Successes and Challenges of Computer Security Research

Stefan Savage
UC San Diego

What do we mean when we say "security"?

UCSDCSE
Computer Science and Engineering

What do we mean when we say "security"?

- Merri

Fre
Fre **y**

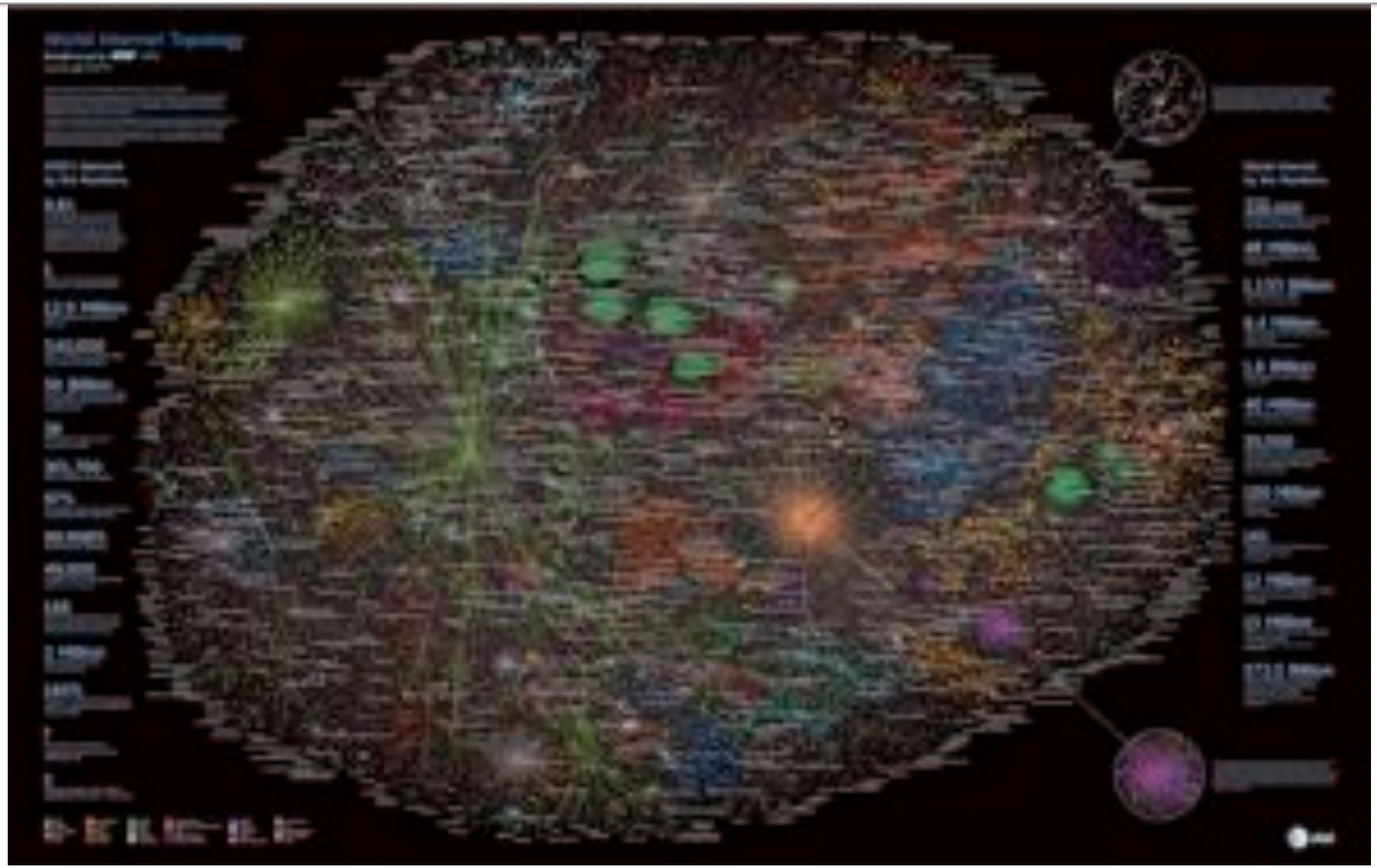
fulfillm
3 : an i s a stock certifi
4 a : sc s taken to guard e (2) **:** an organi

UCSDCSE
Computer Science and Engineering

Technological change = new dangers and new fears

UCSDCSE
Computer Science and Engineering

The big change: global connectivity



UCSDCSE
Computer Science and Engineering

Managing risk

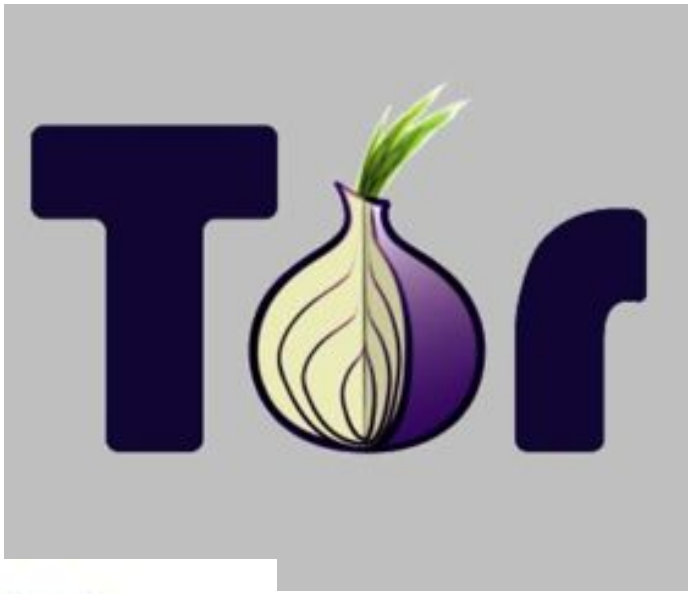
Example: e-commerce

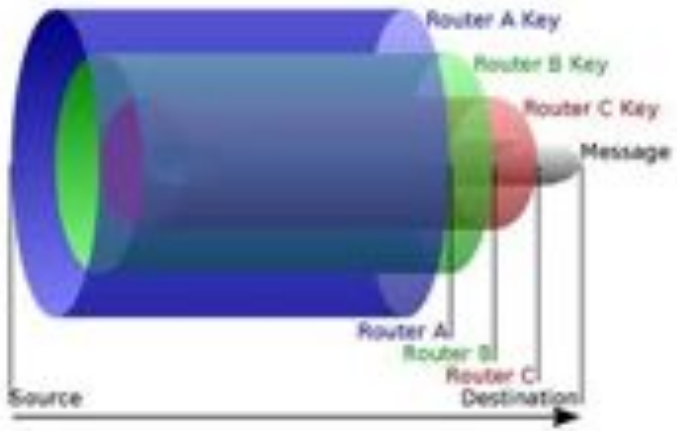
What made this possible?

- Public-key cryptography
- Efficient private-key cryptography
- Key-exchange protocols
- Certificate authorities and trust hierarchies

UCSDCSE
Computer Science and Engineering

Example: anti-censorship





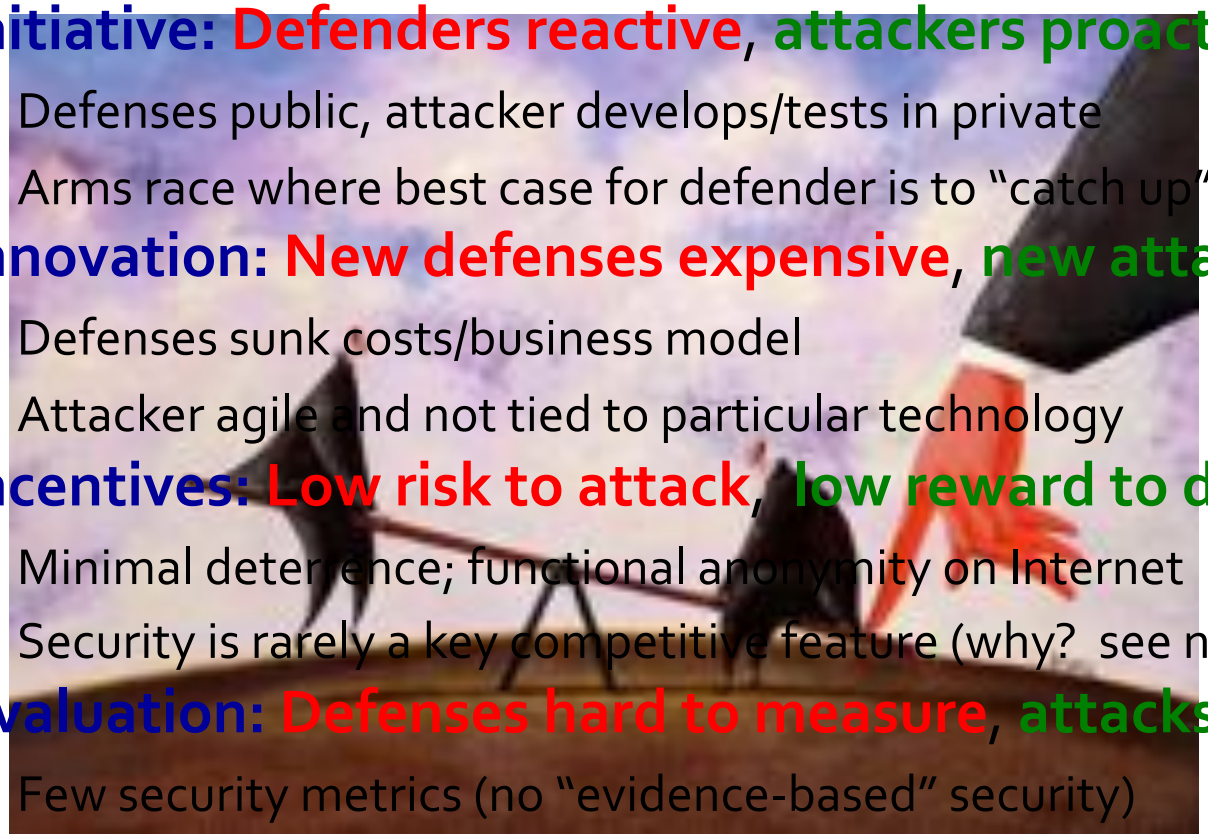
UCSDCSE
Computer Science and Engineering

NITRD efforts underlie most of today's defensive technologies

- Virtual private networks
- Network defenses
  - Firewalls, intrusion detection, data leakage protection
- Two-factor authentication
- Anti-malware
- Exploit mitigation (ASLR, DEP, stack cookies)
- Vulnerability finding tools, safe languages
- Virtual machine isolation

UCSDCSE
Computer Science and Engineering

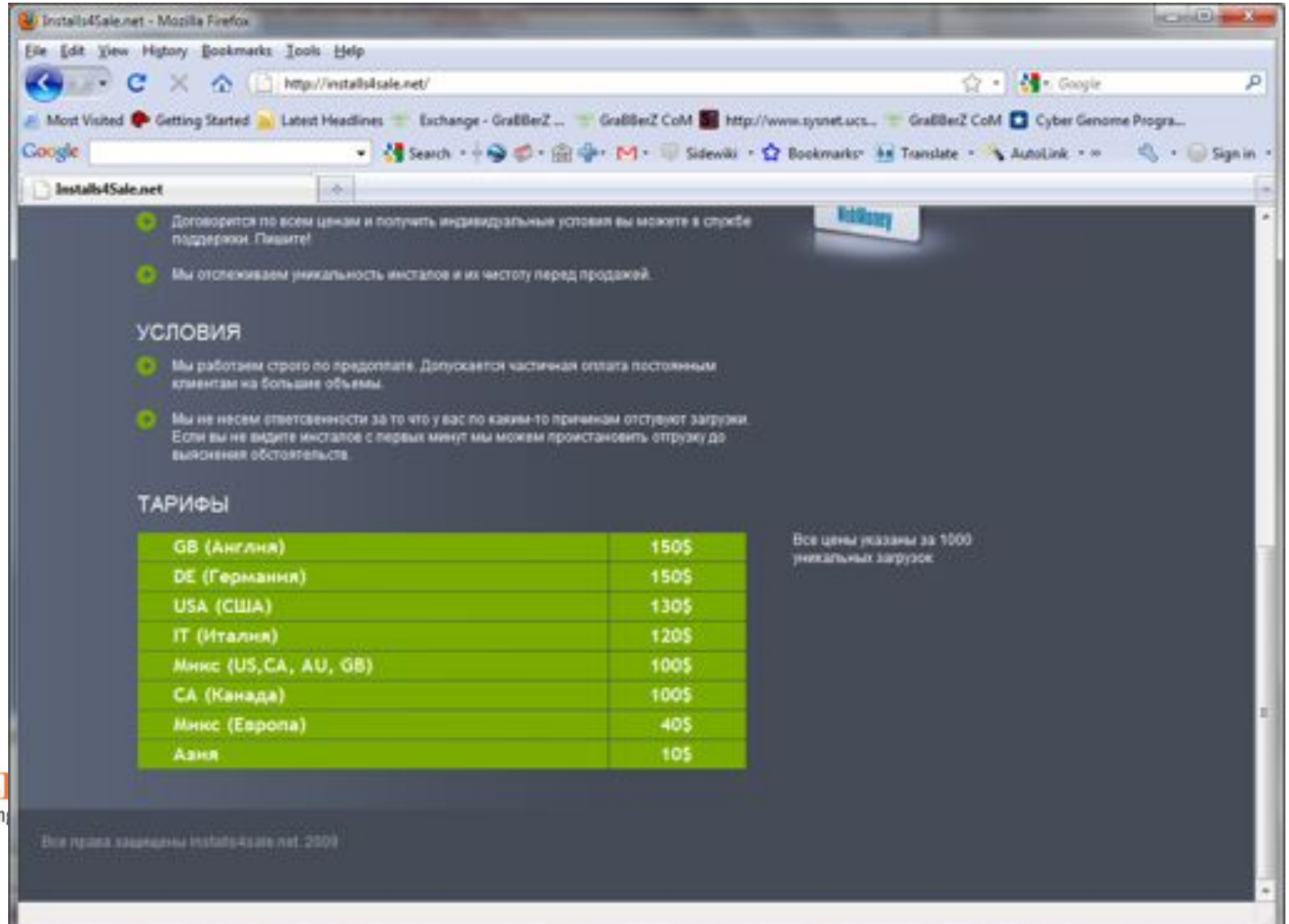
Challenge: structural asymmetries



- **Initiative: Defenders reactive, attackers proactive**
  - Defenses public, attacker develops/tests in private
  - Arms race where best case for defender is to "catch up"
- **Innovation: New defenses expensive, new attacks cheap**
  - Defenses sunk costs/business model
  - Attacker agile and not tied to particular technology
- **Incentives: Low risk to attack, low reward to defend**
  - Minimal deterrence; functional anonymity on Internet
  - Security is rarely a key competitive feature (why? see next)
- **Evaluation: Defenses hard to measure, attacks easy**
  - Few security metrics (no "evidence-based" security)
  - Attackers measure success/monetization which drives attack quality

Challenges: new adversaries

- E-crime as a business



UCSDCSE
Computer Science and Eng

Challenges: new adversaries

- E-crime as a business

UCSDCSE
Computer Science and Engineering

Challenges: new adversaries

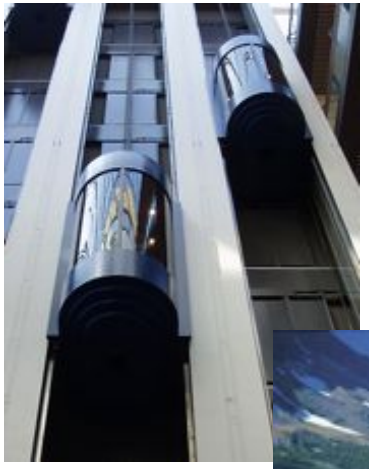
- Mass action/hacktivism

UCSDCSE
Computer Science and Engineering

Challenges: new adversaries

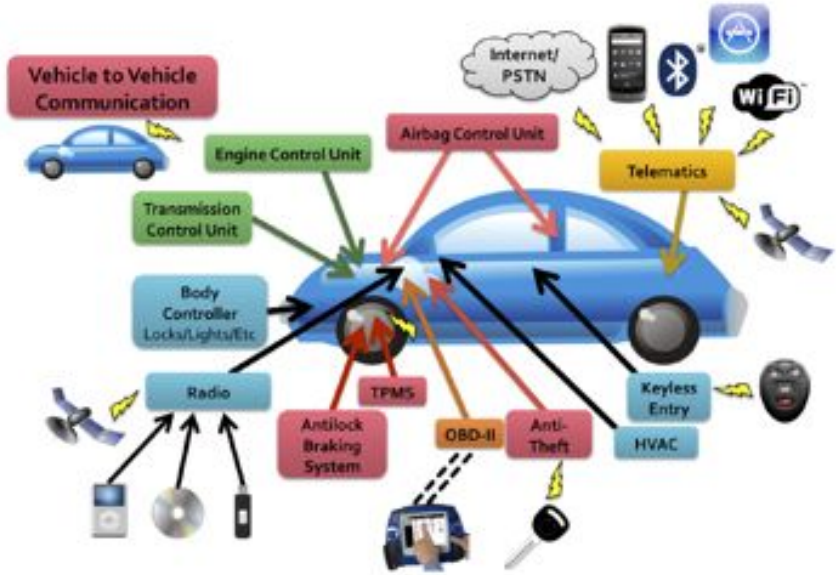
- State-motivated/sponsored actors

Challenges: the Internet of things



UCSDCSE
Computer Science and Engineering

Computer security meets the real world



UCSDCSE
Computer Science and Engineering

The value of security research

- Security is a game of innovation
- Keeping up, staying ahead; readiness

…down the road, the cyberthreat, which cuts across all [FBI] programs, will be the number one threat to the country."

-- Robert Mueller, Jan 31, 2012

UCSDCSE
Computer Science and Engineering

Thank you

- Questions?