COMS30038 — SECURITY BEHAVIOURS

SECURITY ECONOMICS: SECURITY ECONOMICS

Matthew Edwards[*]

---

1 SECURITY ECONOMICS

You hopefully now have a sense of one role that economics has in cybersecurity – understanding the economies of cybercriminals allows us to design interventions that can not just take down individual criminals or hubs of organised crime, but undermine the methods through which they make money, disrupting a whole industry of online crime. We should remember that not all cybercriminals are interested in making money – some cybercriminals are motivated by ideology, or personal grievances. Yet it is also worth remembering not all security problems are the result of cybercriminals per se – previously in this course we have discussed the role of state actors, who might arguably not count as 'criminals', and as will be discussed later in the course security incidents can arise from ordinary human error, unforced by any malicious actor. Can economics apply to problems like these? The answer is, perhaps surprisingly, that it can.

The reason it might seem strange is because in some of these cases there appears to be no money involved – people do not in general engage in cyberbullying because they're getting paid for it, for example. However, economics is not really about the study of money, but the study of *incentives* and how these affect the interactions of economic agents. This turns out to align quite neatly with a growing sense that some of the most important problems in security are not, at root, technical problems, but instead problems that arise from people or organisations simply *not caring* enough about certain security issues, or how responsibility for problems ends up being distributed.

In Douglas Adams' "Life, the Universe and Everything"[1], he introduces the notion of a "Somebody else's problem" field that acts as a cloaking device. Rather than physically hiding something like a standard invisibility field would, a SEP field simply emits a strong suggestion that whatever is happening

[*]matthew.john.edwards@bristol.ac.uk

[1]An excellent book that otherwise has essentially nothing to do with economics, or indeed security. Though it does contain killer robots.

within it simply isn't worth paying attention to, because whatever is happening there is somebody else's problem. People can see what is happening within a SEP field, but they just don't really notice it, and definitely don't do anything about it. Security economics is, to some approximation, the study of SEP fields, and how they can be manipulated or destroyed.

To give a slightly less fanciful example, one of the key observations that sparked the modern field of security economics centred on a historical moment in banking, and card fraud. Due to certain legal precedent, a situation had arisen where, in the US, banks were generally the ones liable for card fraud. If a false transaction occurred on an account, then the customer could dispute it, and the bank must either prove that the customer was trying to cheat them or issue a refund. In the UK and some other European countries, on the other hand, the burden of proof was largely the other way around, and the customer had to demonstrate that the bank was at fault in order to get their money refunded. Now, in which case do you think the banks had better security? When the costs of card fraud would generally fall on the customer, or when costs of card fraud would generally fall on the banks themselves? If your impulse is to the latter, you're correct – the US banks suffered less fraud, despite spending less on security, because their systems were in general less complacent about card fraud [1].

This is a classic situation for security economics. In general, whenever you see a case where the party who is in a position to protect a system is not the one who will suffer when they fail, you are likely to have a problem [1]. Another example of this arose with botnet-controlled machines being used in distributed denial-of-service attacks in the early 2000s. Some security analysts were puzzled as to why consumers were not protecting their systems with anti-virus products. However, this makes perfect sense when the incentives are analysed – a customer might be willing to pay to protect their own machine from being trashed by malware, but in general the malware wasn't harming the *customer*'s machine, it was just using their machine to take down the websites of some rich organisations. If you attempt to explain to a customer that they should pay $40-100 in order to protect Microsoft's website, you can expect a cold reception [1]. This is somebody else's problem – specifically, Microsoft's. Of course, the inverse of this also holds: when you find someone who is being hit particularly hard by a security problem, you have a motivated party for dealing with that problem. When one of the largest spam botnets, Rustock, was taken down in 2011, it was a joint effort on the part of several security experts, together with Microsoft and Pfiezer. Why were Microsoft and Pfiezer involved? Well, Rustock primarily sent spam via Hotmail accounts, creating a burden on Microsoft's infrastructure, and Pfiezer is the patent-holder for Viagra – the product that most of the spam was offering cheap counterfeit versions of [2]. You can generally count on actors to follow their own self-interests, and this produces both good (e.g., stopping crime) and bad (e.g., committing crime) behaviour.

An issue generally confronted by economics is that of *externalities*, or costs

to other people, and how they become a general problem for everyone even when it's in nobody's interest for this to be the case. The classic example is known as the tragedy of the commons. The commons is a plot of communally-owned field near a village, on which each villager has the right to let a limited number of cattle graze, with the purpose of easing the burden of feeding their herds. The temptation for each villager is to allow more than their permitted number of cattle to graze on the commons – they are unlikely to be caught, and it benefits them directly. In fact, the more of their cattle they bring to the commons, the more they benefit. The bind is, every villager faces the same incentives, and because they allow more and more cattle to graze on the commons, the commons becomes overgrazed and barren, and ends up no longer capable of supporting cattle – so the tragedy is that nobody can graze their cattle there anymore. Of course, I'm not telling you this because I expect you to have an interest in communal livestock management. The point of the analogy is that following individual incentives can lead to a collective deficit, and it turns up throughout society – another classic framing is overfishing, where each fisherman benefits from catching as many fish as he can, but fishing as an industry suffers from overfishing, since it becomes harder and harder to fish a depleted ocean. In security, the tragedy of the commons appears as a failure to maintain security—and trust—at various levels of the internet. Participants like end-users, ISPs and software developers all make choices that increase their individual reward while decreasing collective trust and security, and decreasing our collective capacity to benefit from the Internet [3]. For example, if software companies put more effort into preventing their systems from being exploited, this would improve collective security – but their individual incentives are often to get products to market as quickly as they can, and offload security considerations to the users of the product, who are least able to bear them.

Economics also explains some other security issues in the software market. For example, if security features cost money, is expensive software more secure? Economics has the concept of a "market for lemons" [4]. A "lemon" is American slang for a car that you discover is defective after you have bought it. The idea is that customers cannot tell the difference between a good car and a lemon. If a reasonable price for a good car is $3000, and a reasonable price for a lemon might be far less, perhaps $1000, then a customer who is unable to determine the quality of the goods in front of them might take an equal-odds position and decide that they could spend $2000 on a car, to factor in the chance that it might be a lemon. This works against them, however – sellers know whether or not their car is a lemon, and if their car is good then they know it is worth more, and they won't sell. So by and large only lemons will get sold, and buyers will get the impression that goods on the market are of low quality, and start to decrease the price they are willing to pay even further. The situation arises because of an asymmetry – the lack of information on the buyers' part effectively drives high-quality goods from the market. In software security, buyers generally have no idea whether what they

are buying is secure software[2], so a security lemon market is born – cheaper, less-secure products drive out more secure products[3].

Another asymmetry highlighted by economics is the asymmetry of effort when it comes to bug-finding. The question is: given that MacOS developers know its code better than random hacker somewhere, and are better-funded and equipped to search for bugs, why do hackers still manage to find vulnerabilities before the developers and maintainers? The answer is that they both do and don't. Say there are, for sake of argument, one million bugs to find, each taking an average of 1,000 hours of work to uncover. A defender that invests 10 million hours of work in a year might recover and patch 10,000 bugs, while an attacker that invests a measley 1,000 hours of work over a year will find a vulnerability – and the chance that their discovery was also one of the 1% of bugs the defender patched is very low. Even though the incentives are high for the defender, and they're accordingly investing much more into finding vulnerabilities than the attacker, the realisation of the vulnerability is different for the different parties – for a defender, finding a vulnerability is a slow process of creating defences, but any gap in the wall they miss is enough to allow an attacker in.

Generally, security economics gives us a lens for making both theoretical and quantifiable arguments about broad policies and strategies for dealing with security. To take an example, the above argument about the asymmetry of effort led to the question of whether the current practices around finding and reporting vulnerabilities were in fact a good idea – since it seemed like if anything, openly reporting vulnerabilities actually helps the attackers, both by telling them how to attack unpatched systems, and allowing them to direct their efforts for finding new bugs [5]. Empirical observation, however, demonstrated that the effect of vulnerability disclosure was more positive than might be thought – while initially it leads to a spike in attacks exploiting the vulnerability, as predicted, this soon decreases over time, while 'secret' vulnerabilities that aren't reported show a steady increase in attacks over time, until they are reported and patched, when they show a substantial decrease [6] – supporting the current reporting practices. This interplay between the prediction of behaviour based on a model of incentives, the realisation of this in terms of concrete policies, and a correction of the model by empirical data is all a core element of how economics can benefit security at a large scale.

[2]Sometimes intentionally, because the authors want to use closed source models and DRM to obfuscate their product, in order to create lock-in that captures users from the market.

[3]Open source software somewhat breaks this model, however.

2 INTERVENTIONS

So, what does it mean to make a cybersecurity intervention using security economics? There are whole areas of economics that focus on an individual or firm's decision-making under different incentive structures, but one of most straightforward models to use is that of the *cost-benefit tradeoff* for security investment. Under such a model, an organisation works to balance their investment in security measures against the *expected losses* that would occur were they not to take any action. The firm does not want to be spending *too much* on security by paying £10,000 to avoid £1,000 in damages; at the same time the firm wants to avoid under-investing and suffering damages it could have averted for a small cost. Ideally, the firm wants to spend just enough on security that they come out ahead.

One of the issues with attempting to account for security economically is that while the investments are very visible on the balance sheet—SOC staff, security technologies, staff training days—the benefits are harder to quantify. There are no 'units of security' that get produced to be stockpiled or traded, and to the decision-makers of the firm security can seem like a black hole that simply absorbs funding and as a result, at best, nothing happens. The answer to this is to quantify the security risk that the organisation is currently exposed to, and express the benefits of security investments as quantifiable reductions in that risk. Approaches to such risk modelling can be diverse[4], but a simple and common approach is to quantify your *expected* losses by multiplying the cost of some damage that would occur by the probability that such an attack would happen. This quantifies your risk in ordinarily-interpretable figures, so an attack that has a 20% chance of taking place and would cause £1,000 of damage if it happened is represented as a £200 risk. This is a figure that can then be used to justify extra spending on security that would mitigate this risk, up to a cap of £200. The quantifiable benefit of security spending is then the reduction in expected losses. This is the kernel of what is known as the Gordon-Loeb model [8] of information security investment.

As was discussed in the previous section, one of the ways security incentives can go wrong is when addressing the security risk is the responsibility of an actor that will not suffer the consequences for failure. Looking at the expected loss framework outlined above, you might be able to see why. If the firm's own expected losses from an attack are zero, or at least negligibly small, then there is no business justification for spending on security to prevent that attack—the attack is somebody else's problem. Take, for example, a company that holds a lot of sensitive private information on its customers in an insecure manner. Absent external pressures, there may be no reason for the company to invest in securing this information. Attackers that gather this information from the company's servers will go on to cause damage to the *customers*, not the company. The expected loss is nothing, so there are no quantifiable benefits to spending on security, and so the incentives are for the company to spend

[4] See Pan & Tomlinson [7] for an overview.

its money on something else instead[5].

The above incentive structure is leading to a societally bad outcome: people's information is being harvested by attackers and exploited, but the firms it is being stolen from have no reason to better secure their databases. An intervention is needed. Note that what is needed here is not more secure database technology—this could already be very available—but more reason for companies to invest in it. Regulations and legal liability are the common tools of choice here for intervening in market failures. Even simply forcing firms to publicly report on data breaches may start to affect their expectation of losses. Where previously a breach could be ignored and kept quiet, a public disclosure could lead to stock price plunges and customers cancelling business. If these risks are not sufficient, regulators can also impose fines on firms that suffer breaches, adding a minimum threshold to the damages a firm can expect if they suffer an attack – and thereby providing the incentive for them to spend on security in proportion to the risk of receiving such a fine.

Of course, such incentives only appear if regulations are properly enforced, and non-compliance punished. For various reasons, the state may not always want to be directly involved in enforcement of penalties – for one, hiring inspectors is an expensive use of taxpayer money. An alternative to direct enforcement of regulations is for legislation to make firms (or individuals) legally liable for damages occurring to others. Rather than setting up a body to investigate firms that may not be reporting data breaches, the legal situation can be arranged so that private actors (such as customers) can sue firms for causing damages through lax security. This enables the incentives to be changed through penalties (levied via the civil courts), but avoids the state having to use public money to enforce regulation. The conditions under which firms can be held liable can even be targeted specifically to encourage the behaviour desired. For example, in the US, the Digital Millennium Copyright Act provides a "safe harbour" for online service providers, exempting them for liability in matters of copyright infringement, but on the condition that they act promptly to take down material when served with a notice from the rightsholder. The threat of liability is here being used to compel online service providers into taking action.

There are problems to solve in the 'security market' other than just parties creating externalities because they don't have sufficient incentive to invest in security. It can also be the case that a firm is *attempting* to purchase security, but failing to do so because of information asymmetries – they know less about security products than the people selling them do, and so can't purchase risk reductions effectively. Reflect on the 'lemon market' dynamic from the previous section, and you'll see how much of a problem this could be. To address this, one tool regulators have is certification – making it possible for products (or services) to be 'certified' by an expert body so that uninformed consumers can be sure of what they are buying. To avoid spending wastefully, then, firms

[5] It's a little too simple to say there are *no* losses involved in this scenario – there could be an effect on the company's reputation, or the information may be valuable to their competitors.

could buy security risk reductions from accredited providers. Ideally, this creates a more level informational playing-field within the security market, but there are also potential risks. If the number of certified providers is a small, closed set then they may operate as a cartel, collaborating to keep prices high. If certification is not properly controlled, however, poor providers may slip through certification, degrading the value of certification as a marker of quality. Depending on the conditions, it's even possible that security certification could itself be subject to market forces, with providers going to whichever certification system they believe will be most accommodating.

3 OPTIONAL EXERCISES

These are suggestions for students who are particularly interested in the topic of security economics. They are not assessed in any way. You don't need to complete the below to do well on the course.

3.1 *Further Reading*

One of the best resources for security economics reading is Ross Anderson's website[6]. Anderson was one of the three individuals who simultaneously arrived at the idea of using economics to understand broad problems in security, and maintains a list of top publications from across the field.

REFERENCES

References

[1] R. Anderson, "Why information security is hard - An economic perspective," in *Seventeenth Annual Computer Security Applications Conference*. IEEE, 2001, pp. 358–365.

[2] J. M. Rao and D. H. Reiley, "The economics of spam," *Journal of Economic Perspectives*, vol. 26, no. 3, pp. 87–110, 2012.

[3] R. Hurwitz, "Depleted trust in the cyber commons," *Strategic Studies Quarterly*, vol. 6, no. 3, pp. 20–45, 2012.

[4] G. A. Akerlof, "The market for "lemons": Quality uncertainty and the market mechanism," *The Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488–500, 1970.

[5] E. Rescorla, "Is finding security holes a good idea?" *Security & Privacy*, vol. 3, no. 1, pp. 14–19, 2005.

[6] A. Arora, A. Nandkumar, and R. Telang, "Does information security attack frequency increase with vulnerability disclosure? an empirical analysis," *Information Systems Frontiers*, vol. 8, no. 5, pp. 350–362, 2006.

[6] https://www.cl.cam.ac.uk/~rja14/econsec.html

[7] L. Pan and A. Tomlinson, "A systematic review of information security risk assessment," *International Journal of Safety and Security Engineering*, vol. 6, no. 2, pp. 270–281, 2016.

[8] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457, 2002.