Some Security and Privacy issues in the 21st Century Internet

stephen.farrell@cs.tcd.ie

HEANET Conference

November 2016

Background

- Me: Trinity College Dublin, School of Computer Science and Statistics
  - Research topics: security/privacy/DTN;
  - IETF security area director (but not speaking for IETF)
  - Expecting wisdom? Vision? Apologies:-)
- These slides https://down.dsg.cs.tcd.ie/heanet/

TL;DR

The talk will describe some of the ways in which Internet security and privacy have evolved over the past couple of decades. In brief, we have seen and will review some improved deployment of security technologies but in an increasingly hostile environment, yet we also continue to see the same mistakes being made e.g. the absence of small-device software update. The conclusion can be optimistic or pessimistic, depending on one's point of view. However, it is clear that Internet security and privacy issues will continue to create employment opportunities for defenders and attackers.

Summary

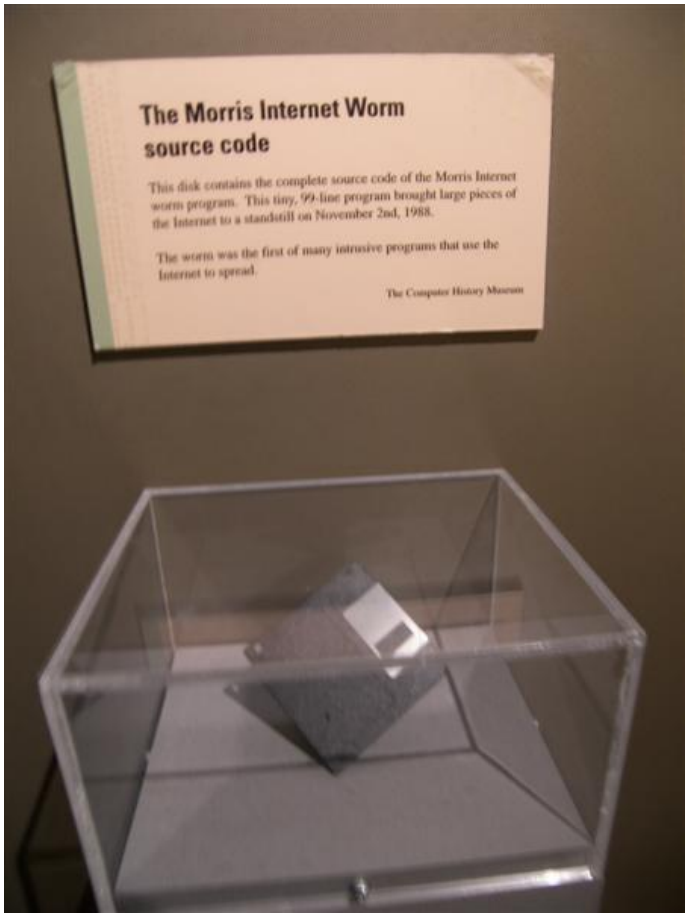
- Same mistakes get made over and over
- But we are finally starting to gain real experience in deploying deployable security technologies
- Same mistakes get made over and over
- Privacy is the real next challenge
- Same mistakes get made over and over
- But there are things you can do to help...

Let's start in the 19th Century

- A little before the Internet but…wires were tapped
  - http://bugsweeps.com/info/wiretap_short_history.html
  - http://www.counterpunch.org/2013/08/09/a-social-history-of-wiretaps-2/
- Basic law enforcement requirement:
  - Everything needs to be tappable
- Same as current lawful intercept
  - Not clearly a great plan

1988 – Morris worm

- First widespread worm in the wild
- Partitioned the Internet for days
- Sendmail debug mode, fingerd buffer overrun, password guessing
  - Password guessing CPU consuption caused the DoS
- Worth reading the initial report as it describes things from first principles
  - http://spaf.cerias.purdue.edu/tech-reps/823.pdf



https://en.wikipedia.org/wiki/File:Morris_Worm.jpg

1993-2016 Name fun: digital.com

- Owned by: DEC, Compaq, HP, and now “Quality Nonsense Ltd.” of London, UK
  - http://www.digital.com/
  - http://betanews.com/2015/03/17/30-years-of-dotcom-what-became-of-the-first-100-domains/
- Of 1st 100 .com domains:
  - 52% still same
  - 24% dead
  - 18% redirect new company
  - 6% redirect same company

https://en.wikipedia.org/wiki/File:Digital_556-flattened4.svg

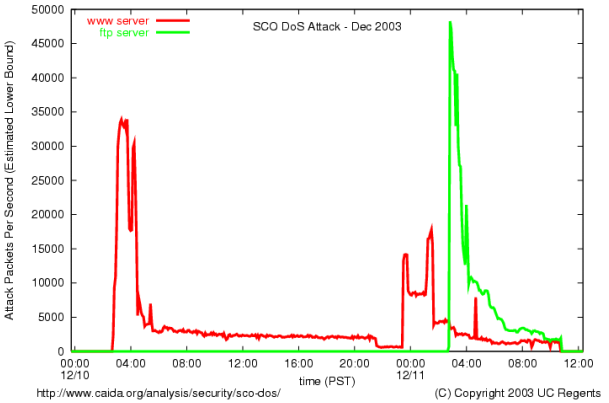
- One might speculate that in the long term only less than 50% of names will remain “good”

1999, 2016 – Crypto product survey

- Surveys done in 1999 and 2016 identifying cryptographic products (incl. OSS) available worldwide
  - Fewer in 2016, 546 vs. 805 “foreign,” but crypto is now a mainstream feature more than a product category
- Not clear surveys are commensurate, except for the intended affect on US policy related to cryptography
  - Any such laws are ultimately not a problem as mathematics is not nationalist!
  - They can be a PITA though
- https://cryptome.org/cpi-survey.htm
- https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf

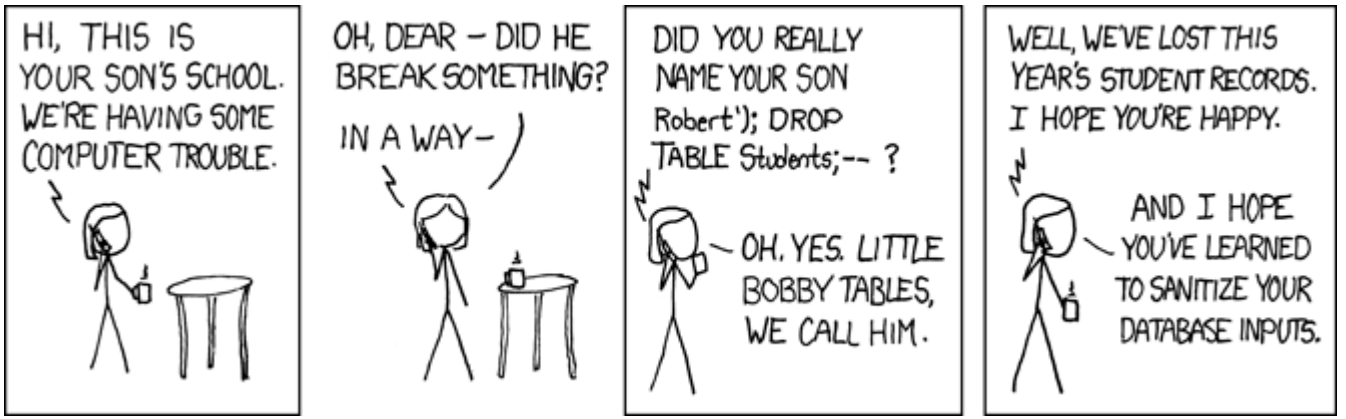
2003-2016 – DDoS Galore

- 2003: SCO case...
  - https://news.netcraft.com/archives/2003/12/10/ddos_takes_sco_site_down.html
  - Web site “down for 3 days” after ~64Mb/s (50,000 packets/s) SYN flooding
  - Our sympathies are where?
- 2016: Brian Krebs case…
  - https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/#more-36426
  - Journalist attacked by subject of article (who is in the business of DDoSing folks:-)
  - 620Gb/s attack, reportedly later 1Tb/s vs. Dyn
  - Botnet of crap devices, not a reflection attack



2003, 2013 – SQL Injection

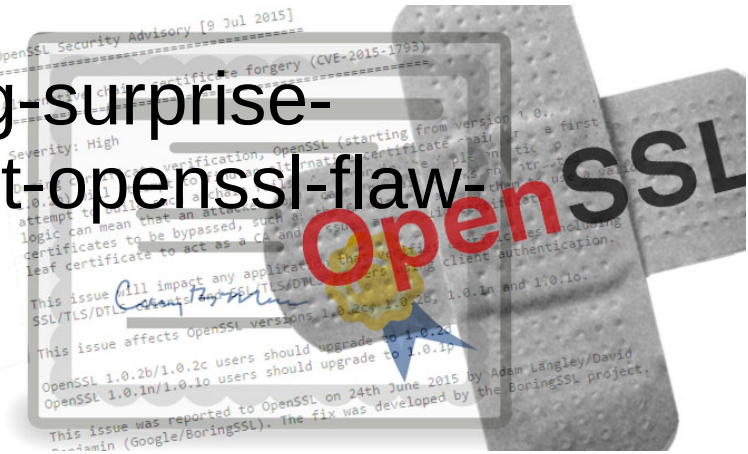
- US FTC threatens web site (petco.com) with sanctions for leaking 500,000 user credit card details
  - https://news.netcraft.com/archives/2003/12/10/us_regulators_probe_security_lapses_at_retailers.html
  - https://www.petco.com Still re-directs to http://www.petco.com so I guess they learned a lot from that, they do use Akamai so at least have IPv6 though:-)
- 2013: OWASP top-10? Still there @ #1!



https://www.xkcd.com/327/

2003,2016 – openssl vulns/updates

- 2003: Various CVEs (bugs) in openssl reported, openssl updated, 50k web sites still using vulnerable old versions ~1 year after CVE
  - https://news.netcraft.com/archives/2003/11/03/vulnerable_versions_of_openssl_apparently_still_widely_deployed_on_commerce_sites.html
- Same old, same old in 2016
  - http://news.softpedia.com/news/big-surprise-companies-are-slow-to-patch-latest-openssl-flaw-504579.shtml



https://threatpost.com/openssl-fixes-critical-bug-introduced-by-latest-update/120851/

2003 – Weird CA Business Model

- A hoster offering “cheap” US$25/yr certs as a way to attract the kind of web site that uses SSL
  - https://news.netcraft.com/archives/2003/09/09/do_ssl_certificate_authorities_still_have_a_margin_generating_business_model.html
- The CA business model was always weird and still is
- Things like LetsEncrypt (2015) and acme do however look promising

https://letsencrypt.org/

2003 – SSO around the corner (still)

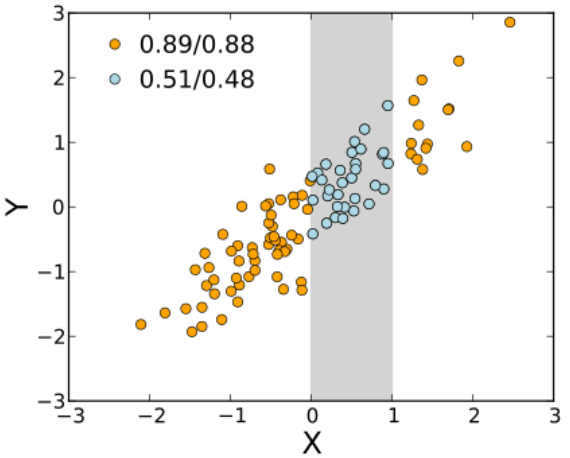
- Large consortium of vendors establish a single-sign-on system and start to deploy that
  - https://news.netcraft.com/archives/2003/01/22/liberty_alliance_identity_server_launched.html
- This still happens, (Fido) there'll always be another fashionable "federated" thing, maybe someday one will work out as planned
- To be fair, some stuff works: Eduroam, login based on ${megacompany} credentials (FB, Google etc

https://web.archive.org/web/19980529171444/http://www.sse.ie/prodserv.html

2007 - Netflix Competition

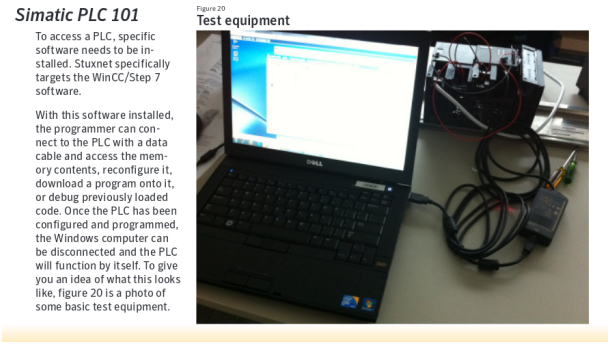
- Anonymised data sets published to allow researchers to improve delivery algorithms
- Correlation of review times with IMDB allow identification (with some embarrassment)
  - https://en.wikipedia.org/wiki/Netflix_prize#Privacy_concerns
  - https://arxiv.org/abs/cs/0610105
- Fine example of unexpected nature of some privacy issues. Many privacy issues however are utterly predictable if one spends a very short amount of time thinking about the topic.

https://en.wikipedia.org/wiki/File:Correlation_range_dependence.svg



2010-ish - Stuxnet

- Targeted controllers for (off-line) Iranian centrifuges involved in Uranium purification, so had to span air-gap
  - https://en.wikipedia.org/wiki/Stuxnet
  - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
- Interesting part of Stuxnet is that the US essentially admitted it! That's pretty stupid really but also set an awful precedent for which we'll continue to pay for some time to come
- Malware attribution is almost never believable, even genetic linkage could/should be faked by those skilled in the art



Simatic PLC 101

To access a PLC, specific software needs to be installed. Stuxnet specifically targets the WinCC/Step 7 software.

With this software installed, the programmer can connect to the PLC with a data cable and access the memory contents, reconfigure it, download a program onto it, or debug previously loaded code. Once the PLC has been configured and programmed, the Windows computer can be disconnected and the PLC will function by itself. To give you an idea of what this looks like, figure 20 is a photo of some basic test equipment.

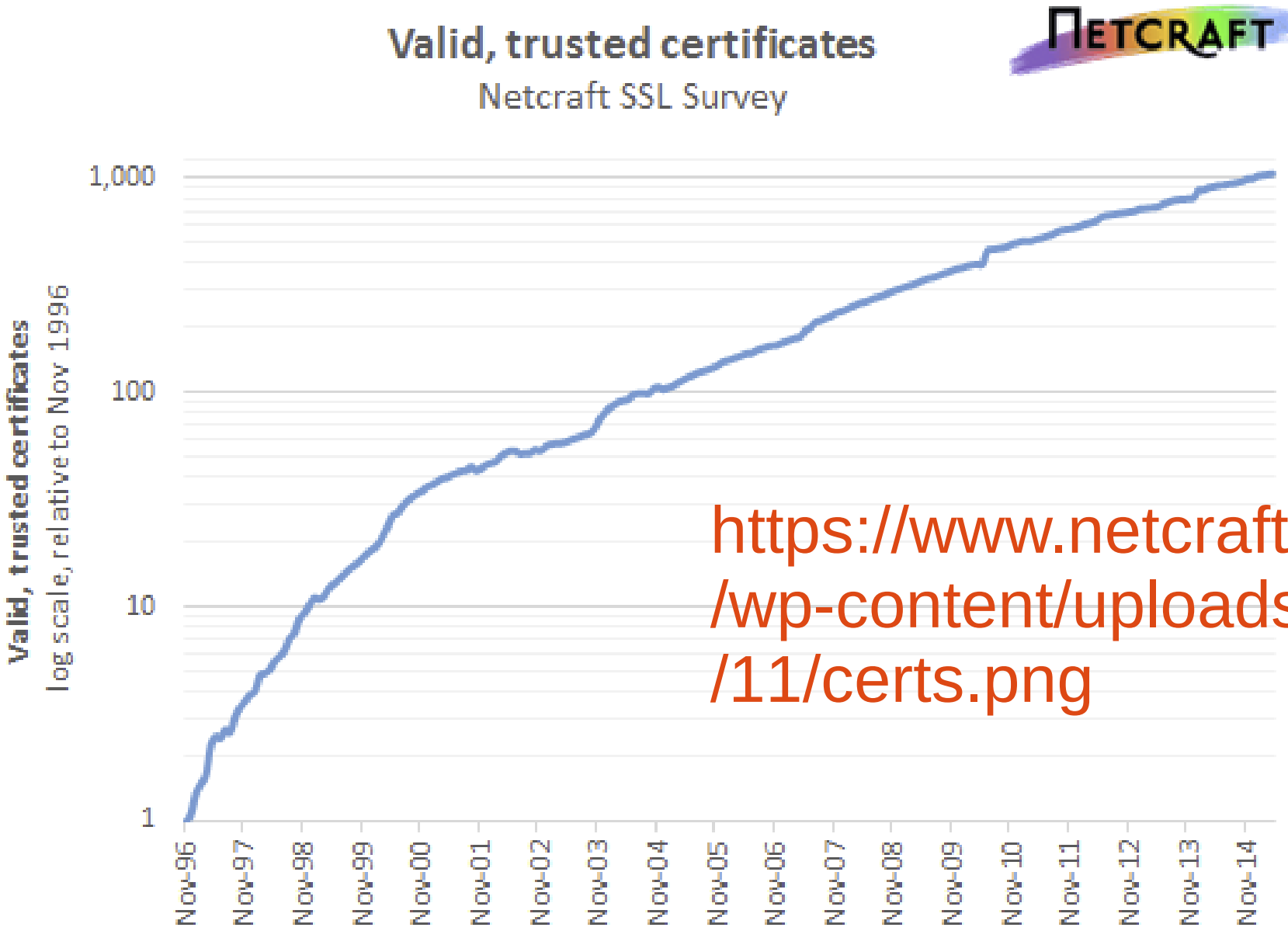
Figure 20
Test equipment

2013 - Snowdonia

- Partial timelines:
  - https://en.wikipedia.org/wiki/Global_surveillance_disclosure
  - https://www.theguardian.com/us-news/nsa
- My favourite:
  - https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo
- My most interesting (politically):
  - http://www.scmagazineuk.com/gchq-faces-new-belgacom-hack-allegations/article/388531/
- My most interesting (technically):
  - The short-range radar thing
  - https://en.wikipedia.org/wiki/NSA_ANT_catalog

https://en.wikipedia.org/wiki/Edward_Snowden

2015 – 1000x as much TLS



https://www.netcraft.com/wp-content/uploads/2015/11/certs.png

2016 – DNC spearphish

- Report on spearphising attempts aimed at US Democratic political party's 2016 presidential election campaign
  - https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign
- 10% of links clicked according to report
- Again, attribution is not convincing
- Role of DKIM signatures is interesting and not considered development

Moving on to the Future...

- Some people talk about the Internet of things but the Internet has always been made up of things
- Though maybe we can re-use the IoT marketing term…

Recently seen in a TCD cubicle...

The Other IoT

The Internet-of-Toilets will use the 5G network. In this IoT, each time a toilet is used, chemical (and perhaps DNA) analysis of the flushed content is done by the device and packets are sent to the network containing the results. IoT devices may be in the home, in businesses or provided by municipalities.

The data may be used for personalised healthcare services, for public health or, of course, advertising (imagine a pop up add over a pub urinal for just that medical condition you have;-). Insurance companies and lots of other businesses would likely be interested in the data. Service-selection and long term storage of the data present challenges.

These IoT devices are multi-user with no sophisticated user interfaces (except in Japan:-) and issues of identity, privacy, confidentiality and consent abound. Lawful intercept considerations would also arise - while societies may consider it ok for law enforcement to be able to listen to audio calls, it is not clear that the same is true for the packets emitted here, yet those are all bytes for the network."

Text from: https://down.dsg.cs.tcd.ie/misc/iot.txt

Some Security and Privacy Issues...

- Who controls the data generated?
- User interfaces and the lack thereof...
- Who is authorised to update devices, and how?
- Random numbers and crypto processing

Data Transport

- Devices generate data & send (secured via TLS?) to some host
- Today, there's no great way to get a (D)TLS server cert to use for that host unless the host has a DNS name
  - Leads to device→cloudy-server lock-in
- Challenge: find ways to authenticate and securely exchange keys between a small device and a host that the device-owner chooses
- Challenge: sometimes emitting a packet (encrypted or not) leaks privacy sensitive information
  - E.g. query sent to NTP server => person arrived home and stuff woke from suspend

Pervasive Monitoring

From RFC7258/BCP188: “Pervasive Monitoring is an Attack”

> Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts, including application content, or protocol meta-data such as headers. Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive monitoring. PM is distinguished by being indiscriminate and very large-scale, rather than by introducing new types of technical compromise.

PM is not everything

- PM is far from the only security or privacy issue on which we need to work
  - Spam, malware, DDoS, …
  - But mitigations for PM can also help a lot with other problems
- Hypothesis: If we work to address PM, and prioritise services and mechanisms that mitigate PM and that are also effective against other attacks then we will be doing the “right thing”
- And the “we” there means us all, not just IETF

Data Storage

- So my devices produce a trickle/ton of data every day, what happens to that?
  - Helps some vendors monetize me?
  - Leaks to some bad actors eventually?
  - Gets deleted when vendors end-of-life service?
- Challenges:
  - Minimise the data that is ever sent/stored
  - Scrub stored data regularly (with what guarantee?)
  - Data portability?

(Lack of) User Interfaces

- Device discovery and provisioning are just hard unless you also have the device call-home to a vendor-selected site
  - Device offering web server? See “data transport”
- Challenge: we need ways to introduce devices to our networks that are acceptable to the owners/operators of those networks
  - While we can all develop some of these, it’s not clear what’s really going to work well enough at big enough scale for the range of devices that will be developed

Opportunistic Security RFC 7435

- Security mafia modus operandi has (in practice) been to define and implement security that works for higher security environments

  => often hard/expensive to deploy => often not used => cleartext often sent even when better options exist

- Opportunistic Security (OS) aims to evaluate these trade-offs on a connection-by-connection basis, explicitly allowing for e.g. unauthenticated endpoints for confidentiality (open-channel key exchange) as an option that is better than cleartext
- I (personally) hope that this concept is followed very often and is fleshed out to the point where we end up with a new security development approach that is based around OS
  - Not there yet: TLS deprecation of RC4 was interesting because of differing perspectives from web and mail folks about what conclusion to draw when following the OS approach

OS example: Deprecating RC4

- RC4 past sell-by date: agreed by all
- For the web ~15% of https sites were using TLS/RC4 (FF 2014 measurement)
  - When RC4 zapped 99% of those just picked a better option (AES, 3DES)
- SMTP+STARTTLS between MTAs
  - There is a widely deployed MTA that only does RC4, 3DES is buggy and won't work (so I'm told)
  - Zapping RC4 means emails will be sent in clear between MTAs when one is the buggy one
- So – which is better: deprecate RC4 entirely or add this and possibly other caveats?
  - IETF rough consensus was to deprecate entirely, but some mail folks were in the rough
- Interesting example implying conclusion from following OS protocol design pattern will depend on scope
  - OS requires us each to figure out some kind of utility or objective function and where those differ enough, different well meaning folks will reach different conclusions
- It is OK that it is harder to figure out what to do when following the OS approach

Updates...

- Non-updatable devices are a recipe for disaster
  - cf. Mirai – plenty of badly engineered devices will continue to be added to (and found on) the public Internet every day
- Challenge(s): Many issues with s/w update in this context, we hosted a workshop on this in TCD in June 2016, see the draft report for details:
  - https://tools.ietf.org/html/draft-iab-iotsu-workshop
- Interesting “conclusion”: device update seems to call for all devices to support a way to “root” the device – both dangerous and seemingly necessary!

Crypto for small devices

- Some very small devices can’t play (D)TLS with the Internet, what then? Roll-your-own crypto? Urgh
- Issue with assurance that the crypto is “good”
  - Dual-ec fiasco http://dualec.org/
- Challenge: initiatives like https://cryptech.is/ needed for smaller platforms
  - More generally: We may need larger players to help fund OSS that makes life easier for small developers of small devices
  - Key part of this: good (P/T)RNGs

What to do? (1)

- Consider privacy issues in your networks and the data you make available
  - Avoid logging potentially sensitive data if you can
  - Find and delete old crap you no longer need
  - That means more work! But you should do it
- Encourage target diversity - Don't all use the same services all the time
  - Even if you're not a huge population, you can start trends

What to do? (2)

- Turn on crypto – ciphertext should be base assumption for new things
    - Consider the OS approach to make that easier
- Don't use new stuff without considering privacy implications
    - Data minimisation will save you some later leaks
- Help with better implementations
    - https://cryptech.is/ and similar

What to do? (3)

- Don't demand the impossible (and do nothing in the meantime)!
  - Encourage clean-slate work, but don't imagine it can all be deployed now – and only deployed things help
- Agitate (if that's your kind of thing:-)
- Consider privacy trade-offs when deploying e.g. IDS, anti-spam or malware detection technologies
- Go and be responsible network operators and take the broader implications of your work into account before, while and after doing it

Summary

- There's a bit of history, mostly bad:-)
- But there has been progress too, and we are getting better in some important respects
- IETF and others have consensus PM is an attack (RFC7258) and are working that problem, as a way to help get more and better deployment of security and privacy technologies
- When/if societies do decide that PM is as bad as it is, then the technical community should have in place the tools to effect that decision – you can help put those in place!

Thanks

Offline questions welcome too
stephen.farrell@cs.tcd.ie

These slides:
https://down.dsg.cs.tcd.ie/heanet/

Backup Stuff

IETF (Re)Action

- Overall: snowdonia has re-energised folks to do better on security and privacy in general (and not solely in response to PM)
  - Side meeting in Berlin @ IETF-87 (July 2013)
  - Tech plenary, major discussion @ IETF-88 (Nov 2013)
  - STRINT workshop before IETF-89 (Feb 2014) [RFC7687]
  - Topic at many meetings/BoFs @ IETF-89 (July 2014)
  - Seeing results from IETF-90 (Nov 2014) onwards...
- Unsurprisingly this is similar to the more broad technical community reaction

IETF work related to PM

- RFC 7258/BCP188 published after major IETF LC debate – sets the basis for further actions
- RFC 7435 defines “Opportunistic Security” - less gold-plating, more deployment
- IAB Statement on Internet Confidentiality: basically: encrypt everything!
- New working groups established:
  - UTA: update BCPs on how to “Use TLS in Applications” - RFC7525
  - DPRIVE: “DNS Privacy”- unthinkable before snowdonia RFC7626
  - TCPINC: “TCP INCreased security”: tcpcrypt proposed two years earlier but rejected
    - Mistakenly, including by me, as ack'd at mic @ IETF-88, bummer
- IAB re-factored security and privacy programme
  - Developed PM threat model document (RFC7624)
- Stuff not going so well
  - Old-RFC privacy/PM review team – go back and see what needs fixing: moribund
  - Endymail email list for discussion of ways IETF can help those working on new e2e interpersonal messaging solutions: hard problem

PM is an Attack RFC 7258

- RFC7258/BCP188 says that all IETF work will consider PM as an attack to be mitigated as part of our normal design processes for all protocol development
  - Note: this does not mean PM is always relevant nor that it's always practical to mitigate PM via protocol mechanisms, but if you can't, you need to be able to say why
- Took ~1000 emails to get rough consensus on that since countering PM is not free
    - Impacts on network management
    - Some folks scared of unreasonable security/privacy nerd dominance

DNS Privacy

- DNSSEC provides integrity and origin authentication but confidentiality/privacy was never considered a requirement
- Since 2013 that has changed, IETF DPRIVE working group was formed to tackle this issue
- Problem statement set out in RFC 7626
- QNAME minimisation RFC 7816
- TLS/TCP on port 853 between stub and recursive almost done, DTLS/UDP equivalent in the works
- Work on recursive to authoritative starting
- Discussion on DNS/HTTP at IETF97 (Nov2016) will certainly include DNS/HTTPS (way too early to say where that might go)

QUIC

- QUIC is a proposed new transport protocol that runs over UDP and that encrypts a lot
  - https://datatracker.ietf.org/doc/charter-ietf-quic/
  - Goal is the same security properties as TLS1.3/TCP
- QUIC is already deployed to some extent
- Privacy is not the only reason things like QUIC use encryption
  - Cleartext allows middleboxes to see and mess with traffic, which has good and bad aspects
- Will likely provide examples of the tension between privacy and the ability to manage a network mentioned in RFC 7258

Other relevant IETF Things

- TLS 1.3 aiming for better handshake encryption properties and learning from previous TLS problems in various ways
- HTTP/2.0, [RFC7540] the major deployment model for which seems to be to run much much more HTTP traffic over TLS
- Extension to HTTP/2.0 defining opportunistic security way of sending http URI schemed content over TLS
- Negatively: deprecate RC4 [RFC7465] in TLS, SSL3 [RFC7568]
- And since all this is IETF stuff, you can (and please do) join in and help if you're willing and able – that's how to make it better!
  - Even a small amount of good researcher input is hugely valuable (but you need to be able to deal with a noisy environment;-)
- New Curves and deprecating old crypto (CURDLE WG)
- OPENPGP WG updating crypto

Non-IETF Things Relevant to IETF

- Crypto Forum Research Group (CFRG) in Internet Research Task Force (IRTF)
  - Goal: provide venue bridging academic crypto and Internet technical community
  - Curve25519, Curve448 [RFC7748]
  - Chacha20/Poliy1305 AEAD construct [RFC7664]
- IEEE 802 have started work on privacy and are considering e.g. MAC address randomisation
  - Collaborating with IETF
- W3C TAG statement on “Securing the Web”
  - Builds on RFC7258 and IAB statement
  - https://www.w3.org/2001/tag/doc/web-https
- … there are loads more

Longer Term Factors at Play

- Spooks will be spooks (whether govt. or private sector)
- Privacy invasive commerce (legitimate and not)
- Legal accountability mechanisms (courts of various kinds)
- Small+good things can transition to (big+bad, dead or living-dead)
- Badly-informed decision makers/commentators/twits
- Government regulation of business (e.g. Data Protection Agencies)
- Commercial reaction to user privacy requirements (even evil corporate behemoths have many good folks working for 'em)
- NGOs working to enhance privacy (and get attention)
- Constantly refreshed naivety of yet another generation of clean-slaters (producing occasional good ideas)
- Guilt-by-association is a fallacy no matter who makes the error
- Technical privacy enhancing/enforcement mechanisms (when those work)

IAB Statement

"We recommend that encryption be deployed throughout the protocol stack since there is not a single place within the stack where all kinds of communication can be protected.

The IAB urges protocol designers to design for confidential operation by default. We strongly encourage developers to include encryption in their implementations, and to make them encrypted by default. We similarly encourage network and service operators to deploy encryption where it is not yet deployed, and we urge firewall policy administrators to permit encrypted traffic."

https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

So what else?

- We've outlined the problem
- We've seen there's work ongoing
  - Most addressing relatively low-hanging fruit in a sense
- Still hard to get agreed/done/finished/deployed
  - Esp. **deployed**, which is REQUIRED for this to be at all useful – Fantasy is of no use here
- But almost are fairly obvious things to do
  - Encrypt more, do more/better security, yay!
- So how about a hard problem or two?

More References (1)

- General IETF stuff:
- https://www.ietf.org/
- https://www.ietf.org/newcomers.html
- Working group details for WG <foo>:
  - https://tools.ietf.org/wg/<foo> - links to charter, docs, mail archive etc
  - Suggested <foo> values:
    - tls, dprive, tcpinc, httpbis, uta

References (2)

- Relevant IETF non-wg lists:
  - All of them (loads): https://www.ietf.org/list/nonwg.html
  - Perpass – triage list for PM related stuff:
    - https://www.ietf.org/mailman/listinfo/perpass
  - Security area list (saag)
    - https://www.ietf.org/mailman/listinfo/perpass
  - Possible e2e interpersonal messaging discussion
    - https://www.ietf.org/mailman/listinfo/endymail
  - General privacy discussion
    - https://www.ietf.org/mailman/listinfo/ietf-privacy
- IRTF:
  - https://www.irtf.org/
  - IRTF Crypto Research Forum Goup: https://irtf.org/cfrg

References (3)

- Videos (ISOC hint:-)
  - IETF youtube stuff in general
  - https://www.youtube.com/user/ietf/videos?sort=p&view=0&flow=grid
- Nov'13 IETF technical plenary video
  - https://www.youtube.com/watch?v=oV71hhEpQ20
- Dan york videos 5 minute summaries of IETF meetings
  - There are loads but these are about PM
  - https://www.youtube.com/watch?v=HG54EsHYKr0
  - https://www.youtube.com/watch?v=fbjs_6Mz-6s
- STRINT workshop (RFC7687)
  - Has all 66 position papers
  - https://www.w3.org/2014/strint/

References (4)

- IEEE Internet Computing “soapbox” column on why PM is bad:
  - http://www.computer.org/csdl/mags/ic/2014/04/mic2014040004.pdf
- Some Internet drafts not referenced above:
  - PM Threat model
    - https://tools.ietf.org/html/draft-iab-privsec-confidentiality-threat
  - DNS Privacy problem statement`
    - RFC7626
  - “Modern” TLS best current practices
    - RFC7525