

Security Research: bad news, good news.

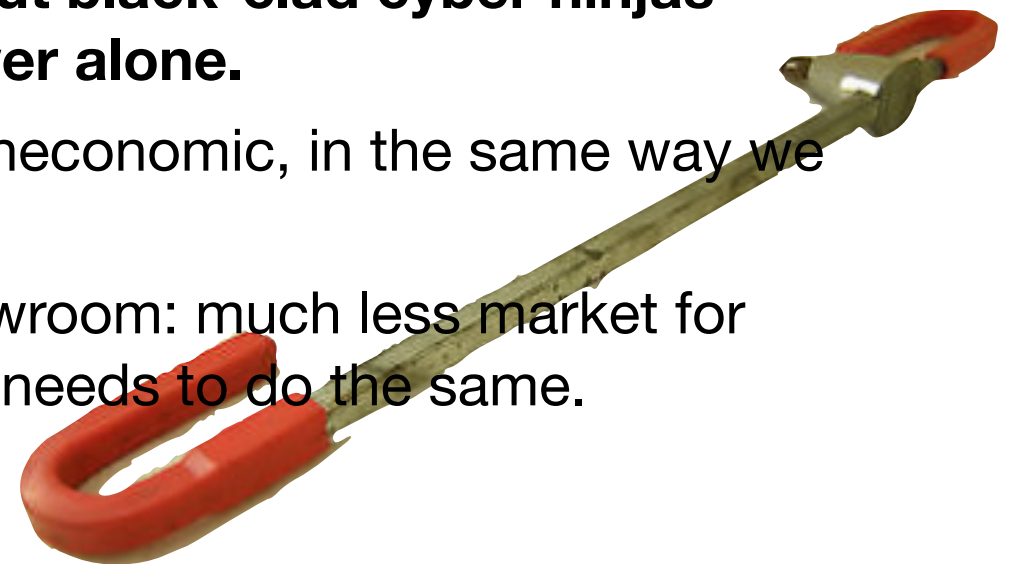
Dr Ian Batten, University of Birmingham
<https://igb.batten.eu.org/>

Who am I?

- Lecturer at University of Birmingham School of Computer Science
- Formerly (until 2010) Head of Information Assurance for a telecoms manufacturer, amongst other things in a 22-year industry career.
- Full time PhD 2010–2014, making my mid-life crisis longer and more expensive than most.
- I should have just bought a motorbike: I've got a full licence already.

My proposition

- Security in most enterprises **could be better**, and there are **genuine attacks being carried out** successfully by opponents of greater and (usually) lesser skill.
 - Probably not on the scale that is sometimes claimed
 - **Usually attackers exploiting either (a) poor internal controls, or (b) well-understood and easily patched vulnerabilities or (c) human gullibility.**
 - And the rest are mostly **old frauds made more powerful, or easier to do remotely, by new technology.**
 - The technological vulnerabilities are old, too: the Talk-Talk vulnerability was older than the hacker accused of exploiting it.
- We **tend to worry about the exotic and exciting**, when the threats are usually much more mundane. As the NCSC CTO says, **it's not about black-clad cyber ninjas who can break into your machines by thought power alone.**
- We can raise the bar to make the lower-skill attacks uneconomic, in the same way we can avoid leaving the keys in the ignition of our cars.
- Cars have become more secure straight from the showroom: much less market for Krookloks (although Flavio Garcia might disagree). IT needs to do the same.



Consider your office

- Is the front door of your office strong enough to keep out someone who doesn't have a key?
- Perhaps, but what about someone with a steel battering ram? A JCB*? A rifle-launched breaching grenade?
- Depends on capability of the adversaries you are dealing with.
- The difficulty for cybersecurity is making those assessments.
- “We” don't make that easy for you.



* Other earth-moving machinery is available

What you hear

- Every week, there are new announcements of failures in security systems
 - In the past year or so, “WiFi is broken”, “Smartcards are broken”, “All microprocessors are broken”.
- It’s important to remember that an attack which is interesting to security researchers may not be as serious as it sounds for end-users
 - Particularly if your knowledge comes via the general media.

For older readers, Y2K

- There were extensive problems in a lot of systems, mostly business-facing rather than safety critical caused by variations on the assumption you can represent years in two digits.
 - Safety-critical systems rarely care what year it is, and the real offender was a language called COBOL used in pre-1990s business applications which routinely stored dates as DDMMYY (PICTURE IS 9(6), and all that).
 - For even older Birmingham users, Multics wasn't Y2K compliant, and the project to resurrect it on emulators had to fix a load of bugs.
- A lot of us worked very hard to fix this.
 - I co-managed the replacement of a major corporate ERP system riddled with this, which would otherwise have failed to drive material purchase correctly from about 1998 onwards.
- But there was also crazy over-reaction in the media, and from the outside it appeared we were predicting the end of the world which then didn't happen, because the problem never existed. Now, Y2K is the go-to metaphor for a fuss about nothing.
- Media presentations of problems flip-flop between over-statement and dismissal. Facts are in short supply. Decision making suffers.

For the older attendees

```
Multics MR12.6e: Batten Multics (Channel d.h000)
Load = 5.0 out of 90.0 units: users = 5, 03/06/18 0244.0 pst Tue
l Batten
Password:
You are protected from preemption.
Batten.SysAdmin logged in 03/06/18 0244.1 pst Tue from ASCII terminal "none".
Last login 03/01/18 0559.0 pst Thu from ASCII terminal "none".
r >user_dir_dir>SysAdmin>Batten 02:44
date
03/06/18
r >user_dir_dir>SysAdmin>Batten 02:44
time
02:44
r >user_dir_dir>SysAdmin>Batten 02:44
who

Multics MR12.6e, load 6.0/90.0; 6 users, 1 interactive, 5 daemons.
Absentee users 0/3
Batten.SysAdmin

r >user_dir_dir>SysAdmin>Batten 02:44
```

What do security researchers want?

- For academic security researchers, vulnerabilities are vital. The vulnerability, its analysis and its countermeasures are each a paper at a conference; three papers plus an introduction and a conclusion makes a PhD you will have no problem getting awarded.
- It doesn't matter if the attack is impractical, uneconomic or of little practical importance, it may have other implications in the academic security research world.
- But the real-world impact may be very different.

What do criminals want?

- Most want money
- Some want fame for themselves or their “cause”
- Some want the admiration of their peers
- Some might be sociopaths who enjoy the damage
- **Very, very few think “I want a paper at CSF so that I can further my post-doctoral research career”.**
- A lot of attacks only make sense in that context.

For example

- There are a range of attacks against contactless payment schemes
- But these attacks are quite difficult to pull off, hard to monetise and require large amounts of equipment.
 - Equipment which would be hard to explain to the police or a jury as having a legitimate purpose, too.
- Which is why the initially-predicted volume of attacks on contactless payment just haven't happened: it's not worth the criminals' time, assuming their motive is money rather than citations for their new publication.
- As the limit on transactions is £30, the typical criminal is better off stealing razors from supermarkets.

Yes, Razors



5. GILLETTE MACH 4 Razor blades really cut it on the resale market, especially Gillette Mach 4s. That's because the replacement-blade packs retail for around \$23 dollars, and lots of whiskered men can't afford that right now. "Check the online auction sites, and

you'll see a tremendous number of people trying to sell razor blades," Custer says. Adds Read Hayes, director of the Loss Prevention Research Council: "In bad economic times, you'll see more basic items stolen." Shaving products account for over 2.7 percent of store inventory losses.

Each took an average of £105 of goods, according to the survey commissioned by Group 4 Securicor. Supermarkets are regarded as the easiest place for shoplifting by 21% of people, followed by garden and DIY centres.

But what do they take? **Top of the list are razor blades**, according to the research.

Law Abiding Criminals

- Few academic security researchers have criminal records. Doing a PhD is pretty much the definition of having been law-abiding for all of your life.
- They therefore do not compare the economics and risk-reward of their work with the economics of shop-lifting.
 - And by economics I include risk/return and opportunity cost.
- They do, however, often have a slightly odd “victim-blaming” attitude to computer crime, which is somehow different to housebreaking.
- I call this the “**law-abiding criminal**” fallacy: assuming we face opponents who are willing to break the Computer Misuse Act, but not steal razor blades from Aldi.

Petty Criminal with Citations

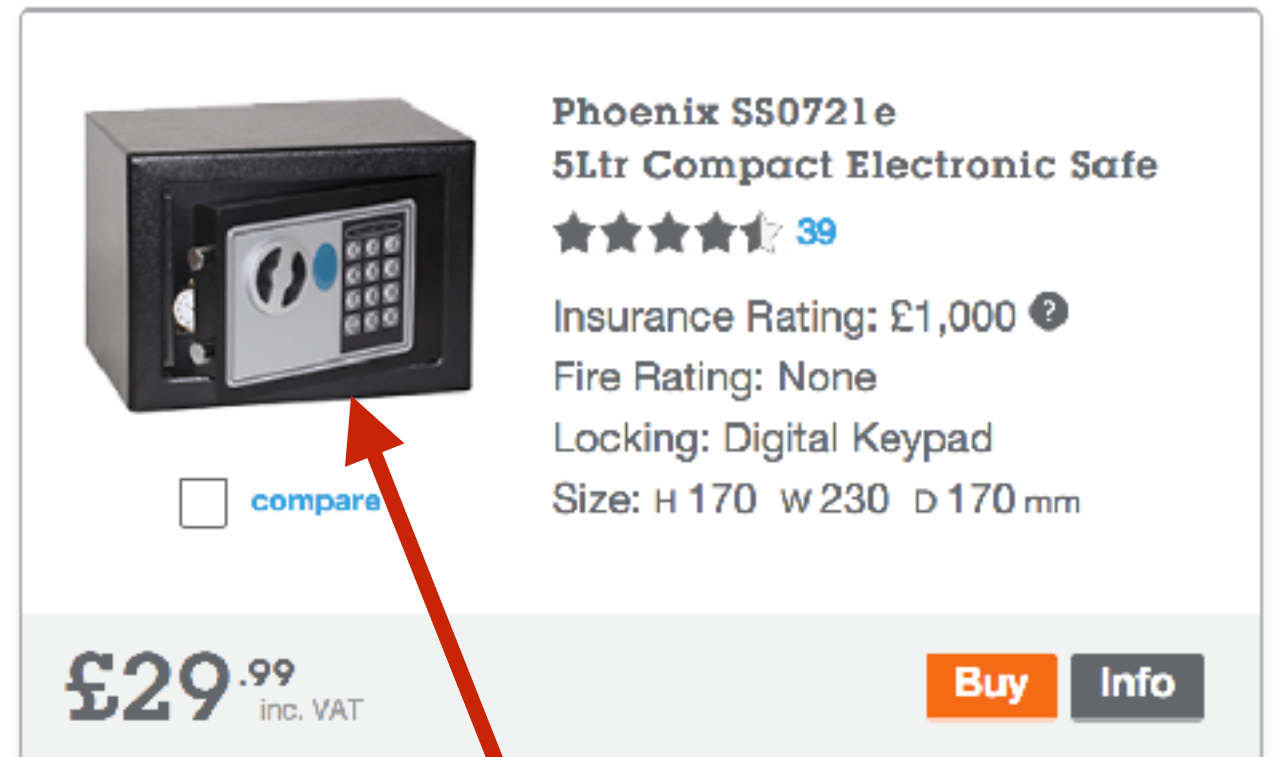
- Many of the conjectured attacks are time-consuming, require specialised equipment and have uncertain pay-offs, with quite a high associated risk of detection (in terms of the payout not being available, even if not criminal).
- But if your end goal is getting a paper at CSF, you don't care if the attack is economically viable: the paper is the pay-off, not any small monetary gain.
- This is the “**petty criminal who cares about their publication history**” fallacy: that you can make an uneconomic attack plausible by citation count.

Break at any cost

- If your PhD depends on a particular vulnerability, you will be willing to work at it until it's usable. Its practical value is somewhat irrelevant: your PhD is a long-term objective which justifies the work.
- However, criminals can just do other crimes in the same time to make more money.
- A vulnerability is competing with all other ways the criminal can make the same or more money.
- This is the “**Breaking computers at any cost**” fallacy: that attackers cannot choose between cyber-crime, indeed a particular form of cyber-crime against a particular target, and other opportunities.

Deterrence by difficulty

- It isn't hard to break into those little safes you get in hotels.
- They're thirty quid, including VAT, retail. What do you expect?
- But all they have to do is make stealing your passport slightly harder, noisier and risky than some other crime.
- They are not proof against Robert de Niro as the uber-criminal in *Heat*, nor are they intended to be.
- But they raise the bar against light-fingered hotel staff.



Phoenix SS0721e
5Ltr Compact Electronic Safe

★★★★☆ 39

Insurance Rating: £1,000 ?
Fire Rating: None
Locking: Digital Keypad
Size: H 170 W 230 D 170 mm

compare

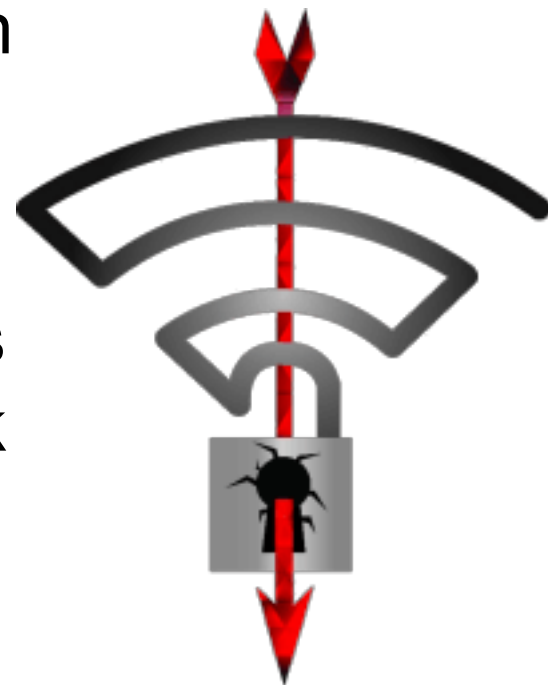
£29.⁹⁹ inc. VAT

Buy Info



Consider: “Krack” versus WPA2 Wireless Networks

- In passing, note the trend of newly uncovered vulnerabilities having a logo and a website before they’re even announced.
- Academically, a fascinating attack: it shows that it’s vital when doing security proofs to define exactly what security properties you are proving things about
 - In the case of Krack, it doesn’t reveal keys, and it often doesn’t permit full decryption.
 - The arrival of an attack on a “proven” protocol which is both a real attack **and** does not invalidate the proofs is quite scary, long-term. #GladMyVivalsNotNextWeek
- <https://www.krackattacks.com>



However...

- It's hard to see the real risks for moderately competent (not GCHQ, just “taking sensible precautions”) users.
- It requires an active attacker able to monitor and transmit radio frames within reach of the victim's machines, so it's about **targeted** attacks, and requires equipment within ~100m of the target.
- It does not provide any significant new means to attack https, or a VPN, and any other “end to end” encryption.
- Anyone with the means to launch the attack has better ways to achieve the same, or better, effect (“rogue AP”).
- You shouldn't be trusting wireless networks anyway, particularly not ones you don't control (“evil AP”).
- None of this nuance was present in media coverage.

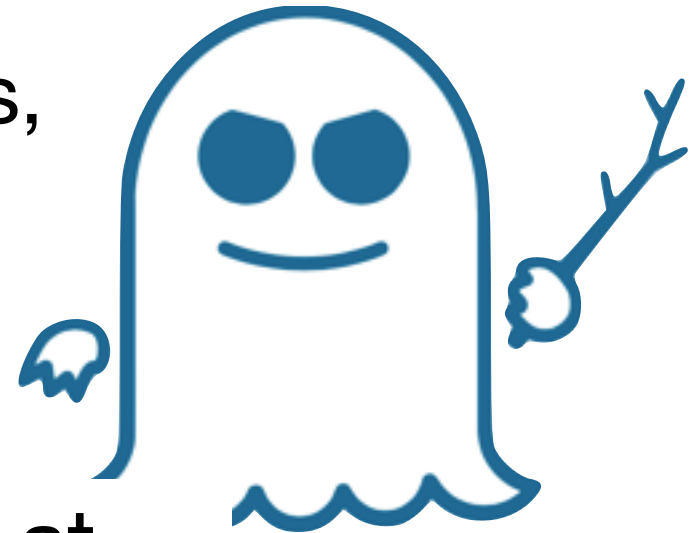
Similarly Smartcards

- Lost under the WPA2 attack that week was a potentially more worrying attack on Infineon smart cards and TPMs.
 - A TPM is a small device fitted to most enterprise servers and laptops which acts as a secure keystore, amongst other things.
- In essence when generating random prime numbers, they do so badly enough that a crucial question for an attacker (“which two 350 digit prime numbers were multiplied together to makes this 700 digit composite?”) moves from impossible to relatively easy (still needs tens of thousands of pounds’ worth of CPU, though).
- https://crocs.fi.muni.cz/public/papers/rsa_ccs17

Similarly Processors

- Meltdown and Spectre (again with the names, again with the logos) gained huge media attention, internationally. I ended up being translated into Vietnamese.

Ian Batten, a computer security specialist at the University of Birmingham (UK), said that the techniques used to speed up microprocessors are common to the industry. Therefore, repairs will lead to slower work rates, but reports indicate that system speeds are slower in the 25-30% range that occurs only in the worst case scenario.



Meltdown and Spectre

- In essence, if you can execute a program of your choice on a particular processor, you can exploit various optimisations in the micro-architecture of the CPU to discover information about other programs, or the operating system, which you otherwise should not be able to obtain.
 - *ie*, the micro-architecture doesn't behave quite the same as the instruction architecture it is implementing, and breaks some security assumptions.
 - Interesting example of how features combine to cause a problem, in this case out-of-order execution, speculative execution and caching.
 - Particularly bad against Intel x86 processors: somewhere in Palo Alto, the ex-Sun Sparc development team and some laid-off Solaris-on-Sparc developers are laughing through their tears.
- <https://meltdownattack.com>

Meltdown and Spectre

- But these attacks require a **very** strong attacker (one able to execute arbitrary code of their choice on your machine), and an attacker in that position is already formidable.
 - If you are in a position where someone can carry out these attacks, you have probably lost already.
 - Does have implications for multi-tenant virtualisation, but only under some quite limited circumstances.
- Would be devastating were this 1984 and universities had timeshare systems as their main computer resource, but it isn't and they don't.

Lessons?

- These attacks are serious, documented by serious people. They are definitely not trivial pieces of work. They are papers at a top conference, and with good cause.
- They have long-term implications both in their own terms, and for what they say about the way we analyse and verify systems.
- They probably (I stress **probably**) present very little **additional** risk to the typical enterprise. Your defences against existing attacks probably defend you against these new attacks.

Meanwhile, in the real world

- Real people are being taken for large amounts of money by “these are our bank details, send your payment here” email scams.
- Require insider knowledge, probably gained by phishing and other penetration.
- Not obvious who is liable, but (for example) the SRA is taking a close look at it for solicitors which may make it your problem.
 - And of course SME are often the victim, too.
- **£120 000** example this week: <https://goo.gl/31edKi>

High Tech?

- No. Probably carried out by phishing attack used to install enough software to interfere with sending of email. Similar frauds were being carried out by phone ten and more years ago.
- But devastating, nonetheless.

Defences

- In the precise case of these payment frauds, “out of band” confirmation of payment details.
 - When it’s my money, I confirm bank details over the phone.
 - The nature of the fraud means the “fake” email may be “genuine” in the sense of being sent from the real originators’ computer.
 - Why not put your bank details on your business card and hand it out when you first engage with a customer?
 - Why not print “we will never use email to send bank details or changes to payment arrangements” on your letterhead?
- But what can we do to deter low-tech / high-impact attacks whose details we don’t as yet know about?

Raising the bar for attackers

- Some controls require that we make full risk-assessments that are difficult to do, particularly for SME, because of the potential to do more harm to the business than good.
 - Capital cost
 - Revenue cost (training, time, inconvenience)
 - Opportunity cost (do other things with the money)
- But some stuff is just basic “make sure your car is taxed and tested” stuff we should all be doing.

Raising the bar for attackers

- **Password managers**
- **Two factor authentication**
- **HTTP encryption everywhere**
- **Disk encryption on everything**
- I'm assuming that "keep your software up to date" doesn't need saying, although the excuses people use for not patching are a shocking array of badness.
- I'm going to step away from "do I need a virus scanner?" as we don't have all day.

Conclusion

- Lots of noise from academic researchers, mostly looking technology rather than end-to-end systems, with priorities different to (from?) those of criminals.
- Amplified by media, who like a story with bliu
- Main risks are lower-tech, with counter-measures we can all put in place
- Fix the fundamentals to keep out the majority of attacks.