Advanced Network Security (2019-2020)

Economics of network security

Harald Vranken

Economics of network security

- Note that **network** in this lecture means
  - Physical communication network (eg. Internet, telephony, fax, telegraph)
  - Economic/virtual network of commercial and non-commercial transactions (eg. community of software users or credit card users)
- We focus on **network economics** to explain **security problems**

- How to handle security problems?
  - **Technical measures** (improve access control policy models, formal proofs of cryptographic protocols, approved firewalls, better ways of detecting intrusions and malicious code, …)
  - **Organisational measures** (improve regulations, responsibilities, governance, …)
  - **Economic measures**
    - What are costs (monetary, reputation, …) and benefits, for whom?
    - Can we adjust **economic incentives**?

Economics of network security

- More and more devices are connected to the Internet(-of-Things)
- Actions by one party might affect another party positively or negatively
- Can we explain why users/organisations (not) take particular security decisions?
  - Can we influence these decisions?
- We will look at security on a more societal level

Agenda

- Economically rational behaviour
- Incentives
- Externalities
- Liability
- Tragedy of the commons
- Markets for lemons (asymmetric information)
- Examples

Economically rational behaviour

- In economics: people only do things if these are economically rational to do
  - "Money makes the world go round"

- Why do people reject security advice?
  - Following the advice will shield them from direct costs of attacks, but burdens them with increased indirect costs

- Direct costs are generally small compared to indirect costs
  - Small chance of being attacked, and recovery requires one-time costs
  - Security advice applies to everyone, and following requires continuous costs
  - Hence, from a cost perspective, rejecting security advice makes sense!

Economically rational behaviour: patching

- Most malware attacks exploit known vulnerabilities for which patches are available

- Attacks could have been prevented if users would have patched their system

- Why didn't they patch?
  - Because they are lazy?
  - Because they are uninformed?
  - Because installing patches is difficult/not user-friendly?
  - Because they lack resources?
  - Or, because it is not economically rational to patch?

Economically rational behaviour: patching

Why is patching not economically rational?

- It is not just one patch
  - Eg. 22,538 vulnerabilities reported by VulnDB in 2019
    (ie. more than 60 each day)
- Patching can break your systems
  - Majority of the outages at a large Dutch telecom provider was due to their own patching

Economically rational behaviour: anti-virus

- Is it economically rational to use anti-virus software?
  - Costs: buying software, daily updating, regular scanning
  - Benefits: once in a while you catch malware (that might have caused harm)

- Banks require you to install anti-virus software when online banking
  - Who pays for anti-virus software?
  - Who is liable?
  - Who benefits?

Economically rational behaviour: more examples

- Example: security advice on choosing strong passwords
  - Largely ineffective if phishing and keylogging are main threats
  - Lock-out after *n* tries prevents online brute-force guessing or dictionary attacks
- Example: security advice to check URLs and recognize phishing sites
  - Largely ineffective since direct loss of users is on average less than a dollar a year
- Example: security advice on checking SSL certificates
  - Attackers avoid using certificates (no certificates on phishing sites and malware hosting sites)
  - Largely ineffective since nearly all certificate errors seen by users are false positives (expired or self-signed certificates, but no malicious intension)
- Also, benefits of security advice are often hugely exaggerated
  - Benefits are projected for worst-case harms, while users care only about average or actual harm
  - Even actual harms of some attacks appear greatly exaggerated (eg. 'only' 0.37% of users per year are victimized by phishing)

Economically rational behaviour: good or bad?

- Hence, not following security advices is economically rational:
  - Advices are complex and growing
  - Users pay indirect costs (mostly by spending their time)
  - Benefits are questionable
  - Users are only partly liable

- Although it is economically rational for users to ignore security advice, the advice is not bad!
  - It is still better to have strong passwords, change them often, and have a different one for each account

Economically rational behaviour: how to change?

- Need better understanding of the actual harms endured by user
  - Users mainly loose time and not money when attacked
  - Users also loose time when following security advice

- Cost of security advice should be in proportion to the victimization rate
  - All users bear costs for user education (security advices), while only victims have benefit
  - Target the at-risk users

- Respect users' time and effort
- Prioritize advice
- Retire advice that is no longer compelling

Economic incentives

- Incentives: factors that influence decisions made by individuals and organizations

- Rooted in economic, formal-legal, and informal mechanisms
  - Specific economic market conditions
  - Interdependence with other players
  - Laws
  - Social norms

- “Security failure is caused at least as often by bad incentives as by bad design” (Ross Anderson & Tyler Moore, 2006)

Security incentives

- Stakeholders of a system
  - The party who can implement security
  - The party who suffers from a securiy incident
  - The party who is liable in case of a security incident

- What is the incentive for implementing security if these parties are different?

- Example: stakeholders for medical payment system
  - Healthcare insurers — pay for development of system
  - Healthcare providers (hospitals, …) — should protect medical data
  - Patients — privacy

Security incentives

- Motivations for a party to (not) perform an action
  - Monetary gain/loss
  - Reputation
  - Peer pressure
  - Liability

Security incentives: ISPs

- ISPs have security-enhancing incentives (but implementation depends on their business models)

Security incentives: ISPs

- Example: incentives for dealing with spam
- Initially
  - Emails considered as personal property of recipients
  - Inspecting content of mails is a violation of privacy
  - End users are responsible for protecting their own systems and for dealing with spam
- Later
  - Exorbitant growth of spam (> 80% of all emails) changed financial implications for ISPs
  - Flood of spam became burden for network infrastructure requiring additional investment
  - Users of infected machines call help desk or customer service, with high cost for ISP
  - Abuse notifications from other ISPs and requests to fix the problem
  - In extreme cases, whole ISP could be blacklisted
  - ISPs started to filter incoming mail and to manage their customers' security more proactively

Misaligned/conflicting incentives

- Incentives for one party reward behaviour that is detrimental to other parties
- Can be repaired by removing/changing/adding incentives
- Typically done by regulation from government
- Example: carbon tax → polluter pays

Conflicting incentives

Player	Security-enhancing	Security-reducing
Internet service providers (ISPs)	Cost of customer support Cost of abuse management Cost of blacklisting Loss of reputation, brand damage Cost of infrastructure expansion Legal provisions requiring security	Cost of security measures Cost of customer acquisition Legal provisions that shield ISPs
Software vendors	Cost of vulnerability patching Loss of reputation, brand damage	Cost of software development and testing (time to market) Benefits of functionality Benefits of compatibility Benefits of user discretion Licensing agreements with hold-harmless clauses
E-commerce providers (banks)	Benefits of online transaction growth Trust in online transactions Loss of reputation, brand damage	Cost of security measures Benefits of usability of the service
Users	Awareness of security risks, realistic self-efficacy, exposure to cybercrime	Poor understanding of risks, overconfidence, cost of security products and services

Source: Cybersecurity: Stakeholder incentives, externalities, and policy options
J.M.Bauer & M.J.G. van Eeten
Telecommunications Policy 33(2009):706–719

Incentives of information technology markets

- Value of a product to a user depends on how many other users adopt it
- Technology often has high fixed costs and low marginal costs
  - Developing software is expensive, but manufacturing copies costs very little
  - Price competition drives revenues steadily down towards marginal cost of production
- Large costs to users from switching technologies (‘vendor lock-in’)

- Incentives for businesses
  - Selling on value rather than on cost
  - Create customer lock-in
    (instead of standard, well analyzed and tested architectures, implement security-by-obscurity)
  - First-mover advantages (“ship it on Tuesday and get it right by version 3”)
  - Make life easy for application developers (no mandatory security)

Externalities

- Definition (Oxford Dictionary)
  - A consequence of an industrial or commercial activity
  - which affects other parties
  - without this being reflected in market prices

- Side-effect of an event/transaction on third parties

- Can be either positive of negative

Negative externalities

- Classical example: pollution
- Reduction of pollution by a company costs money and has no direct effect on the company
- Society bears the consequences (externalities)
  - For example longevity, increased costs of healthcare, cleaning up

Source: https://flic.kr/p/2iGM5z

Positive externalities

- Example: improvement of houses in a neighbourhood
  - Will increase the value of other houses in the neighbourhood as well
- Example: vaccination
  - Majority of population vaccinated protects the other part of the population as well
- Opposite (degeneration if houses are not renovated, refusing vaccination) has negative externalities

Source: https://flic.kr/p/byeLgc

Externalities: spam

- Spammer’s goal is gaining money, doesn't care about externalities
- Sender’s incentives/costs
  - Might make money if spam is successful
  - Needs to invest in some minimal infrastructure to send spam
- Externalities
  - Infrastructure and bandwidth costs (for ISPs)
  - Time wasted by recipients (costs for users/employers)
- In general: total profit from cybercrime is relatively small, societal costs are much higher

Externalities: spam

- Example in numbers
  - Spam campaign in 2008 sent 350 million messages
  - Spammers gained $ 2,731
  - Assume: 1% of spam made it into in-boxes, absorbing 2 seconds/message of recipient's time
  - Corresponds to 1,944 hours of user time wasted, or $ 28,188 at twice the US minimum wage
  - Hence, externalities are more than 10× gain of spammer

Source: Spamalytics: An empirical analysis of spam marketing conversion
by C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage
Proceedings of the 15th ACM Conference on Computer and Communications Security, 2008, p.3-14

Externalities: online banking fraud

- Direct costs are zero-sum: gain of attacker = loss of bank and victims users
- Indirect costs are often many times larger

	Direct costs	Indirect costs (externalities)
Attacker	Gain	Don't care
Bank	Financial loss	More customer support, damage to reputation, decreased incentive for users to bank online
Victim users	Possible financial loss	Time for resolving fraud, possible costs when no longer banking or shopping online
Non-victim users	None	Follow security advice, possible costs when no longer banking or shopping online

Externalities: cybercrime

- Example: anti-virus software
  - Users buy anti-virus software to protect their own systems,
    but do they care about attacks launched from their systems against other systems?
- Example: DDoS
  - Should network operator from which the flooding traffic originates be responsible?
  - They can put pressure on users to install suitable defensive software (or supply it)
- Cybercriminal activity and information security markets co-evolve,
  mutually influencing but not fully determining each other's course
- Asymmetry in relation between the markets for cybercrime and cybersecurity
  - Higher/lower level of cybercrime will increase/decrease overall cost of security,
    effect on level of security remains ambiguous
  - Increased security will increase cost of cybercrime and/or reduce benefits cybercrime,
    hence increased security will reduce level of cybercrime

Policy instruments to enhance security

Predominant policy vector	Cybercrime	Information security
Legal and regulatory measures	• National legislation • Bi- and multi-lateral treaties • Forms and severity of punishment • Law enforcement	• National legislation/regulation of information security • Legislation/regulation of best practices to enhance information security • Liability in case of failure to meet required standards • Tax credits and subsidies
Economic measures	• Measures that increase the direct costs of committing fraud and crime • Measures that increase the opportunity costs of committing fraud and crime • Measures that reduce the benefits of crime	• Level of financial penalties for violations of legal/regulatory provisions (compensatory, punitive) • Payments for access to valuable information • Markets for vulnerabilities • Insurance markets
Technical measures	• Redesign of physical and logical internet infrastructure	• Information security standards • Mandated security testing • Peer-based information security
Informational and behavioral measures	• National and international information sharing on cybercrime	• National and international information sharing on information security • Educational measures

Source: Cybersecurity: Stakeholder incentives, externalities, and policy options
J.M.Bauer & M.J.G. van Eeten
Telecommunications Policy 33(2009):706–719

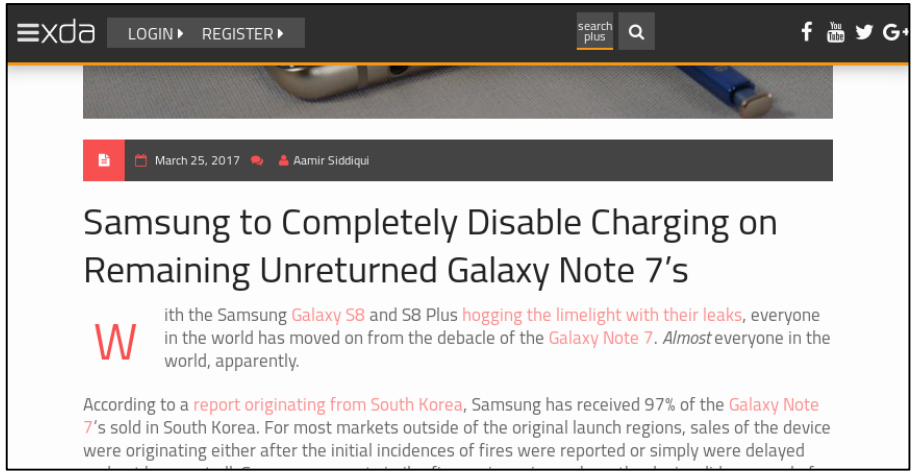
Liability

- Liability can be used to get rid of misalignment of incentives
- Special case: intermediary liability
- Clear liability for physical products
- What about software?
  - Typically no liability
  - The user has to bear the consequences of serious security bugs
- Risk dumping rather than risk management

- Prevention: safety regulation
- Reactive: liability

Liability: phones

- Phones often do not receive updates anymore
  - Manufacturer wants you to buy new phone
  - Reduced performance iOS update
  - Battery life
- Accidents with battery catching fire



Tragedy of the commons

- Users of a shared, unregulated resource that everyone can use for free
  - users act independently according to their own self-interest
  - deplete or spoil that resource through their collective action
  - contrary to the common good of all users

- The increased benefit of one party leads to small costs of other parties, but finally the shared resource will be depleted completely

- How to solve?

Source
- 1833, William Forster Lloyd, unregulated grazing on common land
- 1968, Garrett Hardin, modern economic context

Tragedy of the commons: examples

- Example: Wifi in the train

Market for lemons

- Occurs when there is information asymmetry
  - For example, between user and manufacturer, or consumer and seller
- “Lemon” (slang) is a car that is found to be defective only after it has been bought
- Consumers cannot distinguish the difference in quality between products
- Consumers will base price on price of average product
- Sellers of higher quality product will not be able to compete and leave
- Continues until left with only sellers of lowest quality products
- Even worse when people evaluating products are not the ones who suffer when they fail

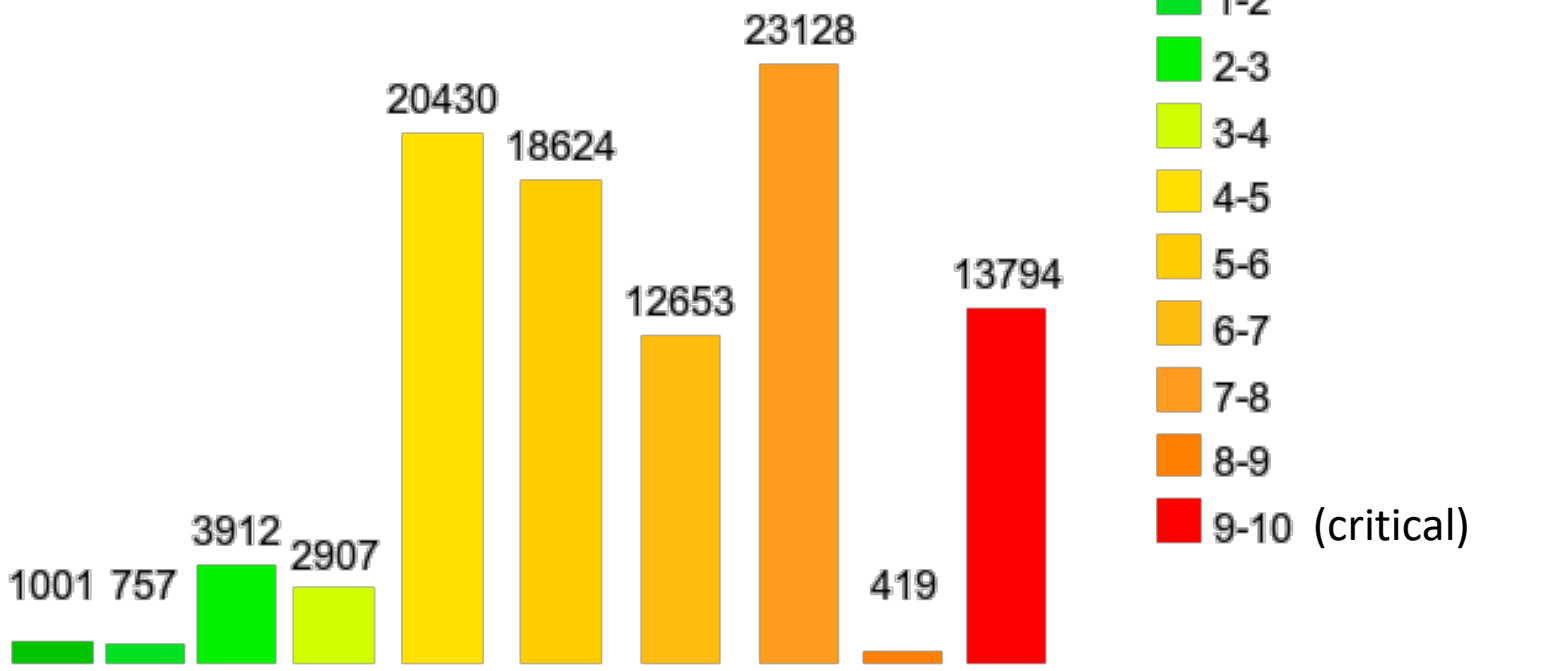
Source: Akerlof, 1970

Market for lemons: examples

- Information asymmetry holds very much for security products
  - Secure USB sticks
  - IoT devices

Market for lemons: CVSS score

- Common Vulnerability Scoring System (CVSS)
- CVSS score assigned to reported vulnerabilities
  - de-facto standard framework for vulnerability risk assessment
- Are high-rated vulnerabilities a problem?



Market for lemons: CVSS score

- Incentives for security researchers
  - High score means more credits and, possibly, higher bounty
- Incentives for security supplier
  - Avoid low rating of vulnerabilities that are used later to compromise clients

- However, many high-rated vulnerabilities are never actually exploited

- “CVSS is DoS-ing your own patching” – Luca Allodi

Agenda

- Economically rational behaviour
- Incentives
- Externalities
- Liability
- Tragedy of the commons
- Markets for lemons (asymmetric information)
- Examples

Example: botnets

- Incentives and externalities related to botnets
- Users of infected machines might not be directly affected
  - Cleaning machine costs time
- The user's ISP might not be directly impacted
  - Eg. every bot only generates a small part of DDoS traffic
- Some bots do not activate in the home country of the bot master
  - Reduce incentive for local law enforcement

- Every infected machine contributes small part, but together they form a serious problem

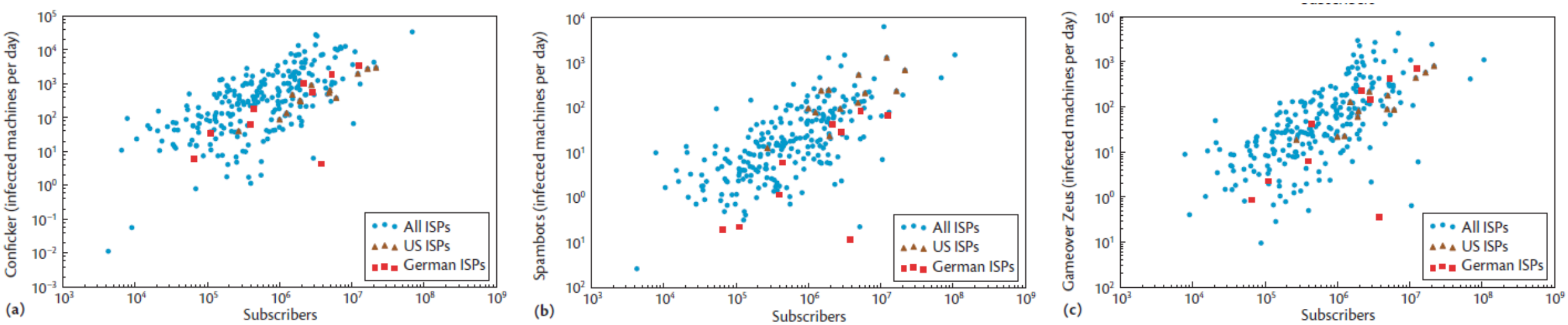
Example: ISPs

- ISPs are typically not directly affected by malware infections of their customers
- Yet, in a good position to address it
  - Filtering outgoing traffic
  - Quarantaining customers
- Why would they (not) get involved?
  - Monetary costs
  - Intermediary liability
  - Peer pressure and reputation
  - Abuse complaints

- National organisations to support this and share costs

Example: ISPs

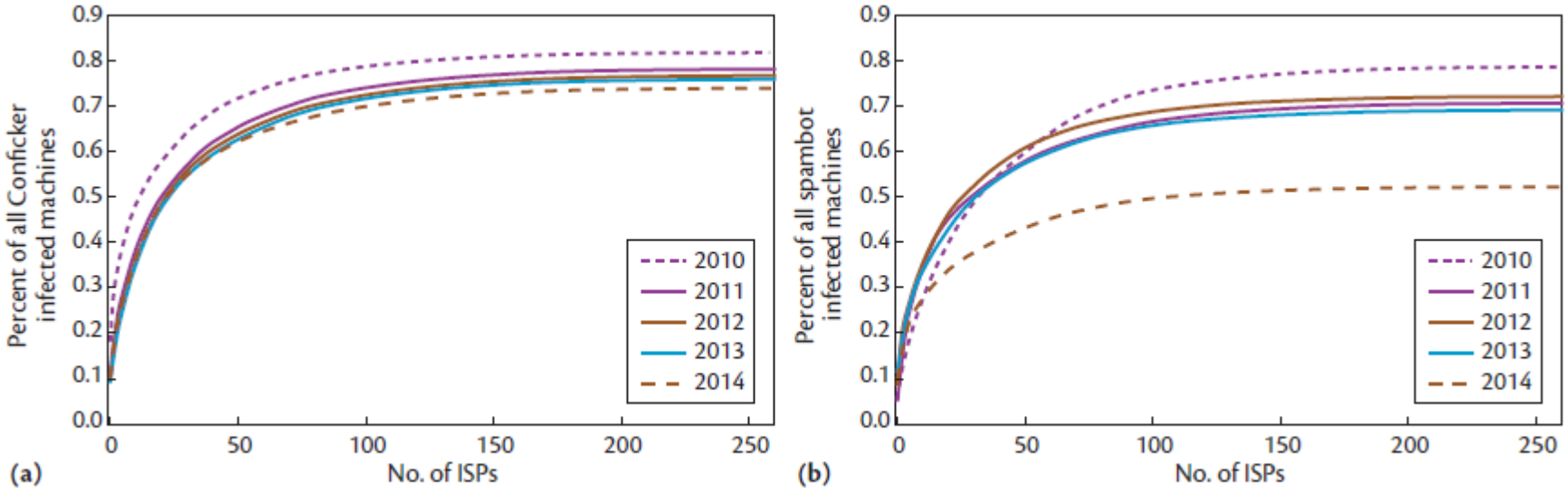
- Relation between ISP size (number of subscribers) and infection levels:
  in general, more subscribers means more infections
- Large variations in infection levels of similarly sized ISPs
  (even in same country, under same competitive pressures and regulatory framework)



Source: Economics of fighting botnets: lessons from a decade of mitigation
H. Asghari, M.J.G. van Eeten, J.M. Bauer
IEEE Security & Privacy, September/October 2015, 16-23

Example: ISPs

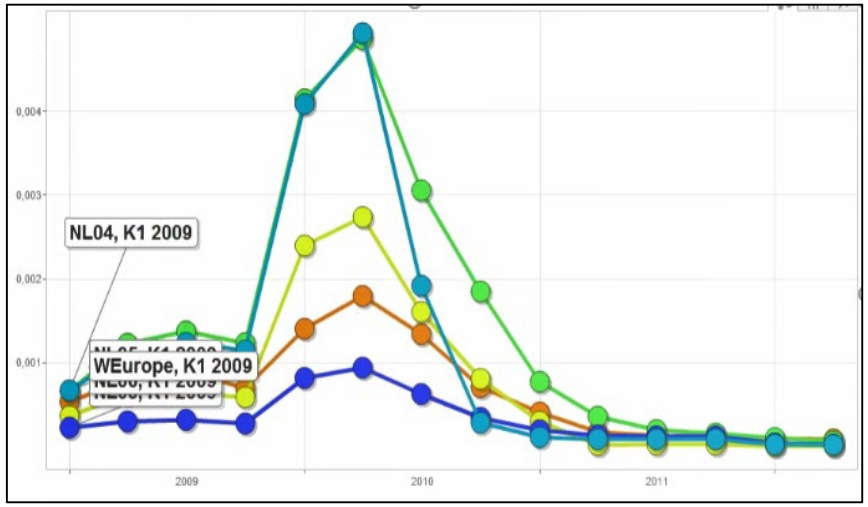
- More than half of all infected machines are located in only 50 large ISPs
  - These ISPs operate leading brands and are well known to regulators in their countries
  - Hence, not located in shady ISPs and countries with poor governance structures
- Hence, ISPs have discretion to enhance mitigation
- Their incentives are mainly cost of mitigation and pressure of regulatory involvement

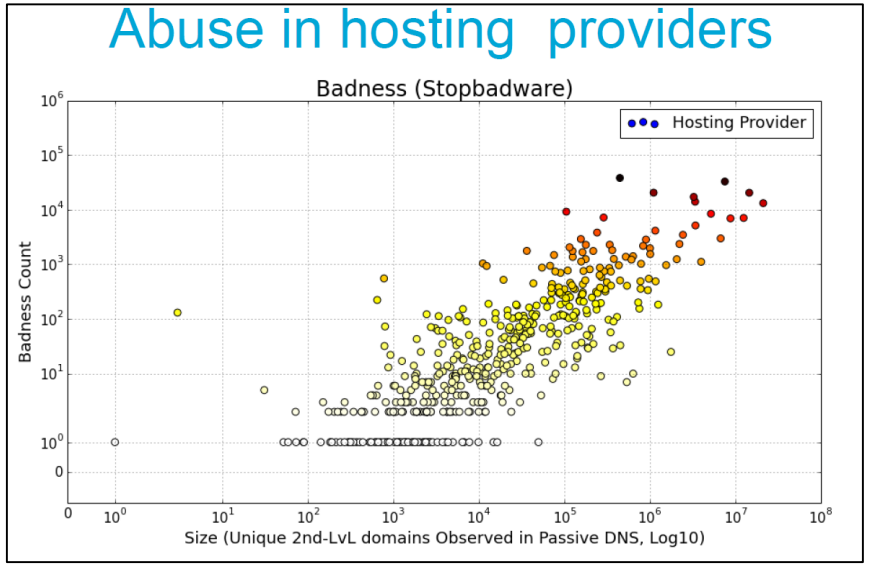


Source: Economics of fighting botnets: lessons from a decade of mitigation
H. Asghari, M.J.G. van Eeten, J.M. Bauer
IEEE Security & Privacy, September/October 2015, 16-23

Example: ISPs

- Big drop after reports (peer-pressure works with ISPs)
- Did not work with hosting providers





Source: Van Eeten et al.

Example: Internet of Things (IoT)

- Most IoT devices are cheap and are never patched
- Users often cannot update their devices
- Users don’t really care if their device is used in DDoS, since device is still working fine

- Misaligned incentives
  - Adding security does not increase profit of manufacturer
  - Users want cheap devices (market for lemons), don’t care about security
- Externalities
  - Other parties bear the costs

- Even worse than with smartphones

Example: Mirai botnet

- Malware family targeted at insecure IoT devices
  - Mainly IP cameras, DVRs, consumer routers
- Spreads like a worm
  - Scan and perform dictionary attacks on SSH and telnet
- Used for DDoS attacks
  - Reported total bandwidth of up to 1 Tbps

Example: Mirai botnet

- Dictionary of default passwords in Mirai source

Password	Device Type	Password	Device Type	Password	Device Type
123456	ACTi IP Camera	klv1234	HiSilicon IP Camera	1111	Xerox Printer
anko	ANKO Products DVR	jvbzd	HiSilicon IP Camera	Zte521	ZTE Router
pass	Axis IP Camera	admin	IPX-DDK Network Camera	1234	Unknown
888888	Dahua DVR	system	IQinVision Cameras	12345	Unknown
666666	Dahua DVR	meinsm	Mobotix Network Camera	admin1234	Unknown
vizxv	Dahua IP Camera	54321	Packet8 VOIP Phone	default	Unknown
7ujMko0vizxv	Dahua IP Camera	00000000	Panasonic Printer	fucker	Unknown
7ujMko0admin	Dahua IP Camera	realtek	RealTek Routers	guest	Unknown
666666	Dahua IP Camera	1111111	Samsung IP Camera	password	Unknown
dreambox	Dreambox TV Receiver	xmhdipc	Shenzhen Anran Camera	root	Unknown
juantech	Guangzhou Juan Optical	smcadmin	SMC Routers	service	Unknown
xc3511	H.264 Chinese DVR	ikwb	Toshiba Network Camera	support	Unknown
OxhlwSG8	HiSilicon IP Camera	ubnt	Ubiquiti AirOS Router	tech	Unknown
cat1029	HiSilicon IP Camera	supervisor	VideoIQ	user	Unknown
hi3518	HiSilicon IP Camera	<none>	Vivotek IP Camera	zlxx.	Unknown
klv123	HiSilicon IP Camera				

Source: Understanding the Mirai Botnet, Antonakakis et al., Proceedings 26th USENIX Security Symposium 2017, p. 1093-1110

Example: Mirai botnet

- Misalignment of incentives
  - Manufacturers want to maximise profit and are not affected by the malicious activity
  - Consumers want cheap devices and are not affected by the attacks their devices perform

- Regulation required to change the incentives
  - EU proposal for certification of IoT devices
  - US IoT Cybersecurity Improvement Act

Example: WPA Enterprise

- Security depends on users configuring their devices correctly

- Why would they do this?
  - It's cumbersome
  - It also works with insecure configuration

- Is all the extra effort worth it?
  - Costs of correct configuring lower than costs of a compromise?

Example: ransomware

- Rise of cryptocurrency-based payment systems caused increase in ransomware attacks
- Consumers can trade-off ex-ante security (patching) protection and ex-post (ransom) payments
- Ransomware directly impacts ransom-paying consumers
- Negative security externality indirectly impacts all unpatched users
  - option to pay ransom is incentive for consumers not to patch
  - also affects software vendors' pricing strategy
- Even worse: insurance against cyberattacks (ransom payment)
- Case study: ransomware at Maastricht University in 2019

Source: Economics of Ransomware Attacks
Terrence August, Duy Daoy, and Marius Florin Niculescu
Workshop on the Economics of Information Security (WEIS), 2019.

Further reading

Read the following papers (mandatory):

- Why information security is hard - an economic perspective
  Ross Anderson
  Proceedings 17th Annual Computer Security Applications Conference (ACSAC), 2001
- So long, and no thanks for the externalities: the rational rejection of security advice by users
  Cormac Herley
  Proceedings of the 2009 workshop on New security paradigms workshop (NSPW)

Further reading (optional)

- ‘Hacks, sticks and carrots’ by prof.dr. Michel van Eeten
  https://www.youtube.com/watch?v=ltTGi3p67kg&list=PLy3I89hClz6ZvKXDdI3tuL5-gvb2Zbadc&index=6
- Economics of fighting botnets: lessons from a decade of mitigation
  H. Asghari, M.J.G. van Eeten, J.M. Bauer
  IEEE Security & Privacy, September/October 2015, 16-23
- Cybersecurity: Stakeholder incentives, externalities, and policy options
  J.M.Bauer & M.J.G. van Eeten
  Telecommunications Policy 33(2009):706–719