

The Economics of Control System Security

Ross Anderson
Cambridge University

Traditional View of Infosec

- People used to think that the Internet was insecure because of lack of features – crypto, authentication, filtering
- So we all worked on providing better, cheaper security features – AES, PKI, firewalls ...
- About 1999, some of us started to realize that this is not enough

New View of Infosec

- 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

Security Economics

- This has grown since 2001 into a field with over 100 active researchers
- Annual Workshop on the Economics of Information Security (WEIS)
- Topics range from econometrics of online crime through return on security investment to managing the patching cycle
- I'll focus on things of obvious interest to SCADA
- We have the tools – tell us your problems!

IT Economics (1)

- The first distinguishing characteristic of many IT product and service markets is 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

IT Economics (2)

- The second common feature of IT product and service markets is high fixed costs and low marginal costs (as in telcos, airlines, hotels ...)
- 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

IT Economics (3)

- Third common feature of IT markets is that 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

IT Economics and Security

- 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’ was not perverse behaviour by Bill Gates but quite rational
- Whichever company had won in the PC OS business would have done the same

IT Economics and Security (2)

- When building a network monopoly, you must appeal to vendors of complementary products
- That's application software developers in the case of PC versus Apple, or now of Symbian versus Linux/Windows/J2EE/Palm
- Lack of security in earlier versions of Windows made it easier to develop applications
- So did the choice of security technologies that dump costs on the user (SSL, not SET)
- Once you've a monopoly, lock it all down!

IT Economics and Security (3)

- While Symbian followed the same pattern as MVS or Windows or Facebook, there's more
- Mobile phones have a complex supply chain
- IP owners – chipmakers – handset makers – OS vendors – network operators – service suppliers – app vendors...
- Everyone tries to grab power while throwing the risk and liability over the fence. E.g., DRM
- Disruptive plays can involve structure challenges

How is SCADA Different?

- This conventional analysis explains why PC and mobile platforms are less secure...
- Control systems have even higher switching costs, lower network effects, higher marginal costs
- Competition not dominated by market races!
Lock-in is long-term, as with set-top boxes
- There are still many results and insights that apply directly

Competition vs Coordination

- It's often hard to get competitors to coordinate, and in SCADA we may have a natural experiment taking place:
 - The USA is going for regulation via NERC-CIP
 - The UK via CPNI is getting users together by sector to become more intelligent and coordinated customers
- I wonder what sort of outcomes we'll see? (Normally the USA does market-led solutions while the EU does regulation)
- Also, some industries care more than others, and some countries just don't care at all

Competition vs Coordination (2)

- It may depend on the detail!
- Another known problem is how to incentivise providers to maintain adequate reserve / emergency capacity (E.g., phone networks now survive a few days without power, not 6 weeks)
- Putting these together: reports (at Electric Power 08) of NERC CIP compliance games: managers removed black start capability in order not to be assessed 'critical' under CIP-2

Conflict theory

- Does the defence 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
- So one lesson is: hire fewer better programmers, more testers, top architects

Adverse Selection, Moral Hazard

- A lot is known about these in other contexts (why do Volvo drivers have more accidents?)
- Neat example: 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’

Certification Failure

- Common Criteria expensive, but easy to abuse
- Many examples – bank terminals certified to take \$25,000 to break penetrated easily
- Bad PP, wrong scope, and CLEF regulation leading to a race to the bottom
- CC also omits usability, dynamics aspects
- Competitive evaluation may well be better
- See our paper at ETFA 2009, Majorca!

Open versus Closed

- It's easier for the attackers to find vulnerabilities, and easier for the defenders to find and fix them
- John Wilkins 1641: “If all those useful Inventions that are liable to abuse, should therefore be concealed, there is not any Art or Science which might be lawfully profest”
- Theorem (2002): openness helps both equally if bugs are random and standard dependability model assumptions apply
- So whether open is better than closed will depend on whether your system differs from the ideal

Open versus Closed (2)

- Big debate at WEIS 2004!
 - Rescorla: patching doesn't improve systems much so failures dominated by patching failures
 - Arora et al: without disclosure, vendors won't improve. Optimal to disclose after a delay
- Empirical work: operating system bugs are correlated in a number of real systems
- Emerging consensus: CERT-type rules plus breach disclosure laws
- How should this apply to control systems?

Security metrics

- VaR approach (Value at Risk) discredited in our field long before the credit crunch. What else?
- Insurance markets – can be dysfunctional because of correlated risk
- Vulnerability markets – in theory can elicit information about cost of attack (led to foundation of iDefense, Tipping Point, ...)
- Stock markets – in theory can elicit information about costs of compromise. Prices drop a few percent after a breach disclosure

How Much to Spend?

- How much should the average company spend on information security?
- Governments, vendors say: much much more than at present
- But they've been saying this for 20 years!
- The total expenditure may be about right – but may be low / high in some firms / industries
- Big firms spend more than small; governments spend way more than the private sector

Government Bias ...

- If you are DirNSA and have a nice new hack on XP and Vista, do you tell Bill?
- Tell – protect 300m Americans
- Don't tell – be able to hack 400m Europeans, 1000m Chinese,...
- If the Chinese hack US systems, they keep quiet. If you hack their systems, you can brag about it to the President
- So offense can be favored over defense

Security and Policy

- Our ENISA report, published last March, has 15 recommendations. The most relevant here are:
 - Security breach disclosure law
 - Data on which ISPs host malware
 - Networked devices to be secure by default
 - Responsible vulnerability disclosure plus liability for unpatched software, with patches separate from updates
 - ...
- See links from my web page

Smart Grids

- UK to install 30m smart meters by 2017
- Threats? “Chinese sabotage, organised crime, ...”
- Security economics: clear tension between power companies and users / regulators
- Also: UK may run short of electricity in 2016 and face brownouts, just like CA, ZA
- Will smart meters be used for energy rationing?
- In that case, the threat model includes your users!

Other Threads

- Might we see an electronic reprise of the 1996 IRA attack on London?
- Or is the ‘SCADA security’ program crying wolf?
- Institutional cultures – defense vs other firms
- The high costs of custom secure systems
- But – Common Criteria issues (see our paper on vulnerabilities in Chip and PIN payment systems)
- And the high costs of multilevel security

Other Threads (2)

- What happens when you merge industries with 15-year and 15-month product cycles? Power generation won't be as disrupted as telecomms
- Models of security investment and risk – financial models, lifecycle models, comparisons across industries, supply chain issues, compliance costs
- How much of the IT infrastructure can we use?
- How do we deal with a world of pervasive malware, with maybe 0.1% – 1% of PCs owned?

To Wrap Up

- Security economics looks like it has a lot to offer the control engineering community
- Protecting SCADA is intertwined with business structures, risk dynamics and regulation
- We've developed a lot of tools over the last eight years – see my Security Economics Resource Page at www.cl.cam.ac.uk/~rja14/econsec.html
- I have a new research student starting in this field
- What are your worst problems?

 WILEY

Security Engineering

Ross Anderson

SECOND EDITION

A Guide to Building Dependable
Distributed Systems