Research and Engineering on Security and Privacy Of Networks and Systems for Ireland and a Better onLine Environment (RESPONSIBLE)

Oriel House, TCD

September 11/12 2017

stephen.farrell@cs.tcd.ie

Slides: https://down.dsg.cs.tcd.ie/responsible/materials/

Welcome

- Thanks to you for coming along
- Thanks to our generous sponsors CONNECT and IEDR

CONNECT
Centre for Future Networks

.ie
Identifiably Irish
Ireland's Domain Registry

- Thanks to Mike Scott for helping with TPC
- Thanks to Peter Lavin for helping logistics
- Apologies for the awful backronym:-)

Logistics - physical

- We’re in this room today and tomorrow
- Fire exits and toilets are…
- Breaks/Coffee etc in the room
  - You have the info about getting back into the building if locked out
- Evening event @ Kennedy’s
  - Who’s coming? (I’d like headcount by 4pm)
- Phones to silent! Use laptops as you prefer.

Logistics - digital

- WiFi via CSopen – see (paper) list for account info and scattered instructions
- Mailing list: responsible@scss.tcd.ie
  - I think you're all on it, but ping me or Mike if not
  - I'd like to see that as a place for discussion but more on that later…
- Meeting notes: dive in to the etherpad and scribble away:
  - https://public.etherpad-mozilla.org/p/responsible
  - We can use that for notes/scribbling ideas – note takers welcome!
- Web site: I've registered responsible.ie and may even have put up a server there by now
- We're not recording/broadcasting meeting afaik

Today’s Rules-of-engagement

- Chats over coffee so far used (my variant of) **Chatham House Rule**
  - https://www.chathamhouse.org/about/chatham-house-rule
  - That basically means what is said is (in theory) public, but “who said what” is not public – i.e., no attribution/quoting
  - Makes it easier for some folks to be more open
  - My variant is that the list of participants is (in theory) public
- We can keep with that or do something else?
- I suggest we keep with that for today and discuss future rules-of-engagement in the pub or in planning sessions tomorrow
- If so, please adhere to this in any social media posting

Don’t be quiet!

- Agenda topics are intended to be discussions, not lectures
  - Do interrupt!
  - Don’t be shy
  - Don’t be quiet
- If it’s ok, I’ll act in a chair-like manner and be neither shy nor quiet about jumping in to keep discussion on topic

Prizes Galore!

- We have some (TPC selected) joke prizes for:
  - Bestest briefest intro
  - Good idea that might even happen
  - Most guerrilla-marketing organisational idea
  - Something random
- Prizes will be given out in the pub

Agenda-Bash

Today:

1300-1315: Opening/intro/logistics, Stephen Farrell, TCD

1315-1330: Attendee intros - ~1 minute per person, a few folks at a time

1330-1430: Overview of problem space, Stephen Farrell, TCD

1430-1500: Coffee

1500-1515: Attendee intros - ~1 minute per person, a few folks at a time

1515-1600: Security-related network measurements, David Malone, NUIM

1600-1615: Attendee intros - ~1 minute per person, a few folks at a time

1616-1700: Selling Crypto - developing crypto in Ireland, Mike Scott, MIRACL

1700-1715: Bio-break/coffee

1715-1745: Unconference planning for day 2

Agenda-Bash

This evening: Pub 1800-late

Tomorrow:

0900-0930: Day 2 plan review

0930-1030: Separate interest parties

- Not sure about rooms yet

1030-1100: Coffee

1100-1200: Summarise plans for work

1200-1230: Wrap-up/further actions/meetings

1230: End/lunch/maybe more pub

Intros

- Please be brief – you are all interesting, but a pile of even the most interesting intros is boring!
  - Try stick to one minute
- Good things to cover:
  - Name & Affiliation
  - Background/general interests
  - Specific interests today/tomorrow
  - How'd you like to see this effort evolve?
- Feel free to put more (links etc.) in the etherpad

/me Intro

- Trinity College Dublin, School of Computer Science and Statistics
- Recently escaped IETF security area director from 2011-2017, v. recently suckered into being a co-chair of IETF homenet working group
- Research topics: Internet security, privacy, delay-tolerant networking
- Hope we find ~3 small projects to get started and go from there, with those and building a sustainable collaboration, maybe under an isoc.ie umbrella

Background/scope disucssion

Outline

- Remember: Do interrupt!
- Some examples
- Background
- A suggestion for scoping
- List of topics raised already
- An idea for getting academics going
  - With help from others

Examples

- Remember: Do interrupt!
- Next few slides are semi-random topics aiming to get us thinking in the right space…
  - The other IoT
  - Data Leaks
  - Implementation issues
  - Scary-movies
  - Regulation
  - Pervasive Monitoring
  - Old reliables
- I have a longer talk trying to take a longer views if you’re interested (from HEANET 2016):
  - https://down.dsg.cs.tcd.ie/heanet/

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

Data Leaks

- Soooo many from which to choose…
- https://www.equifaxsecurity2017.com/
  - Data on 143M US people + ?? non-US folks
    - https://www.theregister.co.uk/2017/09/08/equifax_breach_notification/
  - “... includes names, Social Security numbers, birth dates, addresses and, in some instances, driver’s license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed”
- https://haveibeenpwned.com/Passwords
  - 320M password hashes from various leaks accumulated in last few years released early August, reversed (https://cynosureprime.blogspot.ie/) before end-August

Implementation Issues

- CVE-2017-1000249: file: stack based buffer overflow
  - Sep 5th: https://marc.info/?s=CVE-2017-1000249&l=oss-security
  - The UNIX/Linux “file” command tells you what kind of file a file is:

```
$file thedoor.jpg

thedoor.jpg: JPEG image data, Exif standard: [TIFF image data, little-endian,
direntries=7, xresolution=98, yresolution=106, manufacturer=Jolla, model=Jolla,
orientation=upper-right, datetime=2017:09:07 14:40:46], baseline, precision 8,
3264x1840, frames 3
```

  - Has a buffer overflow
  - But “file” is used in some automated systems, incl. email attachment handlers
  - Those systems might thus be vulnerable

Scary-movies...

- There are some less simple issues facing us in future too: A sufficiently capable quantum-computer (QC) could essentially break all public key cryptography currently in widespread use
  - Lots of people are working to try develop such things
  - Don’t panic! Some years to go, at least. Maybe a decade or two. Maybe more.
- Sensible reaction today could be to assess vulnerability (e.g. data that’ll still be sensitive in N>10 years) and experiment with post-quantum (PQ) cryptography deployments
  - PQ meaning crypto intended to be resistant even if there were such a QC
  - Use of PQ schemes usually means mixing new algs with those considered safe today (“classical crypto” algs)
- One step might be to identify the kinds of data at risk

Regulation...

- GDPR is on it's way
  - http://ec.europa.eu/justice/data-protection/reform/index_en.htm
- NIS directive too
  - https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
- IoST will likely drive some product liability regulations for commercial products
- AI and algorithmic bias may do the same for s/w, maybe even open-source (Huh? How?)
- Counter terrorism vs. privacy tension will persist
  - IMO at least until a really radical and open requirements analysis is done by law enforcement and other interested parties (which won't happen)

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.

Old reliables...

- Many extremely simple problems just never seem to get fixed, or constantly recur:
  - Buffer overflows etc...
  - SQL injection...
  - Wordpress sites not updated...
  - Ransomware + no-backup/restore…
  - <insert your fav here>

Background

- I assume we agree that:
  - Internet and systems security and privacy are important and worth improving
  - There is expertise in Ireland to such work but a lack of critical mass in any one place, whether that’s academic, commercial, government or “civil society”
- It seems credible to me that some local activities could usefully address some local issues in this space and also be more globally relevant
  - Local significance => local interest => potential for sustained collaboration

Moar Background

- Since April I’ve had chats with a bunch of folks on this topic (many here, some not here) and it seems to me that there is interest in this space and people say they’re willing to do work together
- Not yet clear that the set of overlaps is sufficient, nor that people will actually (be able to) do what they’ve said interests them
  - $dayjob does tend to win
  - but I’m hopeful...

Scope

- I’d love if we can focus on work where:
  - it’s credible that work done in Ireland can move the needle locally in a useful manner, relating to Internet security and privacy – if globally interesting too, that's great
  - the results of work done are intended to be public - so not (or rarely) dealing with operational data or embargoed CVEs and hopefully generally with less sensitive data (though there may be some sharing of sensitive data for research purposes of course)
  - we can develop e.g. proofs of concept/guidance/scan-results that can later be used by ops folks or users

Scope Example

- Fixing all IoST issues is not credible to do from Ireland
  - Control over development is elsewhere
  - Maybe some subset of devices could be tackled, not sure
- Local monitoring/testing/whitehackery of such devices is quite doable
  - I expect lots of low-hanging fruit there
- Training wrt the issues involved could be doable
  - E.g., educate about known attacks, battery depletion attacks, privacy issues
- Developing some recommendations could be doable
  - E.g. only buy stuff with an update and an update story for the future (see RFC 8240, when it's published:-)
  - Not sure if "Don't buy <this> crap" recommendations is doable

Topics Raised

- Next few slides from the w/s page, also on the etherpad (do add to/edit that)
  - No harm to just flick over it to populate our caches...
- 3 broad buckets
  - Communications and systems security and privacy
  - Patterns and measurement
  - Advice and best current practices (BCPs)

Communications and systems security and privacy

- Better local security in a BYOD world
- Carrying out example risk analyses of local systems/infrastructure
- Dealing with new security technologies in current and legacy systems (e.g. performance and network management impacts of increased encryption)
- Developing/piloting privacy-sensitive non-commercial local sharing for DDoS mitigation and malware detection
- Improving back-end transparency in a locally significant manner
- Low-cost forensics for SMEs and others
- Methods for integrating post-quantum cryptography into protocols/applications used locally
- Piloting local authentication infrastructure (PKI/2FA)
- Piloting new security and privacy technologies locally, e.g. DNS privacy
- Reproducible/curated builds/mirrors of open-source technologies for local use, possibly SME focused
- Securing local IoT testbeds/pilots/demonstrators
- What can replace outmoded concepts of "consent" locally?
- Whitehat hacking/testing of devices used/considered-for-use locally with responsible disclosure route back to vendors/users if appropriate/possible
- Privacy by design for data analytics

Patterns and measurement

- Audit tools to help detect local instances of PII
- Audits of data using current BCP security mechanisms that could be vulnerable in the presence of a quantum computer
- Automating production of locally useful evidence as part of incident handling
- Developing meta-data guidelines so holders of (large) data-sets can share (or interface with one another) in a more privacy sensitive manner respecting the wishes of data holders/subjects and in accordance with local regulation
- Local co-operative network intrusion detection
- Local detection of unwanted surveillance devices (IMSI catchers, MitM boxen)
- Local impact of analog sensing (video,audio etc.) on security and privacy
- Local surveys (e.g. zmap of HTTP/TLS,SMTP/STARTTLS, AS112 etc.) with some kind of responsible disclosure route back to asset holders with detected issues
- Mechanisms e.g. public ledgers/blockchain to support governance of the large-data meta-data just mentioned
- Measurements (e.g. of data set) aiming to provide empirical evidence of (non)compliance with local laws
- Measuring local IoT deployments, e.g. to scan for vulnerabilities
- Uses of, or acquisition of, passive DNS locally

Advice and BCPs

- Advice and training for local law enforcement
- BCPs for local SMEs on dealing with privacy and security
- Locally, what do we consider provides "consent"
- Minimising impedence mismatch between technology deployments and regulation
- Personal infosec/privacy training for legislators
- Provide advice on policy and appliation impacts of current and near-future cryptographic mechanisms
- Providing advice to help avoid common damagine attacks, e.g. ransomware and Wordpress hacks and measuring the efficacy of such advice when offered
- Technical aspects of dealing locally with current and upcoming EU directives, helping gov.ie and similar folks understand the consequences of possible regulatory actions,
- What does (not) constitute local critical infrastructure?

A modest suggestion

- Now is about the time of year when we (in TCD anyway) set out lists of final year student projects and master’s dissertation topics
- I’m happy to modify my list based on discussion here
  - https://down.dsg.cs.tcd.ie/projects/2017-projects.html
- It’d be a fine thing if others of us in academia were also happy to do that
- Even finer if we co-ordinate a bit on that (not all students are equally capable, some projects could usefully be related)
- Finer again if we could identify non-academic folks who’re interested in collaborating on such projects (could be with data, or setting requirements or whatever)
- From there, maybe we can build towards funded work for whatever kinds of funding make sense in or outside academia
- Note: This is just one idea – more welcome!

Thanks

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

These and other w/s materials:
https://down.dsg.cs.tcd.ie/responsible/materials/