Where is cybersecurity developing towards?

A view on recent trends in the standardization of cybersecurity

Outline of content – an agenda of sorts

- A quick review of where we are and where we want to go
- Existential threats
- Technology opportunities
- Regulatory opportunities
- Forecasting the future

A quick review …

- Where we are
  - We've achieved recognition that security is good and essential and that it's difficult
  - Cryptography is now mainstream and expected
- Where we are in a bit of a rut
  - We're still stuck with security being considered as a synonym of safety
  - We're still stuck with security being confused with privacy
- Where we want to go
  - Effective deployment of security technology to manage risk to reasonable levels

Some review points

- 2G security through 3G, 4G and 5G
  - Strong and state of the art
  - Evolving with added functionality over time:
    - Authentication of the phone, added authentication of the network, added longer keys for authentication (including a CMAC for the mutual element) and encryption, added in keying for higher layer functions, merging WiFi and cellular security models, moving from circuits to sessions
- IoT and ICT towards an Internet of Everything
  - Rooted in IP but extending way beyond
- Better understanding of ephemeral keying
  - Not just TLS1.3 but building out from session keys in 2G

A bit more review

- We’re pushing security at the heart of most standards work
  - In AI
  - In IoT
  - In smart cities
  - In Intelligent Transport
- We are recognising privacy assurances aren’t the same as security assurances
  - Assurance schemes are evolving to be suited for all device types and services

A last review point

- We've achieved convergence (in the standards domain)
  - Services are mostly platform agnostic
  - Networks carry bits and those bits could be voice, data or video
- Speed is available most of the time
  - Domestic offerings of 1Gb/s are common
  - Wireless (cellular) offerings of 100Mb/s and up are available (if not common)
  - Blackspots of connectivity are shrinking
- Digital citizens and digital society exist
- Smart cars, smart cities, smart homes exist

Existential threats

- Quantum
- Pervasive encryption
- Bad guys
- Good guys with good intent but no knowledge
- Crypto
- Energy costs
- AI and its cousin ML

Quantum – an existential threat

- Quantum computing will destroy the tenet of current asymmetric cryptography
  - Most asymmetric cryptography is based on “hard” problems that can be resolved with quantum computers
- Quantum safe algorithms are still in development and still not mature
  - How much time do we need? Probably more than we have
    - X = the number of years the public-key cryptography needs to remain unbroken.
    - Y = the number of years it will take to replace the current system with one that is quantum-safe.
    - Z = the number of years it will take to break the current tools, using quantum computers or other means.
      - If X+Y>Z we’re in deep doodoo
    - T = the number of years it will take to develop trust in quantum safe algorithms
      - Adds a major complication and it now becomes if X+Y+T>Z we’re in deep doodoo
- Quantum safe cryptography requires orders of magnitude increase in key size, signature size, computing resource
  - Even devices that today are unconstrained will be in danger of becoming constrained (unable to offer equivalent functionality)

Pervasive encryption

- Encryption is good, as is cryptography. The role of encryption of information being transported between two end-points has three widely recognized positive purposes depending on the context:
  - confidentiality protection of the transferred content;
  - enhanced trust in the identity of the parties associated with the information; and
  - enhanced trust in the integrity of the information during transport.
- End-to-end encryption = good, is a marketing mantra that isn't all it seems, if it means everything is encrypted
  - It removes pre-emptive filtering of malicious content
  - It means networks are just pipes with no added value – can routing work if everything is encrypted with keys known only to the end points?
  - Regulatory bypass (no oversight, operators are like rabbits caught in the headlights)

Countering threats of pervasive encryption

- Adoption of Zero Trust Architectures
  - Moves from Implicit to Explicit trust
- Require explicability and transparency of where encryption is used
  - Don’t assume – prove

- Work being addressed at ETSI ISG ETI

Bad guys, good guys

- Bad guys will spend €s to make cents – it's a profit thing
  - The risk of penalty is built into their profit motive
- Good guys don't have profits to justify their existence, they're always a cost item (an expense)
  - If you've not suffered from attack is it because your defence is good or you're not a target (yet)? How much should I spend on defence?
- Good guys sometimes make bad decisions:
  - Encryption enables criminal activity to be hidden → let's ban encryption
  - Functionality comes first so let's get the code working and then secure it later
  - That webcam in the child's toy could be used to spy on me. Nobody would do that surely? It's just a toy

Crypto

- As in currency
  - ”I work in crypto” could give the impression to a layperson that you’re in banking or finance
- It’s not a security in the ICT sense but may be a financial security
- Crypto (currency) may divert expertise from everyday ICT security
- Crypto (currency) could be killed off by quantum threats
  - Where does my money go?
  - If there’s no central authority to endorse money does it exist?

Energy costs

- Cryptography consumes a lot of processing cycles
  - The longer the key, the more rounds, the more power that is needed
- Same with memory
  - Needed to store keys, to process the crypto functions
- Same with communications resource
  - Sending keys, overhead of signature

- Today's crypto when used in new processes often becomes energy intense (in a bad way)
  - Bitcoin consensus protocols are notoriously energy inefficient

Artificial Intelligence

- In general terms more intelligence applied to a “hard” problem, and more intelligence power, cracks the problem or prevents the problem ever arising
- AI, and Machine Learning, offer a couple of things to worry base ICT security:
  - Lots of effort to uncover weaknesses in core crypto-systems compressed in time by algorithms finding weak correlations and multiplying them to be causations
  - Patterns unknown as weaknesses discovered by all out machine driven attack – botnets on steroids
- AI at the application level may be even worse – deep fakes destroy trust
  - Uncertainty breeds doubt and doubt destroys trust

Opportunities do exist

- Technological
  - More processing power, more bandwidth, more maths
- Regulation
  - Understanding the need for ICT security in society
    - Waking up to the 21st century being an ICT connected society
    - Recognising the threat to nation state security of ICT threats to institutions, industry, individuals (the 3i's)
  - Mandating for security breaches to be treated criminally (breaches can mean jail time)

Technology is on our side

- Crypto-processing is well understood (for today's crypto)
- Lessons learnt from today will transfer to tomorrow
  - Modern symmetric crypto is often a complex mix of centuries old techniques of substitution (changing one symbol for another) and transposition (moving symbols in a document around) with a key giving the big hint of how to tangle and untangle things
  - These roots will not change all that much, they will be extended in subtle ways though
- Number theory is no longer an arcane field with nobody taking an interest
  - We now teach number theory and algorithms in maths (not just in statistics classes)

Technology, a good companion

- Good guys can use it to thwart the bad guys
  - Harness the power of AI/ML to identify attacks and attackers before they become an issue
  - Use Quantum to give an edge – alongside new processor designs use quantum mechanics to work on new algorithms, use QKD as an extension to more conventional key management schemes, explore the role of superposition and teleportation and entanglement in enabling security
  - Holographic processing (not holostate but multi-path processing in crystalline structures), multi-state processing, neural nets, all have a role to play

Risk management technologies?

- Risk is what we're trying to manage
- Risk assessment needs clear understanding of what we have (components) and how they fit together (interfaces)
- Modern systems are challenging for risk analysis as the components and their interfaces are auto-mutating, auto-evolving
  - We need to improve our ability to track risk in live systems
  - We can harness AI/ML to help us here

Regulation is going to help us

- Security of users is at the core of many new regulatory initiatives:
  - The Cybersecurity Act in the EU
  - The Privacy directives and data protection directives
  - The Radio Equipment Directive
  - The proposed AI Act
- All of the above (and many others) make it clear that poor security which leads to harm is unacceptable
  - Security provisions, commensurate to the risk, are mandated by law
  - Penalties for failure are significant (The UK GDPR and DPA 2018 set a **maximum fine of £17.5 million or 4% of annual global turnover – whichever is greater** – for infringements. Th EU GDPR sets a maximum fine of €20 million (about £18 million) or 4% of annual global turnover – whichever is greater – for infringements)
  - Similar levels of penalty are expected from the other acts

Regulation helps but how?

- Security is still an expense but it’s not optional and can’t be easily cut
- The regulation is deep and broad
  - Requires developers to prove they’ve done the risk assessment and made adequate provisions to minimise it
  - Addresses the entire supply chain
- Governments need to ensure they’ve made provision in education
  - Primary, Secondary, Tertiary and post-grad too, also adult education
  - Employers too need to ensure they keep their experts expert

Regulation and technology work together

- Trust is not just personal but it's still couched in society as if it were
  - Trusted institutions – government, school, church?
    - Why do we trust institutions? Are we simply educated to trust them?
  - Trusted roles – doctors, lawyers, accountants, engineers?
    - Do we trust them because of the steps they go through to become qualified?
  - Trusted technology – Operating systems, applications, hardware, comms
- New trust frameworks for ICT driven societies?
  - ICT led change has moved faster than many of our key institutions and roles
- We need to get to a point where trust is explicit, explicable and transparent in our ICT worlds

The crystal ball bit …

- Disclaimer: Forecasts are by nature unreliable, only hindsight is reliable (with the right analyst anyway)
- The easy bit:
  - Technology will continue to improve (Moore's law downscaled to different levels of efficiency)
  - Software will become more testable
  - Users will expect secure systems by default
- The hard bit:
  - When things will happen is not an easy prediction

Commercial reality of forecasting

- Processor architectures will change and the software they support will change
  - EXAMPLE: Apple have moved into SoCs for all platforms
  - … but only Apple know when actual changes will get to market
- Software developments, and hardware developments, will be driven by sales pressure
  - EXAMPLE: a new OS demands new hardware and the market demands new every year
  - … but this suggests fashion and not novelty
- Society will adopt and mould technology – not the developers
  - EXAMPLE: Facebook and Twitter are quite different as their use became mainstream
  - … but the destination is never certain when we start

Closing remarks #1

- A system without security will not be viable to enter the market
  - Society will demand it, and vendors/developers/providers will have to provide it to survive
- Regulators and nation states have to defend their citizens
  - If ICT is a source of threats then regulators and nation states have to ensure that ICT is secure in order to protect and defend their citizens
  - … and their sovereign wealth
  - … and their borders

Closing remarks #2

- Standards as drivers for interoperability will remain critical
  - The purpose of standards hasn’t changed – they open markets to more players
  - One player can only serve a limited number of customers, a standard could allow 100s of players to serve the market, and that market could be 1000s of times bigger that a single player could serve.
  - One player can only evolve the market at their pace, 100s of players means there is a race for market share and market evolution

A take-away …

- "*Standardization does not mean that we all wear the same color and weave of cloth, eat standard sandwiches, or live in standard rooms with standard furnishings. Homes of infinite variety of design are built with a few types of bricks, and with lumber of standard sizes, and with water and heating pipes and fittings of standard dimensions*",
  W. Edwards Deming

Thanks for listening

Scott CADZOW, scott at cadzow dot com, somewhere in England