THE UNIVERSITY OF BRITISH COLUMBIA

Social and Economic 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,
    - Symbian/iPhone versus Linux/Windows/J2EE/Palm
- 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

THE UNIVERSITY OF BRITISH COLUMBIA

IT economics meets computer security

why Windows was/is 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?

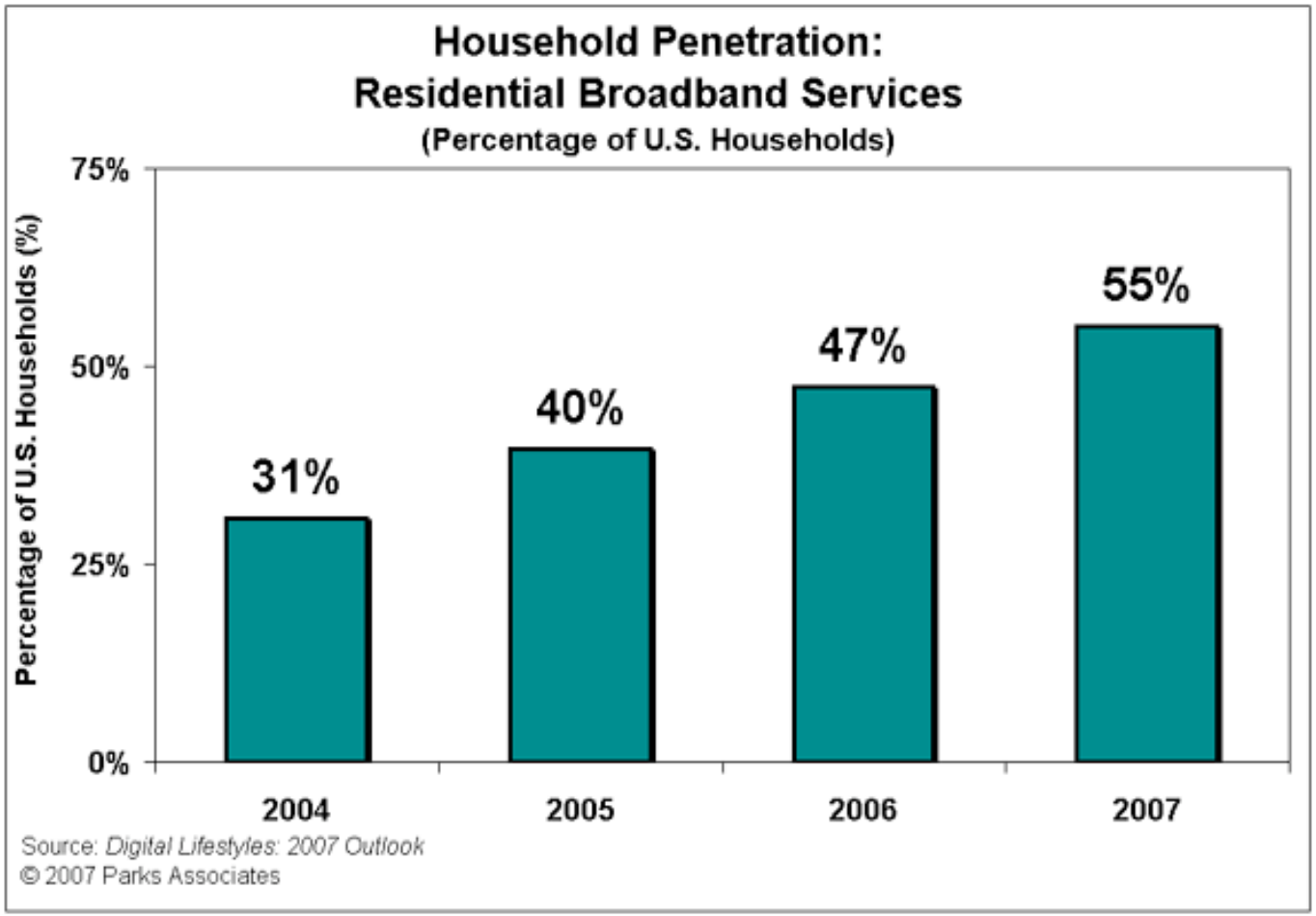
- large companies spend too much on security and small companies too little.
- research shows an adverse selection effect
  - corporate security managers tend to be risk-averse people, often from accounting / finance
  - more risk-loving people may become sales or engineering staff, or small-firm entrepreneurs
- 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

social aspects of IT security

Level of User Security Knowledge Declines



offense or defense?

- If you are the NSA director 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 400,000,000 Europeans, 1,000,000,000 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

Case Study: Cyber War In Estonia

source: slate.com

Estonia 2007

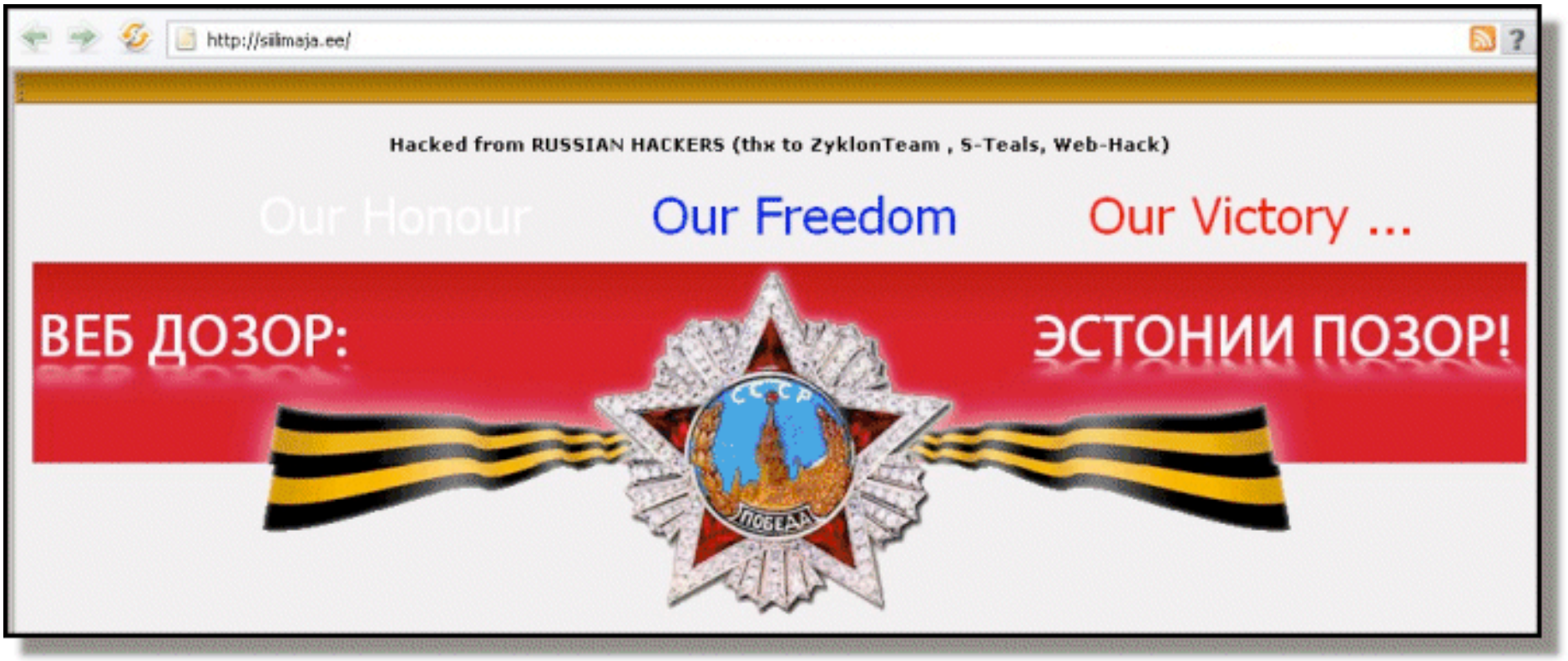
- Highly dependent on computers
  - parking payments
  - Wi-Fi
  - national elections
- Political Incident
  - Estonia's embassy sealed and attacked
  - Cyber attacks continued …

source: economist.com

"Police arrested 600 people and 96 were injured in a second night of clashes in Estonia's capital over the removal of a disputed
World War Two Red Army monument …
Russia has reacted furiously to the moving of the monument …
Estonia has said the monument had become a public order menace as a focus for Estonian and Russian nationalists."

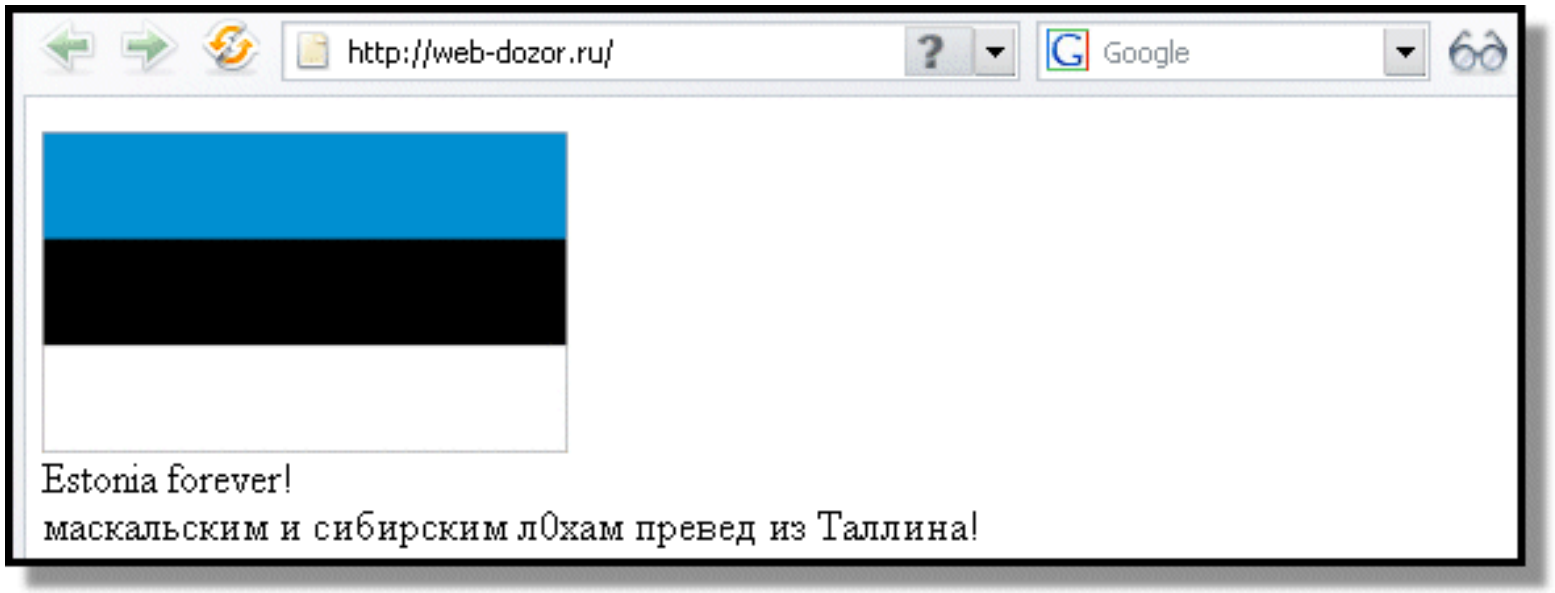
CNN

Defacing Estonian Websites …



source: f-secure.com

some times experiencing reciprocity

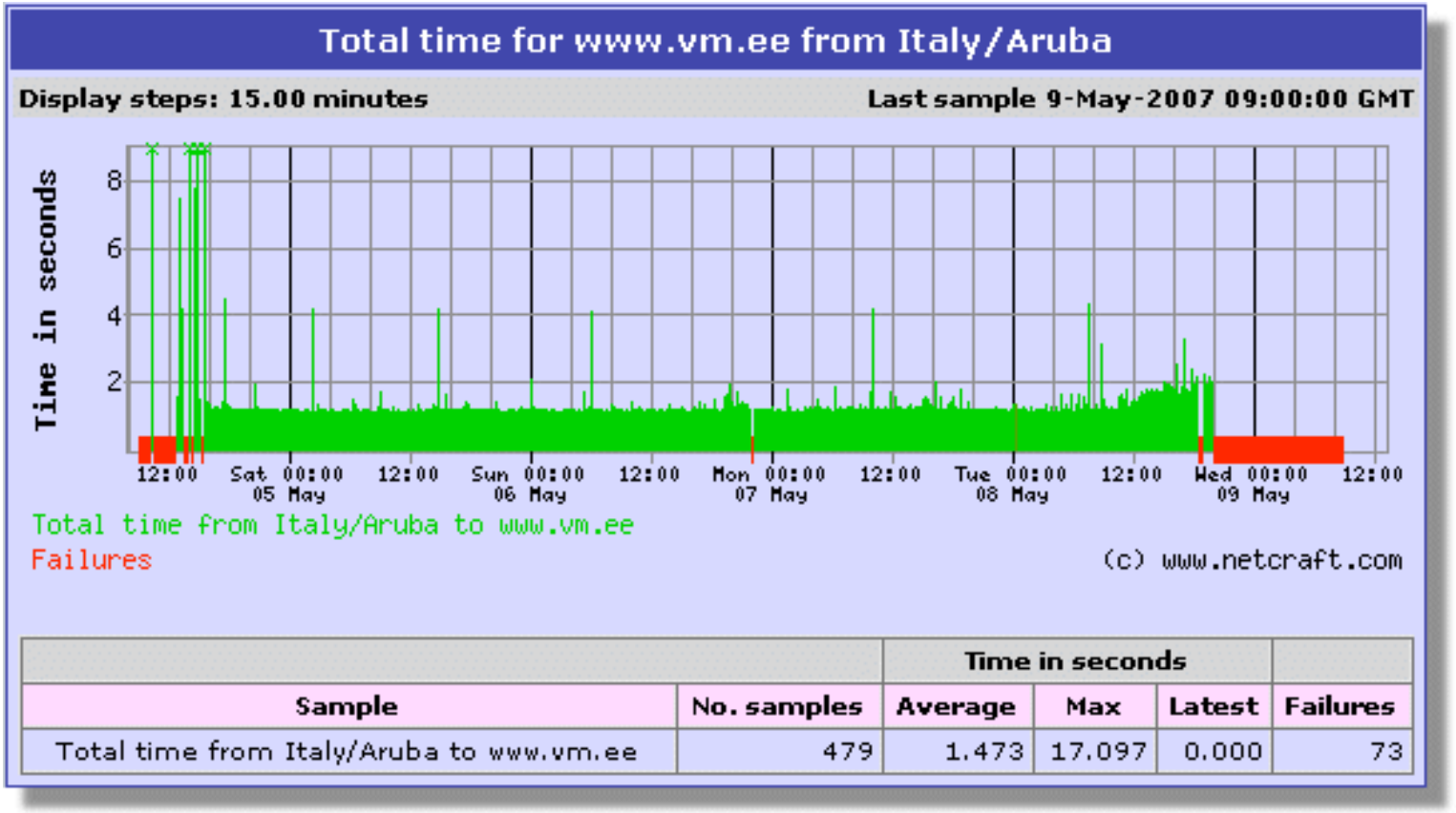


source: f-secure.com

But most importantly ...

Bringing Critical Sites Down …

Availability of Estonian Ministry of Foreign Affairs Web site
May 5-9, 2007



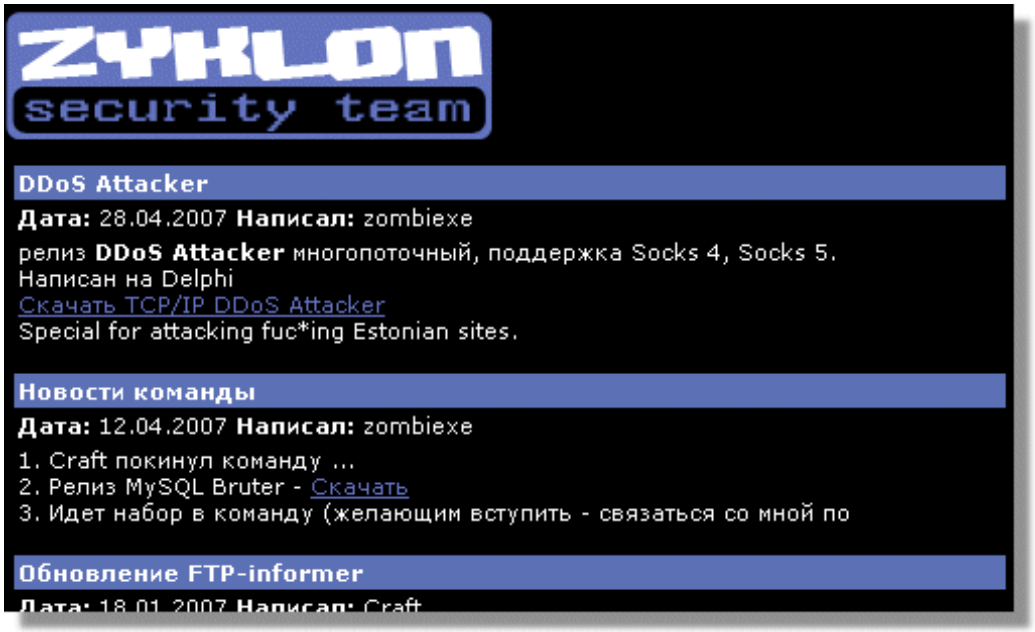
		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from Italy/Aruba to www.vm.ee	479	1.473	17.097	0.000	73

source: f-secure.com

Through Distributed Denial of Service Attacks

- protesters running DoS programs
- botnets
- 128 attacks
  - 115 were ICMP floods
  - 4 TCP SYN floods
  - 9 generic traffic floods
- maxing to 95 Mbps
- up to 10 hours
- shutting 58 sites at once

source: asert.arbornetworks.com



source: f-secure.com

"at its peak over one million computers were involved"
www.crime-research.org

Case Study Social Aspects

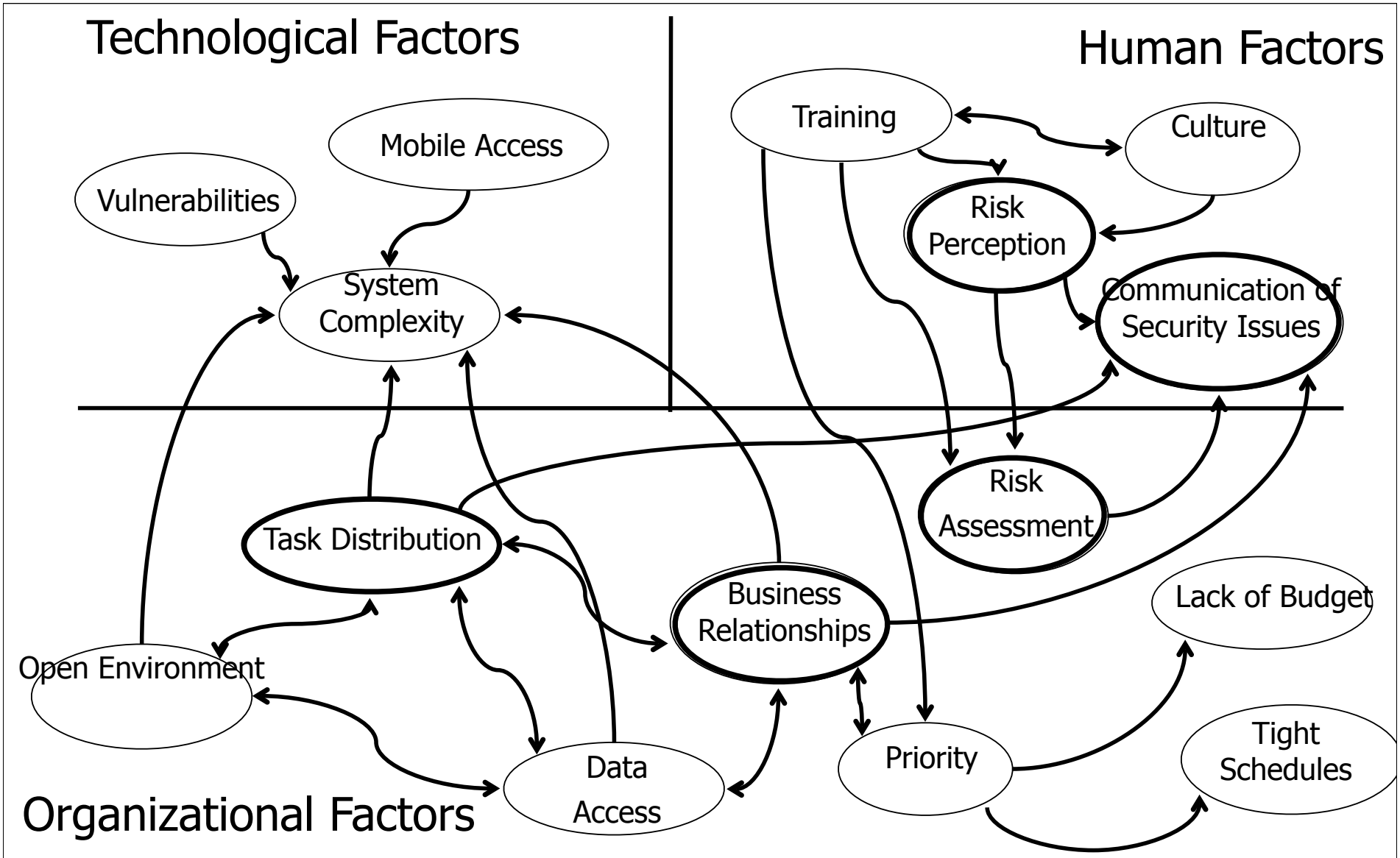
Attackers employed

- simple DoS attacks
- mobilization of activists
- botnet rentals
- flexible communications

Defenders could've

- avoided/reduced sentiments
- disrupted mobilization
- employed deception
- built up social capital
- rented anti-botnets
- made botnets not feasible

(some of the) business aspects of IT security



R. Werlinger, K. Hawkey, K. Beznosov, "Human, Organizational and Technological Challenges of Implementing IT Security in Organizations", in the *Proceedings of the Symposium on Human Aspects in Information Security and Assurance (HAISA)*, Plymouth, UK, 8-10 July 2008.

Stumbling blocks arise when the security program is not aligned with business needs.

Most Enterprise Security Initiatives Fail Due to Lack of Buy-In

Root Causes

- Lack of demonstrated ROI
- Poor definition of success
- No real business alignment
- No long-term strategy to decrease the level of overall security risk and exposure
- No framework within which to design and deploy solutions for new problems
- Technically led, IT-based security projects
- Low prioritization of security as compared to business initiatives
- Lack of appreciation for the importance of security in today's enterprise
- Immaturity of technology solutions

summary

- economics of IT
- economics meet computer security
- social aspects of security
- (some of the) business aspects of security

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
- K. Beznosov and O. Beznosova, "On the Imbalance of the Security Problem Space and its Expected Consequences," Journal of Information Management & Computer Security, Emerald, vol. 15 n.5, September 2007, pp.420-431.
- Kees Jansen, "How Much Security Is Enough?" guest lecture given at EECE 412, March 22, 2007.
- R. Werlinger, K. Hawkey, K. Beznosov, "Human, Organizational and Technological Challenges of Implementing IT Security in Organizations", in the Proceedings of the Symposium on Human Aspects in Information Security and Assurance (HAISA), Plymouth, UK, 8-10 July 2008.