



Economic Issues of Usable Security and Privacy

Prof. Nicholas Economides

Stern School of Business, New York University

<http://www.stern.nyu.edu/networks/>
and NET Institute <http://www.NETinst.org/>
<mailto:economides@stern.nyu.edu>



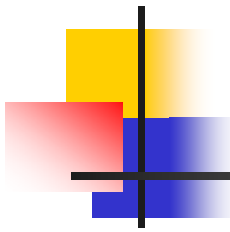
Issues

- At present, the incentives of both users and companies on usable security and privacy diverge from actions that would maximize social benefit
- What economic and legal policies can be implemented to change users' and companies' incentives so that they are closer to maximizing social benefit?



Significant deficit in usable security and privacy

- Current operating systems of PCs, netbooks, mobile phones, and other devices have significant security deficiencies
- Interfaces defining security levels are typically very difficult to follow
- Users are typically unaware of their level privacy (or its lack) in computers



The Internet has multiplied security problems of connected devices and highly increased the global impact of local lack of security

- The Internet was designed for a small number of nodes that knew and trusted each other
- Presently we are almost at a billion nodes worldwide with no mutual knowledge and no trust
- The Internet has no centralized or Internet Service Provider (ISP)-level security
- Security issues have an even more severe impact in “cloud computing”
- Typical users have a very limited understanding of the network capabilities of their computers and the possibilities of abuse in a network setting



Perspectives of the Issue

- The residential user's point of view
- The business user point of view
- A search engine's point of view
- The network's (societal) point of view
- Operating systems (OSs) and computer manufacturers point of view
- ISP's point of view
- Global issues



The user's point of the view

- Different computer communications, usage, and storage require different levels of security
- Does the user understand how secure or insecure his communications, usage, and storage are?
 - Does the user understand the financial consequences to him and others of lack of security in these?
 - How can the user's understanding be enhanced?
- **Does the user have sufficient economic incentives (rewards/punishments) to use sufficient security?**
 - What is the balance between the user's desire for privacy and the user's desire for communication in social networks?
 - Can we improve usability of security so that users who aim for higher security are able to achieve it? How?



Private companies have diverse points of view on security and privacy

1. Some businesses (e.g. banks, stock brokers, electronic commerce firms) generally desire higher security
 - They have found various (private) solutions attempting to make their transactions more secure
2. But advertisers and search engines generally like more disclosure of private information to be able to pitch products closer to a consumer preferences and willingness to pay
 - A very secure Internet where users are fully aware of the impact of disclosures of their private information would cut into the profits of these companies



Private companies perspective (cont.)

3. OS companies typically grew up in the pre-Internet era

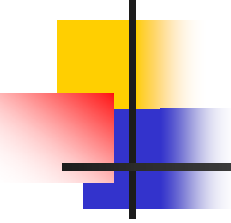
- OSs originally relied on third parties to beef up security
- OSs did not anticipate the potential for global damage created by multiple local infiltrations in a network setting in the presence of even small security flaws
- Ultimately, companies will act to avoid liability
- How should we tweak the law to change the incentives of OS and computing devices manufacturers?

Bottom line: Given the diverse uses of the Internet and the various functions/roles of firms on the Internet, **it is unlikely to have a consensus among companies on security and privacy**



From the network's point of view (societal point of view)

- In general, the value of security is much higher for the network than for an individual user
- Users, left on their own, will generally tend to achieve lower security than society desires
- Low security at a node can lead to catastrophic network events (such as the collapse of attacked nodes or even parts of the Internet) that are much more damaging to society than to the individual node
 - The lack of security at a node is a “negative externality” to the network



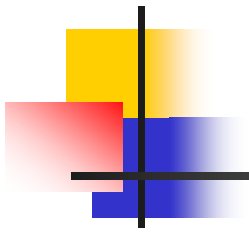
In a network setting there is a crucial divergence between private and social incentives on security

- Presently **most users do not have sufficient incentives to secure their computers to prevent network-wide catastrophic events**
 - Can we create sufficient economic incentives so that users aim for sufficient security? How?
 - How can we improve usability of security so that users who aim for higher security are able to achieve it?



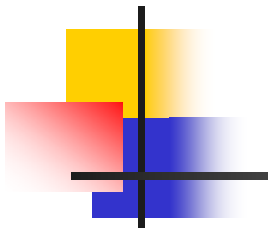
What incentives will induce users to more secure computing behavior?

- Positive monetary incentives (pay people)?
- Awards and other non-monetary positive incentives?
- Punishments for not meeting a security benchmark?
 - Impose on insecure nodes liability for damages created using their node?
 - Limit access to the Internet if computer fails security test?



From the OSs' and computer manufacturers' point of view

- How can we create incentives for computer and operating systems vendors to increase security and maintain it through the useful life of a computer?



Should we require OSs to include and automatically update for free security/antivirus/anti-phishing?

- Should we impose additional liability on operating systems vendors?
 - In the extreme, should we deny computers access to the Internet (except the security checkup and upgrade site) unless they have passed a minimal standard of security?
- Should we require OSs to disable (as the default) various server functions of new computers, network devices, mobile phones, etc.?



The ISPs point of view

- How can we induce ISPs to play a role in limiting or preventing some attacks while adhering to network openness and net neutrality?



Global Issues

- No matter how good security becomes within the U.S., security issues will remain because of the global nature of the Internet
- This underlines the importance
 - of certification of web sites and of measures that improve security in bilateral communications (including web browsing)
 - of requirements on computer and OS manufacturers to increase security and automatically maintain it through the useful life of consumers worldwide



Policy Changes

- To strengthen usable security, what legal and economic policy changes are required
 - at the user level?
 - at the computer and OS manufacturer level?
 - at the web site/server level?
 - at the Internet service provider level?



Some questions

- How will the society deal with the “negative externality” on the network/society created by the lack of usable security of individual nodes?
- How can we provide positive and negative, monetary and non-monetary incentives to users to eliminate the negative externality?
- What role can the OSs play? Design? Post-purchase security maintenance?
- What role can the search engines play in making people aware of privacy issues?
- What role can ISPs play?