Information security: where computer science, economics and psychology meet

By Ross Anderson[1]* And Tyler Moore[2]
1Computer Laboratory, University of Cambridge, 15 JJ Thomson Avenue, Cambridge CB3 0FD, UK
2Center for Research on Computation and Society, Harvard University, 33 Oxford Street, Cambridge, MA 02138, USA

Abstract

Until ca. 2000, information security was seen as a technological discipline, based on computer science but with mathematics helping in the design of ciphers and protocols. That perspective started to change as researchers and practitioners realized the importance of economics. As distributed systems are increasingly composed of machines that belong to principals with divergent interests, incentives are becoming as important to dependability as technical design. A thriving new field of information security economics provides valuable insights not just into 'security' topics such as privacy, bugs, spam and phishing, but into more general areas of system dependability and policy. This research programme has recently started to interact with psychology. One thread is in response to phishing, the most rapidly growing form of online crime, in which fraudsters trick people into giving their credentials to bogus websites; a second is through the increasing importance of security usability; and a third comes through the psychology-and-economics tradition. The promise of this multidisciplinary research programme is a novel framework for analysing information security problems—one that is both principled and effective.

Keywords: information security; economics; incentives; psychology

Introduction

As the Internet has grown, system engineers have realized that security failure is caused at least as often by bad incentives as by bad design. Indeed, the former often explain the latter. Systems are particularly prone to failure when the person operating them does not suffer the full costs of failure. Things also break when system users have conflicting interests, or even just no real reason to cooperate. Thus, while security engineers used to worry about malicious outsiders, the greatest concern now is selfish insiders. As a result, the tools of game theory and microeconomic theory are becoming just as important to the security engineer as the mathematics of cryptography.

** Author for correspondence (ross.anderson@cl.cam.ac.uk).*

*One contribution of 16 to a Theme Issue 'Crossing boundaries: computational science, e-Science and global e-Infrastructure II. Selected papers from the UK e-Science All Hands Meeting 2008'.**We review recent results and live research challenges in the economics of information security. Our goal is to present several promising applications of economic ideas to practical information security problems. We first consider misaligned incentives in the design and deployment of computer systems. Next, we study the impact of externalities: network insecurity is somewhat similar to air pollution or traffic congestion, in that people who connect insecure machines to the Internet do not bear the full consequences of their actions. Asymmetric information presents further problems. Insecure software dominates the market for the simple reason that most users cannot distinguish it from secure software; thus, risks cannot be managed better until we can get better measurements, both of the raw risks and the effects of various countermeasures. Finally, a recent growth area is the application of ideas from the boundary between economics and psychology. These ideas*

provide many useful insights into problems ranging from the ease with which computer users are deceived by fake websites, through why many people say they value privacy yet act otherwise when online, to societal misperceptions of risk. Why is it, for example, that most people care too little about online security and privacy, yet overreact to terrorism?

Misaligned incentives

One of the observations that sparked interest in information security economics came from banking. In the United States, banks are more liable for the costs of card fraud, as consumer protection law is stronger than in Britain. So one might expect that UK banks would spend less on security and fraud than US banks, but the reverse turned out to be the case (Anderson 1994). How could this be? It appears to have been what economists call a moral hazard effect: UK bank staff knew that customer complaints would be stonewalled, so they became lazy and careless. This led to an avalanche of fraud.

Varian (2000) made a similar key observation about the antivirus software market. People did not spend as much on protecting their computers as they might have. Why not? At that time, a typical virus payload was a service-denial attack against the website of a company such as Microsoft. Although a rational consumer might well spend $20 to prevent a virus from trashing his hard disk, he might not (worth $1000 each). The sellers know the difference, but the buyers do not. What will be the market-clearing price? One might initially think $1500, but at that price no one with a good car will offer it for sale, so the market price will quickly end up near $1000. Akerlof's 'market for lemons' explains why so many information security products are poor: buyers are unwilling to pay a premium for quality they cannot measure. This has led to various certification schemes that try to signal product quality to buyers. As well as hidden information, there can be a problem with hidden action. Such problems arise when two parties wish to transact, but one of them can take unobservable actions that affect the outcome. The classic example comes from insurance, where the policyholder may behave recklessly. Hidden information and hidden action can be used to classify computer security problems (Moore 2005). Routers can quietly drop selected packets or falsify responses to routing requests; nodes can redirect network traffic to eavesdrop on conversations; and players in file-sharing systems can hide whether they are sharing with others, and thus 'free-ride' rather than help to sustain the system.

Once this is understood, designers can structure interactions to minimize hidden action or make it easier to enforce contracts. For example, early peer-to-peer systems forced users to cooperate with random other users, while more modern designs have the effect of clustering users by affinity, so that users help to defend other users with similar preferences. This leads to greater solidarity and makes systems more robust (Danezis & Anderson 2005). This model also sheds light on the more general problem of the trade-offs between diversity and solidarity—for example, whether the growing diversity of modern societies is in tension with the solidarity on which welfare systems are do so just to prevent an attack on someone else.

Lawyers have long known that liability should be assigned to whoever can best manage the risk. Yet online risks tend to be allocated poorly, resulting in privacy failures and regulatory tussles. For instance, medical records systems are bought by hospital directors and insurance companies, whose interests in cost control and research conflict with the patients' interests in privacy. Another example was documented by Bohm *et al*. (2000): banks used the move from branch to online banking to shift the liability rules in their favour and against customers. The realization that incentive failures were important, and getting steadily worse, helped spark a research programme in information security economics (Anderson 2001). Researchers found they could use many established microeconomic models. For example, in a Nobel prize-winning work, Akerlof (1970) kicked off the study of asymmetric information. He imagined a town in which 50 good used cars (worth $2000 each) are for sale, along with 50 'lemons'

founded (Goodhart 2004).

Security as an externality

Economists use the term *externality* to describe the side effects of transactions; these can be positive (as with scientific research) or negative (as with environmental pollution). Externalities were already well known in crime prevention. Ayres & Levitt (1997) analysed the Lojack car-theft prevention system and found that once a threshold of car owners in a city had installed it, auto theft plummeted, as the stolen car trade
A particularly important example in the information industries is the network externality: the more people use a service akin to voice over Internet protocol (VOIP), the more people there are to talk to, and so the value of the service scales more rapidly than the number of users. Similarly, the more people use a platform such as WINDOWS, the more
Curiously, this explains why many IT platforms and services are initially designed to be insecure. A firm trying to build a network monopoly must appeal not just to its customers, but also to its complementers, such as the software developers in the case of an operating system. Complicated access controls would
A different set of externalities can be found when we analyse security investment, as protection often depends on the efforts of many other principles. An interesting model, due to Varian (2004), is to consider whether defence depends on the efforts of the laziest defender, or of the most valiant defender, or on the sum total of all the defenders.
Consider a medieval city. If the main threat is a siege, and each family is responsible for maintaining and guarding one stretch of the wall, then the city will depend on the efforts of the laziest family. If disputes are settled by single combat between champions, then it depends on the strength and courage of its most valiant knight. But
Other researchers have modelled interdependent risk. An influential paper by Kunreuther & Heal (2003) noted that

became too hazardous. Camp & Wolfram (2000) built on this to analyse information security vulnerabilities as negative externalities, such as air pollution: someone who connects an insecure PC to the Internet does not face the full economic costs of that, any more than someone burning a coal fire. They proposed trading vulnerability credits in the same way as carbon credits.

firms write software for it, and the more valuable it becomes. These effects—together with the high fixed and low marginal costs of information goods, and the lock-in that comes from controlling interoperability—lead to the information industries having many dominant-firm markets, in which the winner takes all.

make the developers' lives harder, and thus are generally avoided in the early stages. Later, once the platform vendor has established dominance, it will introduce excessive security in order to lock its customers in tightly (Anderson 2001). This pattern has been seen again and again, in mainframe, PC and mobile phone markets.
if wars are a matter of attrition, then the critical factor is the sum of all the citizens' efforts. Of these, sum-of-efforts is the most efficient, best effort is next and least effort gives the least defence of all.
System reliability is a mix of these. A critical vulnerability may be introduced by the most careless programmer; whether it is found prior to deployment depends on the sum of all the testers' efforts; and whether a deployed vulnerability leads to an actual attack may depend on the skill of the security architect, who designed the system's structure and interfaces. So a software company should hire fewer but better programmers, more testers and the best security architect it can find.
security investments can be strategic complements: an individual taking protective measures creates positive

externalities for others that may discourage their own investment. This has implications far beyond information security. An apartment owner who installs a sprinkler system can make his neighbours less likely to do the same, and people thinking whether to vaccinate their children may choose to free ride off the herd immunity instead. The Kunreuther–Heal model shows that several widely varying equilibria are possible, from complete adoption to total refusal, depending on the levels of coordination between principals.There are further implications for technology adoption. A number of core Internet protocols, such as DNS and routing, are known to be insecure. Better protocols exist (DNSSEC and S-BGP), but the challenge is to get them adopted, and quite a lot of users may have to adopt a new protocol before it becomes economic for people to switch. There is a useful model, by Katz & Shapiro (1985), which analyses how network externalities influence the adoption of technology: they lead to the classical S-shaped curve, in which slow early uptake gives way to rapid deployment once the number of users reaches some threshold. Two security protocols that have already been widely deployed, SSH and IPSEC, overcame the bootstrapping problem by providing adopting firms with internal benefits, thus reducing the size of the threshold to less than the size of the larger firms. Thus, adoption could proceed one firm at a time. Fax machines got deployed this way: companies initially bought them to connect their own offices.

Economics of vulnerabilities

There has been debate for centuries about whether security is helped by keeping mechanisms secret. This started with seventeenth-century debates on technology; in the nineteenth century, people debated whether books on locksmithing should be published; and recently governments have used security arguments to cover up various misdeeds. In the systems world, proprietary software vendors have argued with free-software advocates and security researchers over whether actively seeking and disclosing vulnerabilities are socially desirable.

Anderson (2005) showed that, under standard assumptions about depend- ability growth, opening a system helps attackers and defenders equally. Rescorla (2004) argued that in such a case, as removing one bug makes little difference to the likelihood of an attacker finding another one later, and because exploits are often based on vulnerabilities inferred from patches or security advisories, disclosure and frequent patching should be avoided. Arora *et al*. (2004) countered that, as a practical matter, vulnerability disclosure was needed to give vendors an incentive to fix bugs quickly. Ozment (2005) found that for FREEBSD, a popular UNIX operating system that forms the core of Apple OS X, vulnerabilities are in fact correlated, and likely to be rediscovered; Ozment & Schechter (2006*a*,*b*) also found that the rate at which unique vulnerabilities were disclosed for the core FREEBSD operating system has decreased over a 6 year period. These findings suggest that vulnerability disclosure can improve system security over the long term.

Measuring software quality is hard, though. We have already remarked on Akerlof's 'market for lemons' model, whereby the buyers do not know as much about product quality as sellers do; in software it can be even worse, as not even the vendors really know whether their product is secure or not.

There are some interesting new approaches to obtaining more accurate metrics. Schechter (2004) proposed open markets for reports of previously undiscovered vulnerabilities as a means of eliciting all the information available to market participants. Now several firms, led by iDefense and Tipping Point, are openly buying vulnerabilities. Their business model is to provide vulnerability data to their customers as well as to the vendor of the affected product, so that their customers can take precautions early.

An alternative approach is to rely on insurers. The argument is that underwriters assign premiums based on a firm's exposure and, over the long run, they amass a pool of data by which they can value risks more accurately. Right now,

however, the cyber-insurance market is both underdeveloped and under- used. One reason, according to Böhme & Kataria (2006), is the problem of interdependent risk. Cyber-attacks often exploit a vulnerability in a system used by many Insurance is not the only market affected by information security. Some very high-profile debates have centred on Digital Rights Management (DRM); record companies have pushed for years for DRM to be incorporated into computers and consumer electronics, whereas digital rights activists have opposed them. What light can security economics shed on this debate?

Varian (2005) presented a surprising result: that stronger DRM would help system vendors more than it would help the music industry, because the computer industry is more concentrated (with only three serious suppliers of DRM platforms: Microsoft; Sony; and the dominant firm, Apple). The content industry scoffed, but, by the end of 2005, music publishers were protesting that Apple was getting an unreasonably large share of the cash from online music sales. As power in the supply chain moved from the music majors to the platform vendors, so power in the music industry appears to be shifting from the majors to the firms, leading to global risk correlation that pushes up prices. Many writers have called for software risks to be transferred to the vendors; but so far, vendors have succeeded in dumping most software risks.

independents, just as airline deregulation favoured aircraft makers and low-cost airlines.

There are other interesting market failures. Recently, for example, a number of organizations have set up certification services to vouch for the quality of software products or websites. But certification markets can also suffer from adverse selection: if vetting is weak, dubious companies are more likely to buy certificates than reputable ones. Edelman (2006) has shown that this is really happening. Whereas some 3 per cent of websites are malicious, some 8 per cent of websites with certification from one large vendor are malicious. He also compared ordinary Web search results and those from paid advertising: whereas

2.73 per cent of companies ranked at the top in a Google search werebad, 4.44 per cent of companies who had bought ads from the search engine were bad. His conclusion: ‘do not click on ads’.

Economics of privacy

People have worried since the 1960s that computers would undermine privacy, and many countries have privacy laws whose effectiveness is unclear. There are ever stronger incentives for firms to collect personal information about their customers: technology is simultaneously cutting the costs of this and increasing the benefits (Odlyzko 2003).

Yet there remains a mystery at the heart of privacy. If you ask a sample of people whether they care about privacy, approximately one-third say that they care very much and a further one-third say that they care somewhat. Yet, once online, the great majority of people will hand over their personal information for little or no reward. This ‘privacy gap’ between stated and revealed privacy preferences is a notorious problem, which attracts much work by behavioural economists. For example, Acquisti & Grossklags (2004) showed that subjects care less about the privacy effects of decisions taken in an impersonal context, that they lack sufficient information to make informed privacy choices, and that they indulge in ‘hyperbolic discounting’, being too willing to trade short-term benefits for larger long-term risks.

Recently, Loewenstein (2008) has challenged the belief that there even exist stable privacy preferences. He devised a questionnaire to measure students’ privacy preferences by asking embarrassing questions to see how many would be answered, and a control group answered this under neutral university conditions.

A second group answered it having read a detailed privacy policy that gave them strong assurance that their answers would never be linked to them; this group answered fewer questions, not more, showing the effect of making privacy salient. A third group answered the survey on a non-university website that asked 'How BAD are you?' and had a jokey picture of a devil. This group actually disclosed more sensitive information, despite having no privacy at all.

If privacy preferences cannot easily be measured, then what can be? Stock prices, for a start. Campbell *et al*. (2003) found that the stock price of companies reporting a security breach was more likely to fall if the breach leaked confidential information.

1. Social networks and information security

Recently, economists, sociologists and physicists have been applying ideas from the topology of complex networks to study human societies. Networks from the Internet to social networks of human friendship are complex, but emerge from ad hoc interactions of many entities using simple ground rules. A new discipline of network analysis has emerged, and provides tools for modelling and investigating such networks (see Newman (2003), for a recent survey).

Network topology can strongly influence conflict dynamics. Often an attacker tries to disconnect a network or increase its diameter by destroying nodes or edges, while the defender counters with various resilience mechanisms. Examples include a music industry body attempting to close down a peer-to-peer file- sharing network, a police force trying to decapitate a terrorist organization, and a totalitarian government conducting surveillance on dissidents. Police forces have wondered for some years whether network science might be of practical use, either to insurgents or to counterinsurgency forces.

The first result came when Albert et al. (2000) showed that networks with scale-free degree distributions are robust to random attacks, but very vulnerable to targeted attacks. This is because they get much of their connectivity from a handful of nodes with a high vertex order, and, if these 'kingpin' nodes are removed, connectivity collapses. Nagaraja & Anderson (2006) extended this model to the dynamic case, in which the attacker can remove a certain number of nodes at each round and the defenders then recruit other nodes to replace them. Using multiround simulations to study how attack and defence interact, they found that formation of localized clique structures at key network points worked reasonably well, whereas defences based on rings did not work well at all. This helps to explain why peer-to-peer systems with ring architectures turned out to be rather fragile, and also why revolutionaries have tended to organize themselves in cells.

2. Psychology

There have been many fruitful interactions between psychology and computer science over the years, from the insight of Turing, Newell and Simon that thinking could be modelled as computation, to the work of robotics and computer vision researchers who have helped to elucidate the workings of the human visual system. Security and psychology first came in contact through work on social psychology. Asch (1951) showed that most people could be induced to deny the evidence of their own eyes in order to conform to a group; Milgram (1974) showed that most people would torture—they would administer severe electric shocks to an actor playing the role of a 'learner' at the behest of an experimenter playing the role of the 'teacher', even when the learner appeared to be in severe pain and begged them to stop; and in the 1971 Stanford Prisoner Experiment, students playing the role of warders so brutalized students playing the role of prisoners that the experiment had to be stopped (Zimbardo 2008). This is increasingly relevant to protecting systems: a number of attackers simply pretend to be police officers or bank officials, and preventing attacks based on such 'social engineering' is hard. Security usability was the next point of contact. A seminal study by Whitten & Tygar (1999) showed that the most popular email encryption program was simply too difficult for

ordinary people to use; most of them made errors that compromised the protection it offered. Since then, security Since 2001, the misperception of risk has become a hot topic. The overreaction of many people to terrorist attacks—which is of course the mechanism that gives terrorism much of its effect—has led security resources to be misallocated on a large scale. Researchers have countered Since 2004, computer crime has become organized and grown rapidly. The fastest growing type of crime is *phishing*, in which crooks send emails pretending to be from a bank or service provider and inviting its customers to log on at its website. The URLs provided are for copies of the real website, and users who are deceived into disclosing their password or other credentials risk having their accounts emptied. This has driven serious research into deception (Jakobsson & Myers 2007).

A common thread running through work on risk perception and deception has been the application of results from researchers in psychology and economics. Workers in this field—also known as behavioural economics—have studied the heuristics and biases that help to drive human decision-making, especially in unfamiliar circumstances or when the subject is emotionally aroused. Their ideas have turned out to be useful when analysing information security that had long been known to practitioners, but were dismissed as 'bad weather', have turned out to be quite explicable in terms of the incentives facing individuals and organizations, and in terms of different kinds of market failure. This has led to the growth of a vigorous security economics research community (Anderson 2008).

As for the future, the work of the hundred or so researchers active in this field has started to spill over into three new domains. The first is the economics of security generally, where there is convergence with economists studying topics such as crime and warfare. The causes of insurgency, and tools for understanding and dealing with insurgent networks, are an obvious attractor. The second new domain is the economics of usability has established itself as a field with dozens of active researchers.

with attempts to measure terrorist attacks and their sequelae more accurately (Muller 2006), and to understand the psychology of both the terrorists (Atran 2003) and the kind of incidents to which the public overreacts (Gilbert 2006).

privacy, deception and risk perception. There are also some fundamental questions. For example, Humphrey (2003) argues that we developed our intelligence in a social context: the positive way of putting this is that coping with complex social groups became adaptive, while the more cynical version is that people who were good at deception, or at detecting deception in others, had more surviving offspring. The study of deception and of attitudes to risk may thus help us understand deeper questions about our origins and nature.

3. Concluding remarks

Over the past few years, a research program on the economics of security has built many cross-disciplinary links and has produced many useful (and indeed delightful) insights from unexpected quarters. Many perverse aspects of dependability. Why is it, for example, that large IT projects fail? We have much better tools for managing complex projects than we did 30 years ago, yet the same proportion of big projects seem to fail—we just build bigger failures nowadays. This suggests that the causes have as much to do with incentives and organizational behaviour as with intrinsic system complex- ity. Finally, psychology is a new hot topic, driven by factors ranging from the increasing use of deception in online fraud to broader concerns about risk perception in society.

In short, security is becoming a thoroughly multidisciplinary subject that crosses many academic boundaries. Its goal is to develop the tools and concepts that enable us to design systems that remain dependable in the face of mischance and

malice. One of the most powerful tools is to see to it that principals cannot gain by cheating, and do not want to try. Designing bad behaviour out of systems at the start is much more attractive than trying to police it afterward. Although this is not always possible, we can now often recognize when it is; and even where systems are inevitably going to be targets—such as payment systems—there are smart things we can do to minimize the risk.

This is an evolving review paper of a rapidly developing field. The authors have also given a number of invited talks on the subject, and are grateful for much feedback from audiences. T.M. was supported by the UK Marshall Aid Commemoration Commission and by NSF grant DGE- 0636782 (T.M.).

References

Acquisti, A. & Grossklags, J. 2004 Privacy and rationality: preliminary evidence from pilot data. In *Proc. Third Workshop on the Economics of Information Security, Minneapolis, MN, 13–14 May 2004*.

Akerlof, G. A. 1970 The market for 'lemons': quality uncertainty and the market mechanism. *Q. J. Econ.* 84, 488–500. (doi:10.2307/1879431)

Albert, R., Jeong, H. & Barabási, A.-L. 2000 Error and attack tolerance of complex networks. *Nature* 406, 378–382. (doi:10.1038/35019019)

Anderson, R. J. 1994 Why cryptosystems fail. *Commun. ACM* 37, 32–40. (doi:10.1145/188280.188291)

Anderson, R. J. 2001 Why information security is hard—an economic perspective. In *Proc. Seventeenth Annual Computer Security Applications Conf., New Orleans, LA, 11–14 December, 2001*, pp. 358–365.

Anderson, R. J. 2005 Open and closed source systems are equivalent (that is, in an ideal world). In *Perspectives on free and open source software*, pp. 127–142. Cambridge, MA: MIT Press.

Anderson, R. J. 2008 The economics and security resource page. See http://www.cl.cam.ac.uk/rja14/econsec.html.

Arora, A., Krishnan, R., Nandkumar, A., Telang, R. & Yang, Y. 2004 Impact of vulnerability disclosure and patch availability—an empirical analysis. In *Proc. Third Workshop on the Economics of Information Security, Minneapolis, MN, 13–14 May 2004*.

Asch, S. E. 1951 *Social psychology*. New York, NY: Prentice-Hall.

Atran, S. 2003 Genesis of suicide terrorism. *Science* 299, 1534–1539. (doi:10.1126/science.1078854)

Ayres, I. & Levitt, S. 1997 Measuring positive externalities from unobservable victim precaution: an empirical analysis of Lojack. *Q. J. Econ.* 113, 43–77. (doi:10.1162/003355398555522)

Bohm, N., Brown, I. & Gladman, G. 2000 Electronic commerce: who carries the risk of fraud? *J. Inform. Law Technol.* 3.

Böhme, R. & Kataria, G. 2006 Models and measures for correlation in cyber-insurance. In *Proc. Fifth Workshop on the Economics of Information Security, Cambridge, UK, 26–28 June 2006*.

Camp, J. & Wolfram, C. 2000 Pricing security. In *Proc. CERT Information Survivability Workshop, 24–26 October 2000*, pp. 31–39.

Campbell, K., Gordon, L. A., Loeb, M. P. & Zhou, L. 2003 The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *J. Comput. Secur.* 11, 431.

Danezis, G. & Anderson, R. 2005 The economics of resisting censorship. *IEEE Security Privacy* 3, 45–50. (doi:10.1109/MSP.2005.29)

Edelman, B. 2006 Adverse selection in online 'trust' certificates. In *Proc. Fifth Workshop on the Economics of Information Security, Cambridge, UK, 26–28 June 2006*.

Gilbert, D. 2006 If only gay sex caused global warming. *Los Angeles Times* 2 July 2006. Goodhart, D. 2004 Too diverse? *Prospect*. See http://www.guardian.co.uk/race/story/0,11374,1154684,00.html.

Humphrey, N. 2003 *The inner eye:*

social intelligence in evolution. New York, NY: OxfordUniversity Press.
Jakobsson, M. & Myers, S. 2007 *Phishing and countermeasures*. New York, NY: Wiley.
Katz, M. L. & Shapiro, C. 1985 Network externalities, competition, and compatibility. *Am. Econ.*
Rev. 75, 424–440.
Kunreuther, H. & Heal, G. 2003 Interdependent security. *J. Risk Uncertain.* 26, 231–249. (doi:10.
1023/A:1024119208153)
Loewenstein, G. 2008 The best of strangers. In *Workshop on Security and Human Behaviour, Boston, 1 July 2008*. See www.lightbluetouchpaper.org.
Milgram, S. 1974 *Obedience to authority: an experimental view*. New York, NY: HarperCollins. Moore, T. 2005 Countering hidden-action attacks on networked systems. In *Proc. Fourth Workshop on the Economics of Information Security, Cambridge, MA, 2–3 June 2005*.
Muller, J. 2006 *Overblown: how politicians and the terrorism industry inflate national security threats, and why we believe them*. New York, NY: Free Press.
Nagaraja, S. & Anderson, R. J. 2006 The Rescorla, E. 2004 Is finding security holes a good idea? In *Proc. Third Workshop on the Economics of Information Security, Minneapolis, MN, 13–14 May 2004*.
Schechter, S. E. 2004 Computer security strength and risk: a quantitative approach. PhD thesis, Harvard University, Cambridge, MA.
Varian, H. 2000 Managing online security risks. *The New York Times*, 1 June 2000.
Varian, H. 2004 System reliability and free riding. In *Economics of information security* (eds
Privacy and rationality: preliminary evidence from pilot data. In *Proc. Third Workshop on the Economics of Information Security, Minneapolis, MN, 13–14 May 2004*.
Akerlof, G. A. 1970 The market for 'lemons': quality uncertainty and the market mechanism.
topology of covert conflict. In *Proc. Fifth Workshop on the Economics of Information Security, Cambridge, UK, 26–28 June 2006*.
Newman, M. E. J. 2003 The structure and function of complex networks. *SIAM Rev.* 45, 167–256. (doi:10.1137/S003614450342480)
Odlyzko, A. M. O. 2003 Privacy, economics and price discrimination on the Internet. In *Fifth Int.*
Conf. Electronic Commerce, pp. 355–366. New York, NY: ACM Press.
Ozment, A. 2005 The likelihood of vulnerability rediscovery and the social utility of vulnerability hunting. In *Proc. Fourth Workshop on the Economics of Information Security, Cambridge, MA, 2–3 June 2005*.
Ozment, A. & Schechter, S. E. 2006*a* Bootstrapping the adoption of internet security protocols. In *Proc. Fifth Workshop on the Economics of Information Security, Cambridge, UK, 26–28 June 2006*.
Ozment, A. & Schechter S. E. 2006*b* Milk or wine: does software security improve with age? In *Proc. Fifteenth USENIX Security Symposium, Vancouver, BC, 31 July–4 August 2006*, pp. 93–104.
L. J. Camp & S. Lewis), pp. 1–15. Dordrecht, The Netherlands: Kluwer.
Varian, H. 2005 Keynote address to the Third Digital Rights Management Conference, Berlin, Germany, 13 January 2005.
Whitten, A. & Tygar, J. D. 1999 Why Johnny can't encrypt. In *Proc. Eighth USENIX Security Symposium, Washington, DC, 23–26 August 1999*, pp. 169–184.
Zimbardo, P. 2008 *The Lucifer effect*. New York, NY: Random House.

Q. J. Econ. 84, 488–500. (doi:10.2307/1879431)
Albert, R., Jeong, H. & Barabási, A.-L. 2000 Error and attack tolerance of complex networks.
Nature 406, 378–382. (doi:10.1038/35019019)
Anderson, R. J. 1994 Why

cryptosystems fail. *Commun. ACM* 37, 32–40. (doi:10.1145/188280.
188291)
Anderson, R. J. 2001 Why information security is hard—an economic perspective. In *Proc. Seventeenth Annual Computer Security Applications Conf., New Orleans, LA, 11–14 December, 2001*, pp. 358–365.
Arora, A., Krishnan, R., Nandkumar, A., Telang, R. & Yang, Y. 2004 Impact of vulnerability disclosure and patch availability—an empirical analysis. In *Proc. Third Workshop on the Economics of Information Security, Minneapolis, MN, 13–14 May 2004*.
Asch, S. E. 1951 *Social psychology*. New York, NY: Prentice-Hall.
Atran, S. 2003 Genesis of suicide terrorism. *Science* 299, 1534–1539. (doi:10.1126/science.1078854) Ayres, I. & Levitt, S. 1997 Measuring positive externalities from unobservable victim precaution:
an empirical analysis of Lojack. *Q. J. Econ.* 113, 43–77.
Anderson, R. J. 2005 Open and closed source systems are equivalent (that is, in an ideal world). In *Perspectives on free and open source software*, pp. 127–142. Cambridge, MA: MIT Press.
Anderson, R. J. 2008 The economics and security resource page. See http://www.cl.cam.ac.uk/
rja14/econsec.html.
(doi:10.1162/003355398555522) Bohm, N., Brown, I. & Gladman, G. 2000 Electronic commerce: who carries the risk of fraud?
J. Inform. Law Technol. 3.
Böhme, R. & Kataria, G. 2006 Models and measures for correlation in cyber-insurance. In *Proc. Fifth Workshop on the Economics of Information Security, Cambridge, UK, 26–28 June 2006*.
Camp, J. & Wolfram, C. 2000 Pricing security. In *Proc. CERT Information Survivability*
Workshop, 24–26 October 2000, pp. 31–39.