Introduction to Cybersecurity
IO Seminar – Spring 2016

- Background
- Some Research
- Cybersecurity in Israel

Neil Gandal – January 2016

Background - Cybersecurity

- Much of the work in the field has been undertaken by computer scientists/engineers and legal scholars
- Nascent literature at the "intersection" of computer science/engineering and economics on cyber security.
- Why Economists?
- Ross Anderson: "As systems scale globally, incentives start to matter as much as technology. Systems break when the people who could fix them are not the people who suffer the costs of failure. So it's not enough for security engineers to understand crypto, mathematics and the theory of operating systems; we have to understand game theory and microeconomics too. This has led to a rapidly growing interest in 'security economics' "

Viruses: huge potential damages

- The Slammer, Blaster, and Sobig.F viruses exploited vulnerabilities even though security updates had been released.
- According to the Economist, the vulnerabilities exploited by these viruses were reverse engineered by hackers.
- Time between the disclosure of a vulnerability and an attack exploiting the vulnerability has declined significantly.
- Zero-day vulnerabilities

Economics & Public Policy of Cybersecurity

- Why has Internet security worsened even as investment has increased?
- According to a report from the US Secret Service, nearly 2/3 of all data breaches could have been prevented using "simple and cheap" countermeasures. Why aren't they deployed?
- How much should firms invest to protect IT systems?
- How can the past history of cyber incidents guide future investments in defense?
- With cyber/information security breaches in the news almost every day, the question of optimal cybersecurity policy has attracted the attention of academics, corporate decision makers, and nation states.

The Economics & Public Policy of Cybersecurity

- Appropriate Liability Regime
- Researchers have come to realize that the cause of cyber/information security breaches is often not a failure of technology, but rather an absence of appropriate incentives.
- Economics is essential to answering these questions, which seem 'technical' at first glance. But systems often fail because the organizations that defend them do not bear the full costs of failure. This means that incentives are not aligned correctly.
- In order to solve the problems of growing vulnerability and increasing crime, solutions must allocate responsibilities and liabilities so that the appropriate organizations to fix problems have an incentive to do so.

RESEARCH
Network Security, Vulnerabilities and Disclosure Policy (Choi, Fershtman, Gandal)

- Vulnerabilities major concern since attackers can cause substantial damages.
- Firms face a disclosure dilemma:
  - Disclosing vulnerabilities and issuing updates protects consumers who install updates.
  - Not all consumers necessarily install updates
  - Disclosure facilitates reverse engineering by hackers.

Research Goals

- Examine the incentives for a firm to disclose software vulnerabilities. Key tradeoff: "disclosure" provides protection, but also increases probability of attack.

- Disclose and issuance of updates endogenously changes the value of software, increasing it for high-value users (who will employ updates when available) and decreasing it for low-value users (who will not employ updates)

- Examine effects of regulatory policy that requires mandatory disclosure (Is it Desirable?)

- Investigate how changes -- in (I) number of vulnerabilities & (II) probability the firm identifies problems before hackers -- affect disclosure policy

Research Continued…

Rebuilding Trust in Computing Platforms

Eran Tromer

LEISec

Laboratory for Experimental Information Security

TEL AVIV UNIVERSITY

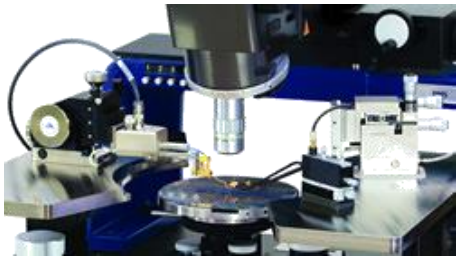
Analyzing vulnerabilities

- Physical leakage from PCs and phones
- Leakage in cloud computing
- Internet auctions

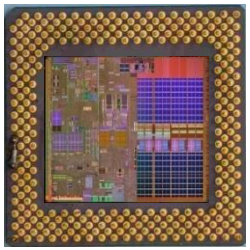
Building secure systems

- Preventing leakage
- Secure digital currency
- Secure CPU enclaves
- Verified+private cloud computing
- Mobile phone security
- Authenticating images
- Wireless network protocols

Side channel attacks



CPU architecture



probing

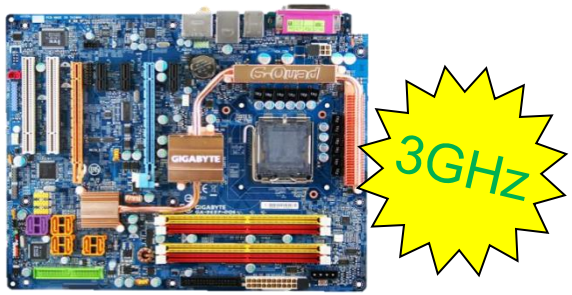
optical

electromagnetic

power

acoustic

- Small devices (smartcards, embedded, chips)
- Peripherals
- **Computation on PCs?**



Stealing secret keys using microphones

[Genkin shamir Tromer 2014]

Stealing encryption keys from 10 meters away

or using a smartphone

Shocks to and Security in the Bitcoin Ecosystem:
Neil Gandal (Tel Aviv University) and Tyler Moore (Tulsa)

- Recent rise in digital currencies, led by the introduction of Bitcoin in 2009, creates an opportunity to measure information security risk in a way that has often not been possible in other contexts.
- Digital currencies aspire to compete against other online payment methods such as credit/debit cards and PayPal, as well as serve as an alternative store of value.
- They have been designed with transparency in mind, which creates an opportunity to quantify risks better.
- In practice the ecosystem is vulnerable to thefts by cybercriminals, frequently targeting intermediaries such as wallets or exchanges.

RESEARCH QUESTIONS

- **Question 1: What are the shocks that affect Bitcoin, and when have they occurred historically?**
- **Question 2: How do shocks disrupt the ecosystem, and how can their effects be measured?**
- **Question 3: How might self-interested participants abuse cryptocurrency financial instruments to carry out deliberate shocks? Is there any evidence that such strategies are being or have been employed?**

The Internet of Things:

- 15 (50) Billion devices connected to the Internet in 2015 (2020)
- Such devices, like "Smart TVs" are not designed as computers
- Hence, they do not come with antivirus software. Indeed, there is no antivirus software available.
- Many such devices lack the ability to be "patched." So even if vulnerabilities are found, it is not possible to fix them
- Security "after the fact" is difficult and expensive

- **What incentives would make IOT less vulnerable?**
- Basic Regulatory Standards:
  - Devices must be capable of being "patched"
  - Security Breach disclosure laws should be expanded to cover IOT
- Liability Regime:
  - As software becomes integrated into (say) medical devices, it will not be possible for software companies to write licensing agreements disclaiming responsibility for everything bad than can happen.
- Provide incentives to write secure code.
- Develop Institutions like CMU's CERT.

Cybersecurity in Israel

- Israeli firms are dominant in worldwide industry. (Article in Fortune)
- Cybersecurity is important for the economy, and provides high-quality jobs for skilled workers – and fights the "brain drain."
- There are mature companies like Check Point
- There are venture capitalists which focus on cyber Jerusalem Venture Partners (JVP) Cyber Labs;
- There are research collaborations (Deutsche Telekom Innovation Laboratories activity at Ben-Gurion University. This array of expertise has turned heads, worldwide.)
- Government support of science & science education→ most major IT vendors have research facilities in Israel

CYBERSECURITY & ISRAEL
5th Annual International Cybersecurity Conference

June 22nd-25th, 2015 Smolarz Auditorium ,

Tel Aviv University, Israel

Sponsored by:

KETER

Check Point SOFTWARE TECHNOLOGIES LTD. · CYBERBIT PROTECTING A NEW DIMENSION · EMC² RSA · IAI ISRAEL AEROSPACE INDUSTRIES · IBM · intel Security

LOCKHEED MARTIN · Microsoft · QUALCOMM · TEAM8 · VERINT

CYBERARK · SOPHOS · ThetaRay · YL VENTURES

AGC PARTNERS · Glilot Capital Partners · IATA

Media partner:
In association with:

TheMarker · Cellcom · 22 LIVE

anantа · ISRAEL-AMERICA Chamber of Commerce · ISRAEL-BRITAIN CHAMBER OF COMMERCE · CII Confederation of Indian Industry · comtec · CYBERLY · ITA

MINISTRY OF ECONOMY · ENTERPRISE FORUM ISRAEL · NOVAWIND · SAGIVTECH · StarTau