Security Engineering

The economics of security

Ross Anderson

Security economics

- If Alice guards a system but Bob pays the cost of failure, you can expect trouble!
- Economic analysis lets us identify
  - When firms have no incentive to collaborate at all
  - How firms acquire and abuse market power
  - How market failures lead to security failures
  - What sort of crimes scale
- Economic tools also let us quantify harm and prioritise responses; we'll look at cybercrime
- Analysis plus data can help influence policy

Cooperation or conflict

- One way of getting what you want is to make it, or make something else and trade for it – 'Economics'
- Another way is to just take it, whether by force or via the ballot box – 'Politics'
- Choices between cooperation and conflict are made at many levels all the time, between people, organisations and states
- We can analyse them using game theory

Game theory

- The study of problems of cooperation and conflict among independent decision-makers
- Its focus is games of strategy, rather than chance
- It abstracts to players, choices, payoffs, strategies
- There are
  - games of perfect information (such as chess and go)
  - games of imperfect information (which are often more interesting to analyse)
  - one-shot and iterated games

Strategic form

- Example: matching pennies. Alice and Bob throw H or T. If they're different, Alice gets Bob's penny; else he gets hers. The strategic form is

Bob

Alice	H	T
H	-1, 1	1, -1
T	1, -1	-1, 1

- This is an example of a zero-sum game: Alice's gain = Bob's loss

Dominant strategy equlibrium

- In the following game, Bob's better off playing left; similarly Alice is always better off playing bottom

Bob

Alice

	Left	Right
Top	1, 2	0, 1
Bottom	2, 1	1, 0

- A strategy is an algorithm: input state, output play
- Here, each player's optimal play is a constant
- The is called a 'dominant strategy equilibrium'

Nash equlibrium

- Consider this game:

Bob

Alice	Left	Right
Top	2, 1	0, 0
Bottom	0, 0	1, 2

- Each player's optimal strategy depends on what they think the other will do
- Two strategies are in Nash equilibrium when A's choice is optimal given B's, and vice versa
- Here there are two: top left and bottom right

Prisoners' dilemma

- Alfie and Benjy are arrested on suspicion of planning a robbery. The police tell them separately: if neither confesses, one year each for gun possession; if one confesses he goes free and the other gets 6 years; if both confess then each will get 3 years

Benjy

Alfie

	confess	deny
confess	-3, -3	0, -6
deny	-6, 0	-1, -1

- (confess, confess) is the dominant strategy equilibrium
- It's obviously not optimal for the villains!
- Is this a problem? If so, what's the solution?

Prisoners' dilemma (2)

- You might answer 'serves them right'!
- But this can't apply to all instances of the dilemma
  - Reducing carbon emissions
  - Defence spending
  - Whether to extradite (or even investigate) people who commit crimes against residents of other countries
  - …
- Tough but inescapable conclusion: if the game is truly as described, there is no escape. Both will cheat rather than cooperate, and lose out
- To fix this, you need to change the game!

The evolution of cooperation

- If PD played repeatedly, there's a fix!
- 'Tit-for tat': cooperate at round 1, then at round n do what the other guy did at n-1
- Simulation competitions run by Bob Axelrod played off many iterated-game strategies; tit-for-tat did consistently well
- In the presence of noise, tit-for-tat gets locked into (defect, defect). So: forgive the other player occasionally
- People have realised in the last 30 years or so that strategy evolution explains a lot of behaviour

Game theory and evolution

- John Maynard Smith proposed the 'Hawk-dove' game as a simple model of animal behaviour. Consider a mixed population of aggressive and docile individuals:

	Hawk	Dove
Hawk	(v-c)/2, (v-c)/2	v, 0
Dove	0, v	v/2, v/2

- Food v at each round; doves share; hawks take food from doves; hawks fight (with risk of death c)
- If v > c, whole population becomes hawk (dominant strategy)
- What happens if c > v?

Game theory and evolution (2)

- If c > v, a small number of hawks will prosper as most interactions will be with doves. Equilibrium reached at hawk probability p setting hawk payoff = dove payoff

	Hawk	Dove
Hawk	(v-c)/2, (v-c)/2	v, 0
Dove	0, v	v/2, v/2

- i.e. $p(v-c)/2 + (1-p)v = (1-p)v/2$

  $\Leftrightarrow pv - pc + 2v - 2pv = v - pv$

  $\Leftrightarrow -pc = -v \Leftrightarrow p = v/c$

- Hence a spectrum of aggression (among people / firms / states)

When are markets efficient?

- Adam Smith described the ‘invisible hand’ of the market coordinating economic activity
- It took 200 years to make this precise!
- A market with many buyers and sellers will clear at a price where supply = demand
- Stanley Jevons / Karl Menger, 19th century: this is where the marginal supplier is just breaking even
- When is this efficient?

What is efficiency?

- A Pareto improvement is a change that makes at least one player better off without making anyone worse off
- A Pareto efficient allocation has no Pareto improvements
- This is a very weak definition!
- It says nothing about fairness – for example, pure communism (everyone gets the same) is Pareto efficient, as is pure monarchy (the king gets the lot)

So are markets efficient?

- Victorian model: markets efficient if no monopoly
- Welfare theorems (Arrow & Debreu, 1948)
  - First theorem: market equilibrium is Pareto optimal
  - Second theorem: any Pareto optimal allocation can be achieved by market forces provided preferences are convex
  - Conditions include rational actors, property rights, complete information, no transaction costs
- The interesting cases for us are where these conditions fail (firms try to make them fail in order to create monopolies and make money :-)

Competition and information

- The marginal cost of producing information is zero, so that's often the market clearing price!
- Example – machine-readable phone books
  - 1986 – Nynex charge $10,000 per disk
  - ProCD had the phone book retyped in Peking and started selling for $300
  - ABI joined in and the price collapsed to $20
- By 1998 it was sort-of free online
- Hence Wikipedia, Linux, and the Free Software Foundation slogan: 'information wants to be free'
- So how can you make money out of selling information – software, books, music, …?

Externalities

- Externalities are goods / bads people care about, but not traded: they are typically side-effects
- Negative externalities include a steelworks polluting a fishery, firms and households emitting CO_2 and insecure IoT devices ending up in botnets
- Positive externalities include education (1 more year = 2% crime reduction), tech standards, …
- In the presence of externalities, competitive equilibria are unlikely to be Pareto efficient
- Can in theory fix with property rights (steelworks), but this is hard with many players (households, IoT)

Public goods

- A public good is non-rivalrous and non-excludable
- Example: scientific knowledge. The producer can appropriate a small part of the benefit (e.g. PhD thesis); the rest spills over to all
- Example of a public bad: CO_2 emissions. Again, everyone gets to 'consume' the same amount
- Strong temptation for people to free-ride!
- Topical example: policing cybercrime. The US agencies (FBI, secret service...) spend as much as the next 10 countries together (as with conventional defence!)

Network externalities

- Many networks become more valuable to each user the more people use them
- Metcalfe's law: the value of a network is proportional to the square of the number of users
- It's actually more complex than this
- Overall effect: past some threshold, network use takes off rapidly (and creates lock-in)
  - Telephone – late 19th century
  - Email – 1995–99
  - Facebook – 2008–11

Technical lock-in

- Often, buying a product commits you to buying more of it, or spending money on one or more of:
  - durable complementary assets, such as apps
  - skills, e.g. fluency with Win/Mac/Linux or Office
  - Services – network service, cloud service, subscription
- Same applies to services – cloud service firms make it hard to switch to their competitors (how?)
- This is not new (last century, fewer people changed their bankers than their spouses) but has pronounced effects in information goods markets

Switching costs

- 'Fundamental theorem' (Shapiro, Varian); the net present value of your customer base is the total cost of switching
  - Suppose you're an ISP and it costs £25 to set up a new customer
  - Suppose it costs a customer £50 of hassle to switch
  - If your new business model makes the customer worth £100, offer them £60 cashback to switch
  - They're £10 ahead, you're £15 ahead
- So the value of Microsoft is what it would cost people to switch to Google Docs and Linux …

Vendor security vs user security

- Each of these factors – low marginal costs, technical lock-in and network externalities – tends to lead to a dominant-firm market model
- Given all three, monopoly is even more likely
- Hence the race for market share whenever a new product or service market opens
  - Microsoft ‘ship it Tuesday and get it right by version 3’
  - Android phones mostly not patched up to date
  - Facebook privacy theatre
- With two-sided markets, networks are built to appeal to the other side too!

Monopoly and policy

- Policy: do you hope that the incumbents become obsolete, or do you regulate?
- EU law: a fairly-won monopoly is OK but using dominance in one field to get it in another is illegal
- US: monopoly used to be measured by consumer surplus
- This doesn’t work for Google, Facebook, Amazon (or Wikipedia!)
- So new antitrust approaches being developed by the Biden administration

Asymmetric information

- Akerlof won the Nobel for the ‘market for lemons’
  - 100 used cars for sale – 50 good cars worth $2000, 50 lemons worth $1000
  - Buyers can’t tell difference – so price $1000
- One fix is for sellers to offer a warranty – this is cheaper for owners of good cars, so can act as a ‘signal’ for the hidden information
- Why is an Edinburgh degree valuable? Interviews don’t always measure the right things, so many employers use education as a signal
- Signaling theory underpins recommender systems

Asymmetric information (2)

- Do Volvo drivers have more accidents because:
  - Bad drivers buy a Volvo to survive accidents better (hidden information, or 'adverse selection')
  - Volvo drivers compensate for safety by driving faster (hidden action, or 'moral hazard')?
- Adverse selection can lead to a "lemons market" – security products and services
- Moral hazard can trash insurance markets; hence excess, no-claims bonus, …
- Cyber-insurance is seriously hard! How secure is a firm really? Do you pay out on ransomware?

Econometrics

- It’s nice to have intuitive economic theories But are they right? The world is complex!
- So once we have theories, test them with data
- Example: in the 2000s, big debate about whether to publish security vulnerabilities
  - Never publish – vendors won’t patch
  - Publish at once – their customers get hacked
- Evidence led to system of coordinated disclosure, after a delay (90 days for Google, 45 for CERT...)
- Additions: bug bounties, vulnerability markets...

Cybercrime

- Measuring fraud and abuse is important, but hard
- Most sources of data have some agenda or other
- Banks will blame customers for fraud if they can
- Police massage the stats too – from 2005–15, they told victims to report fraud to the bank first
- For ten years, crime seemed to fall; it was going online, and most of the online stuff was ignored
- When the Office for National Statistics included fraud in their victimization survey, it shot up!

Measuring the Costs of Cybercrime

- We did surveys in 2012 and 2019
- Patterns mostly stable despite move from laptops to phones, from on-prem to cloud, and to “social”
  - Tax fraud, welfare fraud, several hundred £/$/€ p.p.p.a.
  - Payment fraud, several tens £/$/€ p.p.p.a.
  - ‘Pure’ cybercrime, several £/$/€ p.p.p.a.
- But cybercrime infrastructure (botnets) and countermeasures (AV) costs several tens!
- Notable change: ransomware / cryptocrime was $2bn pa. by 2018 and has grown since then