

Security Economics and Psychology

SecAppDev

February 2014

Steven Murdoch

<http://www.cl.cam.ac.uk/users/sjm217/>

Based on slides by Richard Clayton



UNIVERSITY OF
CAMBRIDGE

Computer Laboratory

Outline

- Security economics
 - A powerful way of looking at overall system security
- Some examples
 - IT economics
 - Adverse selection in security seals
- Security psychology
 - How the brain works
 - Classic techniques used by scammers

Economics and Security

- Over the last eight years or so, we have started to apply an economic analysis to information security issues
- Economic analysis often addresses the underlying causes of security failures within a system, whereas a technical analysis will merely identify the mechanism!
- Tackling the problem in economic terms can lead to valuable insights as to how to create permanent fixes
- Clearly shows that consumers need access to better information so they can make informed decisions about security
- Meanwhile, the trend is for information security mechanisms (such as cryptographic protocols) to be used to support business models rather than to manage risk

Traditional View of Information Security

- People used to think that the reason that the Internet was insecure because of lack of features or that there was not enough crypto / authentication / filtering
- If only people had a proper checklist of security issues to tackle then we would all be more secure
- So engineers worked on providing better, cheaper, (and even occasionally easy-to-use) security features – developing secure building blocks such as SHA-1, AES, PKI, firewalls...
- About 1999, we started to realize that this is not enough

Using Economics to Explain Security

- Electronic banking: UK banks were less liable for fraud than US banks, so they got careless and ended up suffering more fraud and error. The economists call this a “moral hazard”
- Distributed denial of service: viruses no longer attack the infected machine but they use it to attack others. Why should customers spend \$20 on anti-virus software when it isn't their data that is trashed? Economists call this an “externality”
- Health records: hospitals, not patients, buy IT systems, so they protect the hospitals' interests rather than patient privacy. These are “incentive” and “liability” failures

and

- Why is Microsoft software so insecure, despite its market dominance? The economists can explain this as well!

New Uses of Security Mechanisms

- Xerox started using authentication in ink cartridges to tie them to the printer
 - followed by HP, Lexmark. . . and Lexmark's case against SCC
 - note that the profit is in the consumables – purchasers compare ticket price rather than total cost of ownership
- Accessory control now spreading to more and more industries
 - games, mobile phones, cars...
- Digital rights management (TPMs): Apple grabs control of music downloads, Microsoft accused of trying to control distribution of HD video content...
- Cryptography is being used to tackle the obvious contradiction between the decentralization of network intelligence and the operators desire to retain control

The New View of Information Security

- Systems are commonly insecure because the people who could fix them have a limited incentive to do so
 - bank customers suffer when poorly-designed bank systems make fraud and phishing easier
 - patients suffer when hospital systems put administrators' convenience before patient privacy
 - casino websites suffer when infected PCs attack them
- In these scenarios security has become what economists call an “externality” – just like environmental pollution
- This can sometimes be fixed by “the market” but will often require regulatory (Government) intervention

IT Economics

- Economic “rules” for the IT industry are different
- Network effects
 - value of a network grows super-linearly to its size (Metcalfe’s Law says n^2 , Briscoe/Odlyzko/Tilly suggest $n \log n$)
 - this drives monopolies, and is why we have just one Internet
- High fixed and low marginal costs
 - competition drives price down to marginal costs of production; but in IT industries this is usually (near as makes no difference) zero
 - hence copyright, patents &c needed to recover capital investment
- Switching costs determine value
 - switching from an IT product or service is usually expensive
 - Shapiro-Varian theorem: net present value of a software company is the total switching costs
 - once you have 1000 songs on your iPod, you're locked into iPods

IT Economics and Security I

- The high fixed and low marginal costs, the network effects and switching costs are all powerful drivers towards dominant-firm markets with a big “first-mover” advantage
- Hence the “time-to-market” is critical
- Paying attention to security rarely assists scheduling
- Thus the Microsoft philosophy of “we’ll ship it Tuesday and get it right by version 3” is not perverse behaviour by Bill Gates or a moral failing, but absolutely rational behaviour
- If Microsoft had not acted this way, then almost any other company which took the same approach would now be the dominant player in the PC operating system business (and/or in the office productivity tools business)

IT Economics and Security II

- When building a network monopoly, it is critical to appeal to the vendors of complementary products
 - remember the old mantra of “find the software product then ask which machine and operating system to buy”...
 - ... Microsoft spent huge amounts assisting developers
 - can see the same pattern with PC v Apple; Symbian v WinCE, WMP v RealPlayer, not to mention the console games market
- The lack of security in earlier versions of Windows made it significantly easier to develop applications
- It's also easy for vendors to choose security technologies that dump support costs onto the users (SSL, PKI, . . .)
- SSH succeeded because the switching cost was low (Telnet++) and there's benefit to early adopters; S-BGP, DNSSEC struggle

Key Problem of the Information Society

- More and more goods contain software so more and more industries are starting to become like the software industry
- The Good
 - flexibility, rapid response
- The Bad
 - Complexity, frustration, bugs
- The Ugly
 - attacks, frauds, monopolies
- How will regulation evolve to cope with this?

Adverse Selection in Security Software

- George Akerlof's "market for lemons" [Nobel Prize 2001]
 - considered the trade in second-hand cars as a metaphor for a market with asymmetric information
 - buyers cannot determine car quality, so they are unwilling to pay a premium for a quality car
 - sellers know this, so market is flooded with low-quality goods
- Software market is a market for lemons (Anderson 2001)
 - vendors may believe their software is secure, but buyers have no reason to accept that this is correct
 - so buyers refuse to pay a premium for secure software, and vendors refuse to devote resources to make it secure
- How can we reduce this asymmetry of information?

Markets for Vulnerabilities

- Need a way to easily measure a system's security
- One possible approach: establish a market price for an undiscovered vulnerability (Schechter 2002)
 - reward software testers (hackers) for identifying new vulnerability
 - products with higher outstanding rewards are more secure
- Not simply academic fantasy
 - iDefense, Tipping Point have created quasi-markets for vulnerabilities (& now WabiSabiLabi has an auction site)
 - however, their business models have been shown to be socially sub-optimal (e.g., they provide disclosure information only to subscribers and they have an incentive to disclose vulnerabilities to harm non-subscribers)
 - unfortunately, no public information (at present) on pricing

Economics is not a “Silver Bullet”

- Many of the most pressing information security issues today are not solely programming errors (e.g., spam, phishing, malware)
 - bad code is a factor, but bad designs more significant
 - incentives matter here as well – JavaScript isn’t really optional
- Users are bad at differentiating between legitimate and illegitimate websites (asymmetric information again)
- Companies have attempted to self-regulate by using third-party trusted certification seals (e.g., TRUSTe)
- Recent research has shown that these signalling devices are worse than ineffective; in fact, “untrustworthy” companies are more likely to hold a certificate!

Adverse Selection in Seals and Adverts

- Ben Edelman (WEIS 2006) used data from SiteAdvisor to identify “bad” sites distributing spam and malware
 - 2.5% of all sites were found to be “bad”
- But “bad” companies are more likely to be TRUSTe-certified:
 - 5.4% of TRUSTe-certified sites are “bad”
 - However, sites with the BBBOnline seal are slightly more trustworthy than random sites (but their process is very slow and there were only 631 certificates issued)
- Similarly, untrustworthy sites are over-represented in paid advertisement links compared to the organic search results
 - 2 to 3% of organic results are “bad” (0% for top hit at Yahoo!)
 - 5 to 8% of advertising links are “bad”

Tackling Adverse Selection by Regulation

- When the market fails you regulate!
- Options:
 - require certification authorities and search engines to devote more resources to policing content
 - assign liability to certification entities if certifications are granted without proper vetting
 - alternatively, regulate enforcement actions by requiring complaints to be published
 - search engine operators could be required to exercise “reasonable diligence” before agreeing to accept an advertisement
- But so far, we’re just tolerating/ignoring the problem

Economic Barriers to Security

All the stuff I've been talking about so far:

- Information asymmetries
- Externalities
- Liability dumping
- Lack of diversity in platforms and networks
- Fragmentation of legislation and law enforcement

Options for Overcoming Externalities

- #1 Self-regulation, reputation etc (hasn't worked so far)
- #2 Tax on "digital pollution" (likely to be vehemently opposed)
- #3 Cap-and-trade system (dirty ISPs would purchase "emission permits" from clean ones)
- #4 Joint legal liability of ISP with user
- #5 Fixed-penalty scheme (cf EU rules on overbooked aircraft)
- It's controversial! but what should be done instead?

Liability Misallocation

- Software vendors (and many service firms) disclaim all possible liability using contract terms
- There have been many calls for this to change, e.g. UK House of Lords suggested negligence should be punished
- Clearly not a policy that can be adopted in a single member state, and perhaps not even on a regional basis
- Of course governments should not interfere in business contracts without good reason! Nevertheless intervention may be necessary to deal with market failures such as monopolies, and for ensuring consumer protection
 - consider example of using a GPS navigator and getting stuck on a country lane: is the map or the routing algorithm at fault? Is what has failed a product or a service? Is it a consumer or a business?

Liability & Politics

- Tackling the “culture of impunity” in software is going to be absolutely essential as civilization comes to depend ever more upon software
- But it’s too hard to do in one go! So need a long-term vision
- Suggested strategy:
 - leave standalone embedded systems to safety legislation, product liability and consumer regulation
 - with networked systems, start by preventing harm to others
 - relentlessly reallocate slices of liability to promote best practice
- Need to robustly tackle the “open source” issues. Why should giving it away “for free” justify negligence or carelessness about security? Might a role develop for bundlers (Red Hat) and consortiums (Apache Foundation) to stand behind individuals?

Vendor Liability Options

- #1 EU Directive that ensures that liability for defects can't be dumped by contract
- #2 Statutory right to sue vendors for damages. If ISPs are liable for "bad traffic" (see earlier recommendation) then can ensure they can recover charges and costs
- #3 Do nothing and rely on market pressure (make it a big deal that Sun and HP patch slower than Microsoft and Red Hat)
- #4 Insist upon "safety by default"
you can't sell a car without a seatbelt, so why should you be allowed to sell an O/S without patching service?

Consumer Liability Issues

- Network insecurity causes privacy failures and service failures but the main effect on consumers is financial
- There is wide variation in the handling of customer complaints of fraudulent eBanking transactions (UK, DE the worst)
- eCommerce depends on financial intermediaries managing risk, but individual banks will try to externalize this
- The Payment Services Directive fudged the issue – and so this needs to be revisited

Article 59: *“Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider shall in itself not **necessarily** be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under Article 56.”* (my emphasis)

Attack and Defence (Conflict Theory)

- Weakest Link
 - Anarchia: flood defences run by individual families
- Best effort
 - Missile defence depends on best shot
- Sum of efforts
 - Total contribution
- The last is optimal; the first is really awful
- Software is a mix: it depends on the worst effort of the least careful programmer, the best effort of the security architect, and the sum of efforts of the testers
- Moral: hire fewer better programmers, more testers, top architects

Security Psychology (Anderson/Schneier)

- Traditional Economics makes assumption of the “rational actor” who impartially weighs up expected benefits of all options and selects the optimum
- Real people, companies, governments are far from this predictable
- Psychology (behavioral economics) tries to build more realistic modes of human behavior
- There are direct applications to security
- Criminals have been doing this for some time!

Social Engineering/Pretexting

- Highly effective technique
- Not often measured in organizations (in contrast to IDS alerts)
 - 1996 experiment: 30 calls per week to a health-authority
 - Result: stop trial
- More likely to be combined with technical attacks
- Kevin Mitnick used pretexting as his main attack technique
 - Standard approach: employee asking for help
- Hit the news with HP private investigator hired to investigate board members

People want to be helpful



Phishing

- Simple approach: ask for password
 - Stupid attacks work for enough people to be viable
 - Clever attacks are indistinguishable from bank marketing
- 2FA and transaction authentication require more sophistication
 - Give reasons for changing usual security measures
 - Why must customer enter details into their device
- Malware makes this easier
 - Still have to get it onto the PC by social engineering or exploiting a vulnerability

Brains vs Computers

- Capture errors
 - Easy to perform often repeated tasks without thinking
 - Users trained to click OK to get their work done
- Post completion errors
 - After the job is done, errors are more likely to occur
 - This is why well-designed ATM gets user to take card first
- Following wrong rules
 - When there are multiple rules to follow, the strongest one wins
 - Looking for bank name is stronger than parsing a URL
 - <http://paypal.secureauthentication.com/>
- Wrong cognitive model
 - What does the padlock mean in a browser?

Perceptual Bias

- Risk aversion vs risk loving
 - Many people dislike losing \$100 more than they value winning \$100
 - Backed up by fMRI scans: different bits of brain light up
- Availability heuristic
 - Base decisions on easily remembered analogies
 - 9/11 TV coverage
- Worry too much about unlikely events and those where are are not in control
- Behavior designed for small social groups with reasonable reputation mechanisms
 - Do not scale to largely anonymous markets

“If only gay sex caused global warming”

- Article by Daniel Gilbert
- Why we are more afraid of terrorism than climate change
 - More wary of hostile intent
 - Global warming doesn't violate moral sensibilities
 - Long-term threat rather than present danger
 - Involves slow change

Satisficing

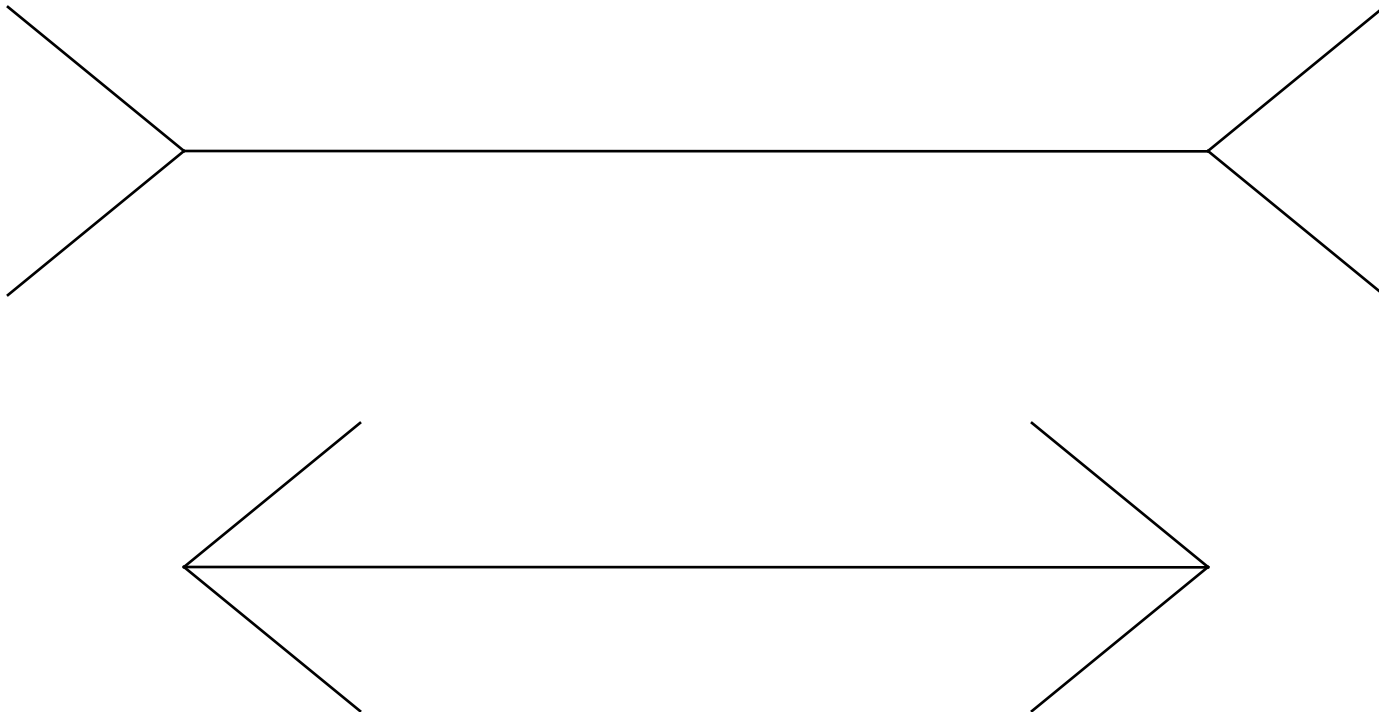
- Rather than think fully about difficult situations to find the optimum, choose something easy and acceptable
- One reason so many people stick to default system configurations
- Safe defaults also work because emotion is sometimes used when reason fails
- Natural tendency to explain things by intent rather than situation

Everyone is different

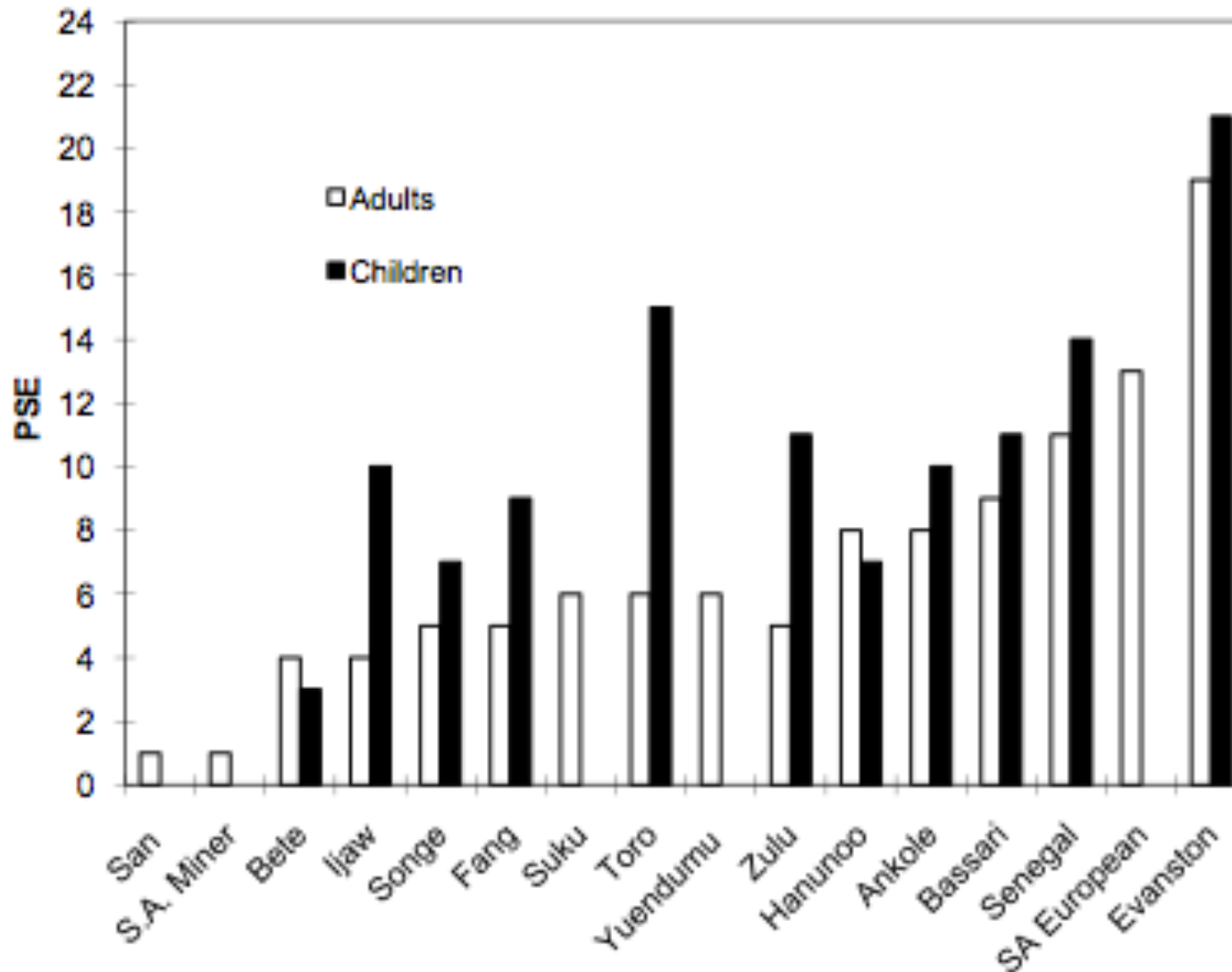
- Everyone is unique, but there are tendencies which are gender specific
 - Women use peripheral vision more than men
 - Larger displays reduce gender bias
- Very little research in this area, but it has far reaching effects in terms of both computing and law
- Studies generally done on “WEIRD” subjects (Henrich et. al.)
 - White
 - Educated
 - Industrialized
 - Rich
 - Democratic
- Least representative of average population

Mueller-Lyer Illusion

- Which is longer?



WEIRD (one of many examples)



Social psychology

- People will tend to agree with the majority
 - Only 29% of experimental participants disagreed with an obviously wrong statement about the length of a line
- Milgram and Zimbardo experiments
 - 60% of people will follow immoral orders
 - Experiment halted after six days on ethical grounds
- “Officer Scott” asked for beatings and sexual assault of “suspect”
 - At least 13 complied
 - McDonalds was held liable and had to pay compensation to detained staff member and her manager
- People are more likely to continue rather than accept they have been duped

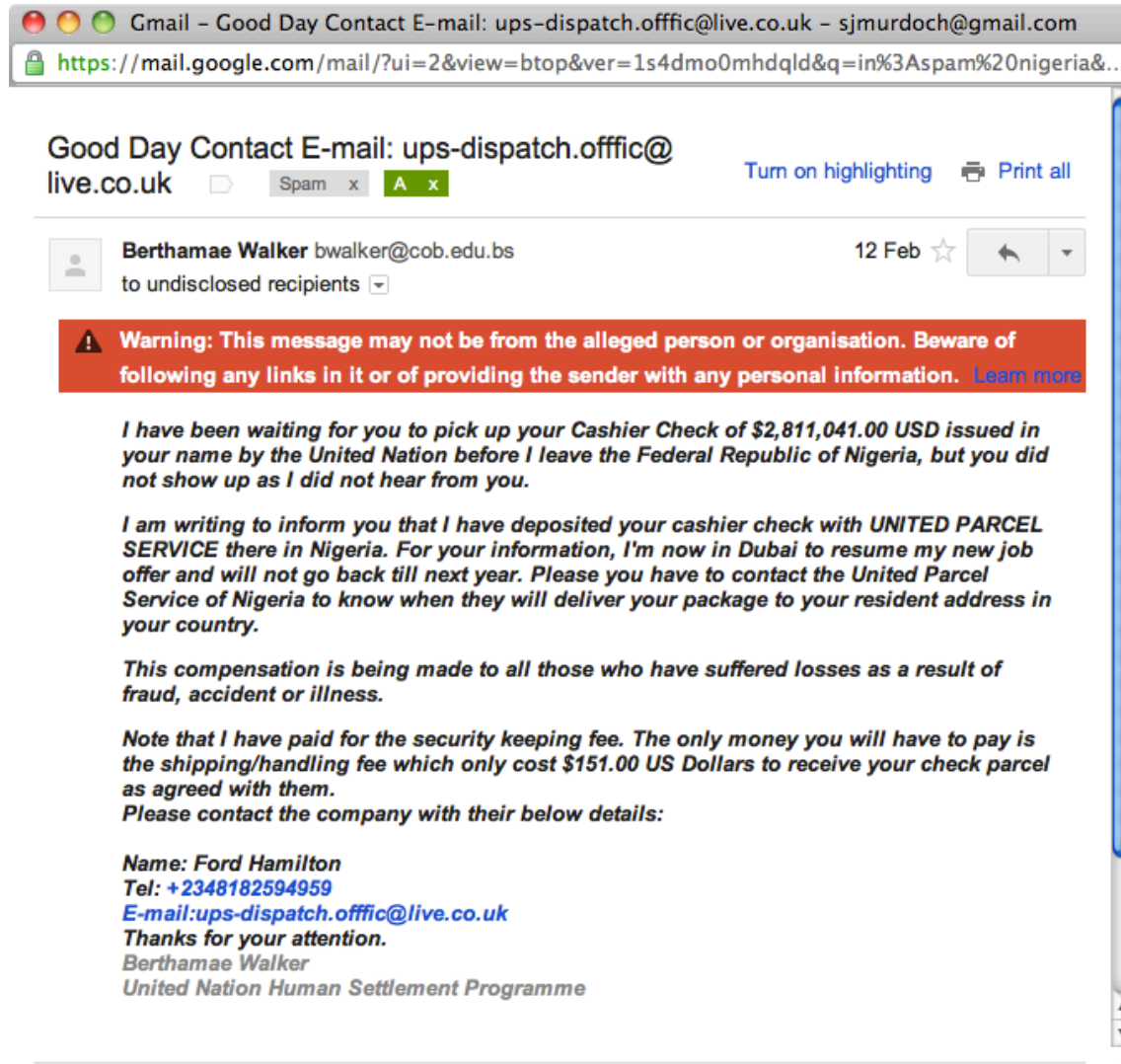
Principles of scammers (Stajano/Wilson)

- Distraction principle. While you are distracted by what retains your interest, hustlers can do anything to you and you won't notice.
 - Monte: crowd distracts the mark
- Social Compliance principle. Society trains people not to question authority. Hustlers exploit this “suspension of suspiciousness” to make you do what they want.
 - Counterfeit-pen scam: scammer impersonates a police officer

Principles of scammers (Stajano/Wilson)

- Herd principle. Even suspicious marks will let their guard down when everyone next to them appears to share the same risks.
Safety in numbers?
 - Cash machine con: people consider the ATM safe because others are using it
- Dishonesty principle. Your larceny is what hooks you initially. Thereafter, anything illegal you do will be used against you by the fraudster.
 - Lottery scam: mark participates in scam to defraud lottery-winning illegal immigrant

Who is the scammer



The screenshot shows a Gmail interface with the following elements:

- Browser Tab:** Gmail - Good Day Contact E-mail: ups-dispatch.offfic@live.co.uk - sjmurdoch@gmail.com
- Address Bar:** <https://mail.google.com/mail/?ui=2&view=bt&ver=1s4dmo0mhdqld&q=in%3AAspam%20nigeria&...>
- Sender:** Good Day Contact E-mail: ups-dispatch.offfic@live.co.uk
- Actions:** Turn on highlighting, Print all
- Recipient:** Berthamae Walker bwalker@cob.edu.bs
- Date:** 12 Feb
- Warning:** Warning: This message may not be from the alleged person or organisation. Beware of following any links in it or of providing the sender with any personal information. [Learn more](#)
- Body Text:**

I have been waiting for you to pick up your Cashier Check of \$2,811,041.00 USD issued in your name by the United Nation before I leave the Federal Republic of Nigeria, but you did not show up as I did not hear from you.

I am writing to inform you that I have deposited your cashier check with UNITED PARCEL SERVICE there in Nigeria. For your information, I'm now in Dubai to resume my new job offer and will not go back till next year. Please you have to contact the United Parcel Service of Nigeria to know when they will deliver your package to your resident address in your country.

This compensation is being made to all those who have suffered losses as a result of fraud, accident or illness.

Note that I have paid for the security keeping fee. The only money you will have to pay is the shipping/handling fee which only cost \$151.00 US Dollars to receive your check parcel as agreed with them.

Please contact the company with their below details:

Name: Ford Hamilton
Tel: +2348182594959
E-mail: ups-dispatch.offfic@live.co.uk
Thanks for your attention.
Berthamae Walker
United Nation Human Settlement Programme

Principles of scammers (Stajano/Wilson)

- Deception principle. Things and people are not what they seem. Hustlers know how to manipulate you to make you believe that they are.
 - Valet steal: impersonate a hotel guest , steal the car
- Need and Greed principle. Your needs and desires make you vulnerable. Once hustlers know what you really want, they can easily manipulate you.
 - Gadget scam: recharges Oyster cards (but really sleight of hand)
- Time principle. When you are under time pressure to make an important choice, you use a different decision strategy. Hustlers steer you towards one involving less reasoning.
 - Ring reward: mark tries to profit, but isn't given time to think

Conclusions

- Amateurs study cryptography; professionals study economics (and psychology)
- Economics can explain information security failures
- Economics is also frequently the goal of information security
- Its predictive power is however limited by unrealistic assumptions
- Psychology can explain many “irrational” behaviors
- Criminals and marketers are already expert in exploiting these
- Academic study is still continuing but is making good progress

More..

ENISA Report (and comments)

[http://www.enisa.europa.eu/pages/
analys_barr_incent_for_nis_20080306.htm](http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm)

Economics and Security Resource Page

<http://www.cl.cam.ac.uk/~rja14/econsec.html>

Security Psychology Resource Page

<http://www.cl.cam.ac.uk/~rja14/psysec.html>

Cambridge Security Group Blog

<http://www.lightbluetouchpaper.org>



UNIVERSITY OF
CAMBRIDGE
Computer Laboratory