

# Successes and Challenges of Computer Security Research

Stefan Savage  
UC San Diego

# What do we mean when we say "security"?



# What do we mean when we say "security"?

- Merriam-Webster

*Fre*  
*Fre*

fulfillm  
3 : an i  
certific  
4 a : so  
guard  
organi



is a stock

is taken to  
e (2) : an

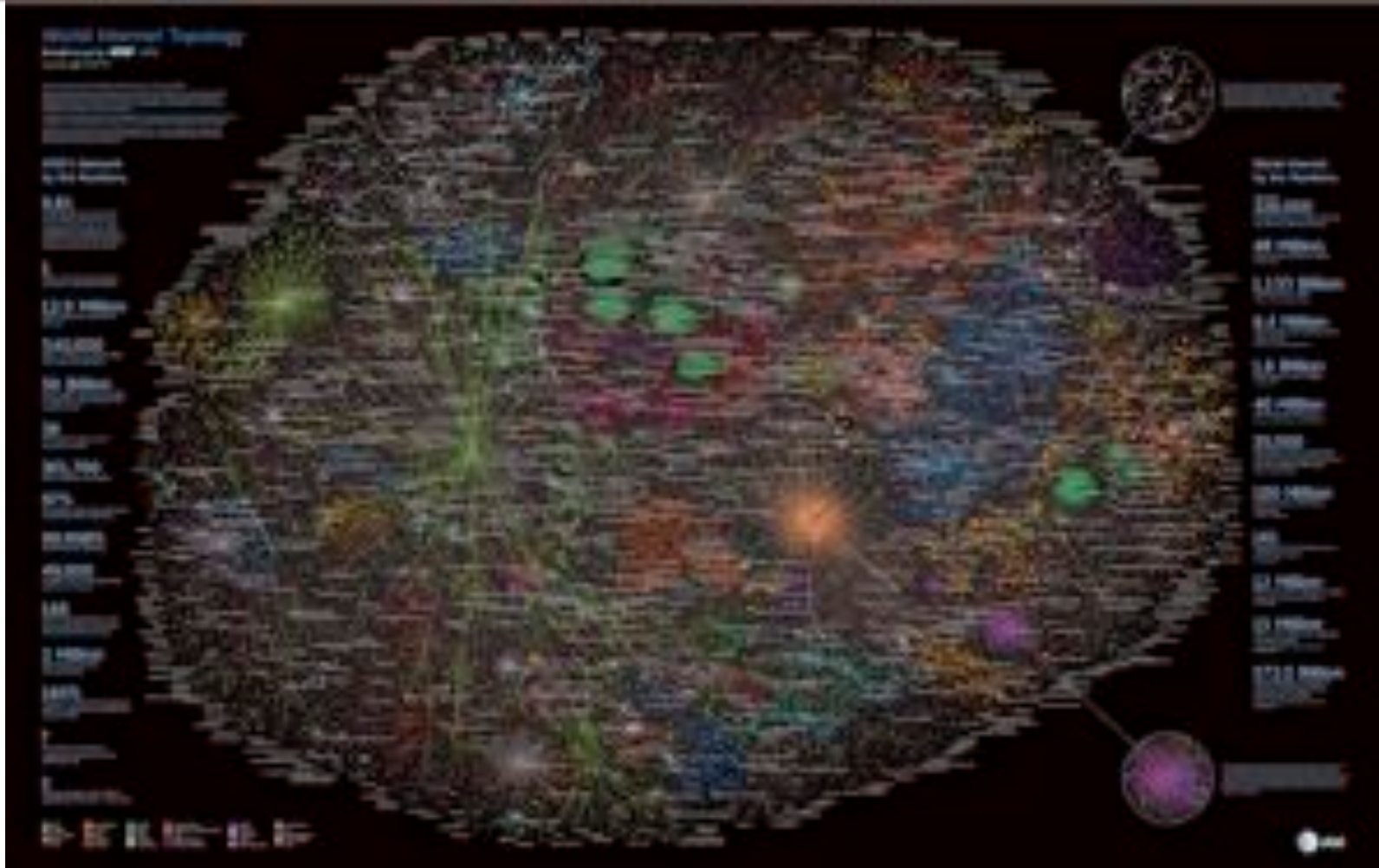


**Technological change =  
new dangers and new fears**





# The big change: global connectivity



# Managing risk



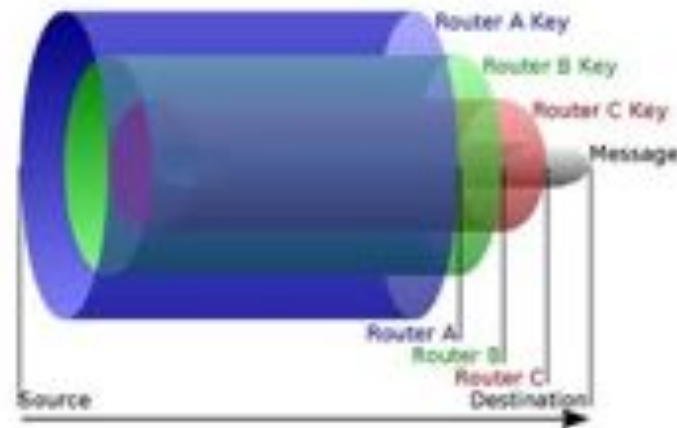
# Example: e-commerce

What made this possible?

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



# Example: anti-censorship





# 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

# 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

The screenshot shows a Mozilla Firefox browser window displaying the website Installs4Sale.net. The browser's address bar shows the URL http://installs4sale.net/. The page content is in Russian and includes the following sections:

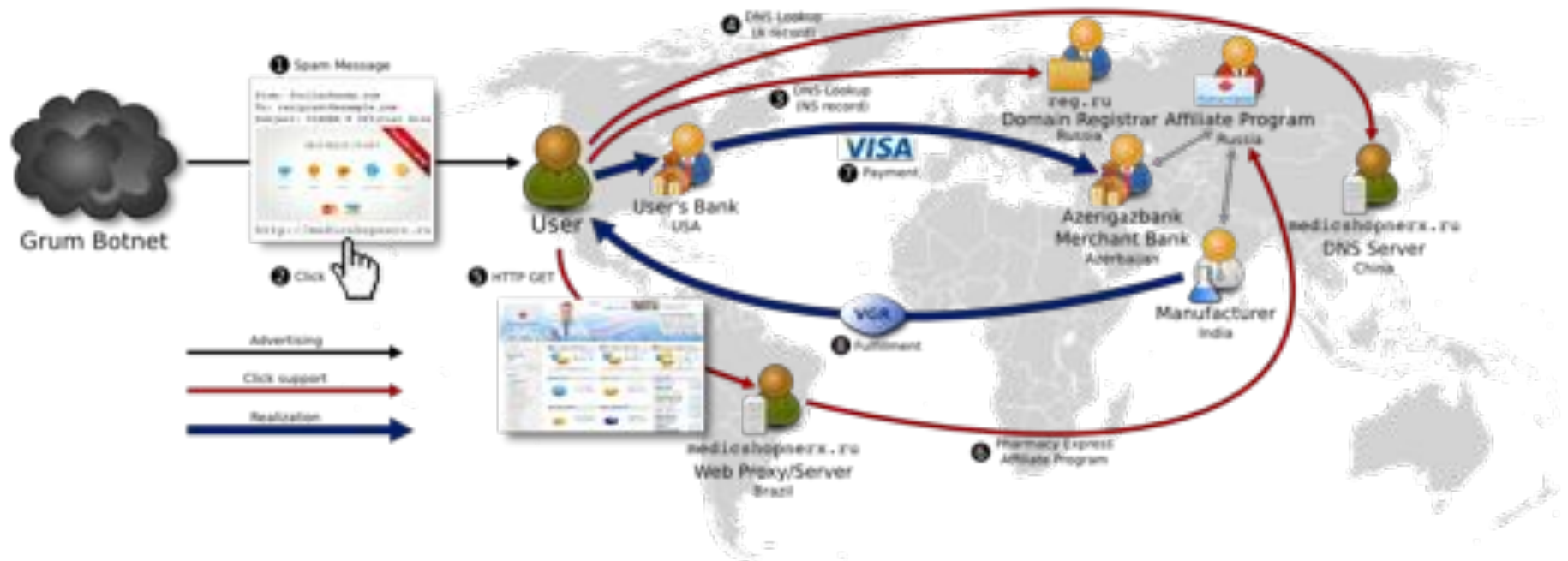
- УСЛОВИЯ** (Conditions):
  - Договорится по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пожалуйста!
  - Мы отслеживаем уникальность инсталлов и их чистоту перед продажей.
- ТАРИФЫ** (Rates):

GB (Англия)	150\$
DE (Германия)	150\$
USA (США)	130\$
IT (Италия)	120\$
Микс (US, CA, AU, GB)	100\$
CA (Канада)	100\$
Микс (Европа)	40\$
Азия	10\$

Все цены указаны за 1000 уникальных загрузок
- Copyright notice: Все права защищены Installs4Sale.net. 2009

# Challenges: new adversaries

- E-crime as a business





# Challenges: new adversaries

- Mass action/hacktivism

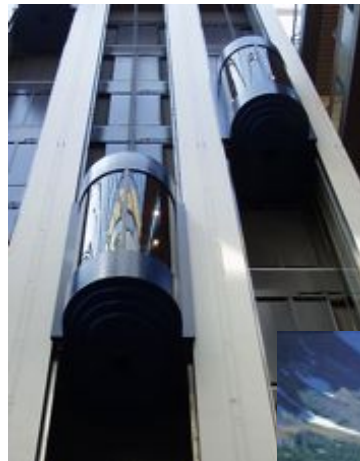


# Challenges: new adversaries

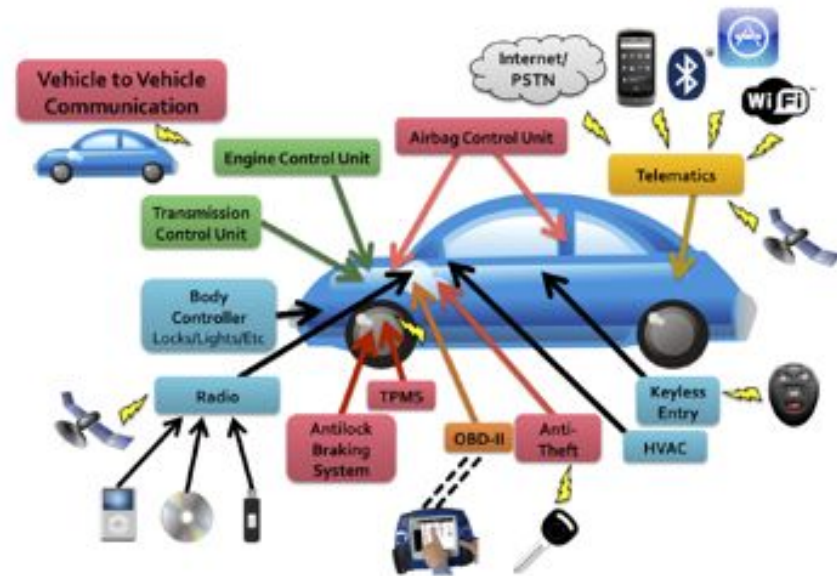
- State-motivated/sponsored actors



# Challenges: the Internet of things



# Computer security meets the real world





# 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

# Thank you

- Questions?

