The Future of IoT Security and "Cybercrime"

Craig Heath
@heathcr

IoT Security Foundation Conference
06 Dec 2016

Franklin Heath Ltd

Predicting the Future

- Considering trends + thought experiments
- Where I'm coming from:
  - personal experience
    - first job in software 1977
    - computer security specialist since 1988
  - history of information security
    - Bletchley Park 1939-45
- But isn't the Internet of Things new and different?

What is “Cybercrime”?

- Computers used to commit “traditional” crimes
  - Roswell Steffen 1973 (embezzlement > $1.5M)
- Unauthorised use of computers
  - Stephen Gold, Robert Schiffreen 1985
  - Kevin Mitnick 1987
- Breaching computer security has itself become defined as a new type of crime
  - UK Computer Misuse Act 1990
  - US Digital Millennium Copyright Act 2000

Past Trends: What Has Stayed the Same?

- Information theory & computer science
  - Kerckhoffs 1883
  - Turing 1936
  - Shannon 1948
  - Saltzer & Schroeder 1975
- Passwords
  - easy to understand and implement
- Social engineering attacks
  - “rubber-hose cryptanalysis”

Past Trends: What Has Changed?

- Number of devices, connectivity and bandwidth
  - billions, always-on with multiple Mbps
- "Classic" crimes have moved online
  - e.g. confidence tricks → phishing, extortion → ransomware
- "Beta culture"
  - continual enhancement and patching
- Magnification of capabilities and consequences
  - a fix can be rolled out to millions of users
  - a single attacker can harm millions of users
- The "attribution problem"
  - nation state or a kid in a cyber café?

Is Computer Security Getting Worse?

- I don't know any computer security professional who would argue it's getting significantly better
- I don't know anyone who has stopped using the Internet because it's getting significantly worse
- Hypothesis: did we reach a sort of equilibrium in the 1990s that is acceptable to society, now maintained by governments and market forces?

Will the Game Change?

- IoT
  - Orders of magnitude more devices
  - Unregulated, connected devices which affect the real world
- Quantum Computing
  - Risks for Public Key crypto algorithms
  - “Post-Quantum” cryptography is being researched

Downside Influences

- Increasing complexity of systems and algorithms
  - if you don't understand it, you can't fix it
- Increasing value available to attackers
  - transaction limits increase
  - ever more data goes online
- Increasing ability to affect the real world
  - "Cyber Physical Systems"
- Better policing of non-computer crimes
  - bad guys usually follow the path of least resistance

Upside Influences

- Market forces
  - consumer awareness
    - but worry about “The Market for Lemons” (Akerlof 1970)
  - risk of reputational damage
    - e.g. Ratner, Ashley Madison, VTech?
  - cost of breaches
    - and/or conditions of business insurance
- Legal forces
  - regulation (c.f. building regulations)
  - licensing (c.f. chartered civil engineers)
  - fines or compensation awards for affected consumers

Crystal Ball Time

- Computer security fashions change, but fundamentals don't
  - Old-fashioned: firewalls, anti-virus
  - Today's fashion: penetration testing
  - Tomorrow: addressing the causes?
    - better development process
    - better platforms and tools
    - better developers
- We (society) need to choose which market forces and legal forces we want
  - Similar to public health issues?

Questions?

craig@franklinheath.co.uk

@heathcr

@franklinheath