# Security Economics
# A personal perspective

Ross Anderson

Cambridge

# The birth of security economics

- 'Why Information Security is Hard – An Economic Perspective', ACSAC, Dec 2001
- Now: a field with over 100 active researchers and one of NITRD's growth areas
- What led up to the ACSAC paper?
- How did it develop after that?
- What are the challenges for the next decade?

# Early questionings

- 1991: NRC wrote on DoD concerns that the security market not working
- My 1993 CCS paper “Why Cryptosystems Fail” noted fraud liability variance UK / USA
- Hal Varian’s “Economic Aspects of Personal Privacy” in 1996
- Andrew Odlyzko’s “Smart and Stupid Networks” in 1998
- May 2000: Hal and I met at Oakland

# The spark

- Hal Varian wondered if liability assignment was the key to making online payments work
- I wanted to know why UK banks spent more than US banks despite less liability
- Hal suggested this was classic moral hazard, and gave me a copy of “Information Rules”
- We also talked about why people didn’t buy much antivirus software
- We talked through most of the reception…

# The Role of “Security Engineering”

- I was finalising ‘Security Engineering – A Guide to Building Dependable Distributed Systems’
- I found that economic analysis was the glue that held a lot of the stories together, and sent a couple of chapters to Hal to proofread
- The manuscript finally went off in Jan 2001
- The economic analyses I’d added in the last six months became the ACSAC paper

# A key SE / ACSAC paper insight

- Three distinguishing characteristics of many IT product and service markets are
  - Network effects: value of a network increases more rapidly then the number of users
  - Low marginal costs: price competition will drive prices to near zero
  - Technical lock-in: in fact the value of a platform is in theory equal to the total lock-in of all users
- Value of company = total lock-in of all customers!
- These effects tend to lead to dominant-firm markets where the winner takes all

# IT economics and dependability

- When building a network monopoly, you must appeal to vendors of complementary products
- I.e. app developers for PC versus Apple, Symbian versus Palm, Facebook versus Myspace
- Little security in early versions so easier to develop apps; win the market; then lock in down
- We've seen this over and over again!
- Payment networks: appeal to merchants first
- Online: choose security technologies that dump costs on the user (SSL, not SET)

# From 9/11 to the first WEIS

- I'd already arranged to spend Oct-Dec 01 and Apr-June 02 on sabbatical with Hal at Berkeley
- Then 9/11! Obvious that overreaction would be inevitable and damaging; what could we do?
- Discussed security economics during invited talk at SOSP in Banff, then to Berkeley where the theory folks were doing mechanism design
- We started planning the first Workshop on the Economics of Information Security (WEIS)
- Then on to ACSAC in New Orleans

# WEIS

- First WEIS (Berkeley June 2002) included
  - Alessandro Acquisti: behavioural economics of privacy
  - Jean Camp: vulnerability markets, externalities
  - Barb Fox: economics of standards
  - Larry Gordon, Marty Loeb: information sharing
  - Kevin Soo Hoo: returns on security investmemt
- It was clear we had the beginnings of a coherent and important subject
- What next?

# “Trusted Computing”

- The Trusted Computing Platform Alliance proposed TPM chips, information rights management and remote attestation
- Lock-in: to move your firm from Office to OpenOffice you’d need permission from all authors of protected documents
- The TCPA FAQ made security economics salient!
- November 2002: Software engineering economics conference in Toulouse talk on the economics of open versus closed

# WEIS 2003

- We had papers on most of the topics that now make up the subject including
  - Evaluating costs and benefits of security mechanisms and postures
  - Marty and Larry's model of investment in security
  - The privacy gap: why people say they value it but behave otherwise
- … plus a debate on Trusted Computing. How could we make progress on the open v closed issue?

# Econometrics

- WEIS 2004 opened with a debate on vulnerability disclosure
  - Eric Rescorla: don't disclose as there are so many bugs we don't improve by patching
  - Rahul Telang: must disclose as otherwise vendors will never fix vulnerabilities
  - Eventual consensus: systems do get better over time; they're less like milk and more like wine ☺
- WEIS 2005: why are insurance markets broken?
- Can we get more realistic threat models?

# Econometrics (2)

- If you want evidence-based policy, you'd better go out and collect the evidence
- 'Security Economics and the Internal Market' (ENISA, 2008) advocated breach disclosure laws – now underway in EU data protection directive
- 'Resilience of the Internet Interconnection Ecosystem' (ENISA, 2011) on what might break the Internet and how to forestall that (BGP SEC, regulatory failures, contingency planning …)

# Econometrics (3)

- 'Measuring the Cost of Cybercrime' (WEIS 2012) in response to scaremongering that cybercrime cost 2% of GDP
  - Old-fashioned fraud (tax, welfare etc): direct costs several times the indirect costs
  - Card fraud: about equal
  - 'Pure' cybercrimes: indirect costs often two orders of magnitude greater than direct costs
- Conclusion: spend more effort on locking up the bad guys

# Behavioral Economics

- Application to privacy kicked off by Alessandro Acquisti at WEIS 2002
- A few months later, Danny Kahneman got the Nobel for founding the whole field in the 1970s
- In 2005, SOUPS got a usability community going
- By WEIS 2007, behavioral security was the focus of WEIS; George Loewenstein keynote
- The Workshop on Security and Human Behavior started in 2008

# Behavioral Economics (2)

- Example of work on the privacy paradox: CMU 'privacy meter'
- Questionnaire for students on sensitive behavior (exam cheating, partner cheating, drug use …)
  - Control group: neutral academic setting
  - T1: give strong privacy assurances
  - T2: "howbadareyou.com"
- Do stable privacy preferences exist at all, or is privacy just too context-sensitive?

# Information asymmetry

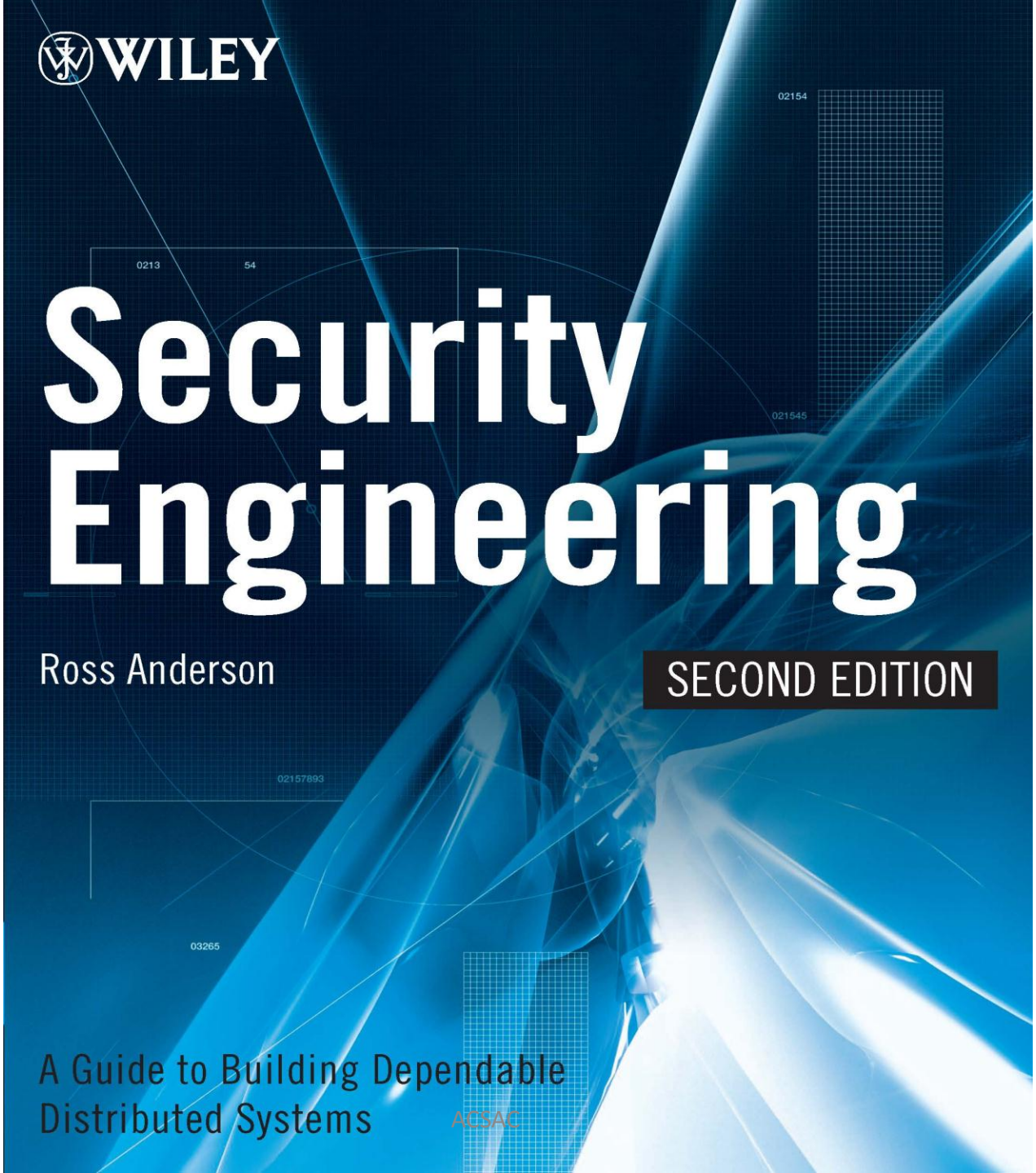
- 2001 (while I was at Berkeley) George Akerlof won the Nobel for "A market for lemons"
  - Town has 100 used cars for sale – 50 plums worth $2000 and 50 lemons worth $1000
  - What's the market price?
- Adverse selection versus moral hazard
- Ben Edelman: websites with a "TRUSTe" certification are twice as likely to be malicious
- Ditto top search ad vs. top free search result

# Recent highlights

- Hospitals in US cities with competition have less secure patient records than monopolies
- The pay-per-install market is driven by porn sites
- Network games: do you fight a flu pandemic by closing the schools or the mass transit?
- < 6% of websites do certification right (why?)
- Should (and can) ISPs clean up malware?
- People's willingness to do online crime varies with local government corruption, not GDP

# Conclusion

- A 2001 ACSAC paper with an audience of 17 has grown into a research field of 150–200
- It started in a cross-disciplinary collaboration
- Its growth was boosted by the war on terror and by trusted computing
- We need game theoretic and other economic models to understand security of systems with multiple competing principals
- What new papers this year will be big in 2023?


WILEY
Security Engineering
Ross Anderson
SECOND EDITION
A Guide to Building Dependable Distributed Systems
ACSAC