THE UNIVERSITY OF BRITISH COLUMBIA

Social, Economic, and Organizational aspects of computer security

Konstantin (Kosta) Beznosov

traditional view

Why are computer systems insecure?

reason: lack of features – crypto, authentication, filtering

solution: provide better, cheaper security features – AES, PKI, firewalls

but there are phenomena that cannot be explained using traditional view

Electronic banking:

UK banks were less liable for fraud, so ended up suffering more internal fraud and more errors

Distributed denial of service:

viruses now don't attack the infected machine so much as using it to attack others

Microsoft is software:

insecure, despite market dominance

why is that?

socioeconomic view

Systems are often insecure because the people who guard them, or who could fix them, have insufficient incentives

Bank customers suffer when poorly-designed bank systems make fraud and phishing easier

Casino websites suffer when infected PCs run DDoS attacks on them

Insecurity is often what economists call an 'externality' – a side-effect, like environmental pollution

IT economics

network effects

Metcalfe's law

the value of a network is the square of the number of users

Real networks – phones, fax, email

Virtual networks – PC architecture versus MAC, or Symbian versus WinCE

Network effects tend to lead to dominant firm markets where the winner takes all

high fixed costs and low marginal costs

Competition can drive down prices to marginal cost of production

This can make it hard to recover capital investment, unless stopped by patent, brand, compatibility …

These effects can also lead to dominant-firm market structures

switching from one product or service to another is expensive

E.g. switching from Windows to Linux means retraining staff, rewriting apps

Shapiro-Varian theorem:

> the net present value of a software company is the total switching costs

So major effort goes into managing switching costs – once you have $3000 worth of songs on a $300 iPod, you're locked into iPods

dominant-firm markets

High fixed/low marginal costs, network effects and switching costs all tend to lead to dominant-firm markets with big first-mover advantage

So time-to-market is critical

Microsoft philosophy of "we'll ship it Tuesday and get it right by version 3" is not perverse behavior by Bill Gates but quite rational

Whichever company had won in the PC OS business would have done the same

how to build a monopoly on an IT market

you must appeal to vendors of complementary products

- application software developers in the case of
  - PC versus Apple,
  - iPhone versus Linux/Windows/J2EE

once you have a monopoly, lock it all down!

summary on IT economics

network effects

high fixed costs and low marginal costs

switching from one product or service to another is expensive

above factors tend to lead to dominant-firm markets with big first-mover advantage

winners appeal to application developers, and then lock developers and users in

IT economics meets computer security

why Windows was so insecure?

lack of security in earlier versions of Windows made it easier to develop applications

so did the choice of security technologies that dump usability costs on the user (SSL, not SET)

Security products and “lemons market”

Why are so many security products ineffective?

Akerlof’s Nobel-prizewinning paper, “The Market for Lemons” introduced asymmetric information

Suppose a town has 100 used cars for sale: 50 good ones worth $2,000 and 50 lemons worth $1,000

What is the equilibrium price of used cars?

If $1,500, no good cars will be offered for sale …

Started the study of asymmetric information

lessons from the conflict theory

Does the defense of a country or a system depend on the least effort, on the best effort, or on the sum of efforts?

the last is optimal; the first is really awful

software is a mix: it depends on

- the worst effort of the least careful programmer,
- the best effort of the security architect, and
- the sum of efforts of the testers

moral: hire fewer better programmers, more testers, top architects

adverse selection and moral hazard matter

why do Volvo drivers have more accidents?

application to trust: Ben Edelman, 'Adverse selection on online trust certifications' (WEIS 06)

- websites with a TRUSTe certification are more than twice as likely to be malicious

the top Google ad is about twice as likely as the top free search result to be malicious (other search engines worse …)

Conclusion: "Don't click on ads"

why companies spend on security what they spend?

large companies spend too much on security and small companies too little.

research shows an adverse selection effect

- corporate security managers tend to be risk-averse people, often from accounting / finance
- more risk-loving people may become sales or engineering staff, or small-firm entrepreneurs

also due-diligence, government and insurance regulations

summary on economics & security

insecure platforms are easier to develop for, and thus attract application developers

markets of IT security/secure products are "lemons markets" with only "lemons" tend to be sold

hire fewer better programmers, more testers, top architects

large companies spend too much on security and small companies too little

credits and further reading

This presentation is based on material from the following

Ross Anderson, "Security Engineering" 2nd edition. Chapter 7.

Ross Anderson, "Towards a science of security and human behaviour," invited talk at SOUPS 2008, Pittsburgh, PA, July 24.