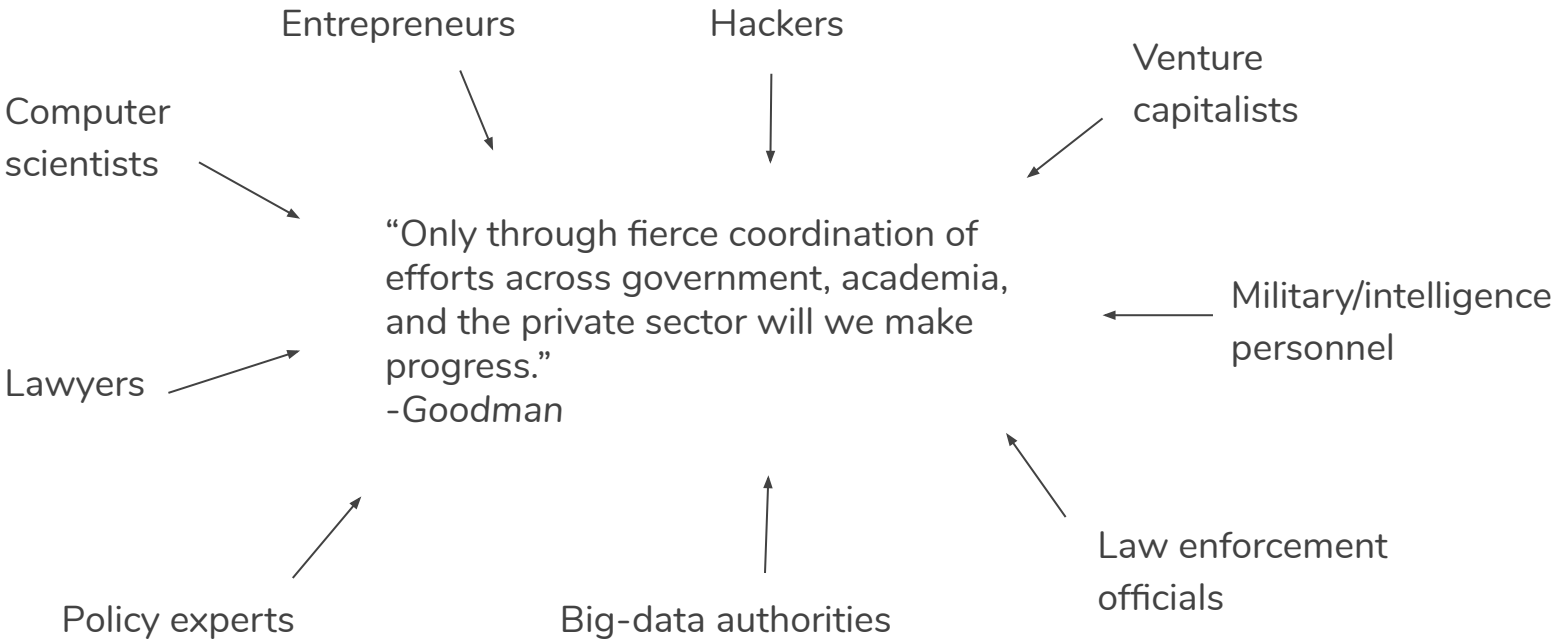
a. Build “games” with rewards to identify cybersecurity threats
b. E.g., *MalariaSpot*: crowdsourced Malaria detection game
    i. Over 700,000 detections made

Incentive competitions

a. XPRIZE Foundation: creates prize competitions
    i. Original XPRIZE: $10 million to launch a manned spaceship (only 100km high) and return
    ii. Next: cybersecurity XPRIZE

A Manhattan Project for Cyber

Call to action



“Let no one be discouraged by the belief there is nothing one person can do against the enormous array of the world’s ills, misery, ignorance, and violence. Few will have the greatness to bend history, but each of us can work to change a small portion of events. And in the total of all those acts will be written the history of a generation.”
-Robert F. Kennedy

Thank you!

Questions?