Security by Design is an Oxymoron

German/IranianForum on Security Research Areas
October 29th, 2016

Dieter Gollmann
Security in Distributed Applications
Hamburg University of Technology

TUHH
Technische Universität Hamburg-Harburg

Scylla & Charybdis

- Two monsters from ancient Greek mythology

Scylla & Charybdis

- Two monsters from ancient Greek mythology
- Straits of Messina, between Sicily and the Italian mainland
- Major trade route from Eastern to Western Mediterranean
- Trade routes – hazard risks and opportunity risks
  - Storms and currents
  - Pirates and competing powers
- Parallels between the internet and the Open Seas?

Scylla – The Criminal World

- Criminals are innovative
- New applications provide new opportunities
- Criminal energy is inexhaustible
- How can you be secure by design if you do not know all you have to defend against?

Scylla – The Criminal World

- Criminals are innovative
- New applications provide new opportunities
- Criminal energy is inexhaustible
- How can you be secure by design if you do not know all you have to defend against?

- In security, the defender has to move before the attacker
- Unless you believe in penetrate-and-patch

Defending Against the Unknown

- How can you be secure by design if you do not know all you have to defend against?

- Design of block ciphers (1980s)
  - New ‘improved’ block ciphers proposed in aftermath of DES
  - When academia rediscovered differential cryptanalysis the ‘improved’ ciphers turned out to be weaker than DES

- Smart cards for public key cryptography (1990s)
  - Research on faster algorithms for enhancing performance
  - When side-channel analysis was discovered it was found that performance enhancements were leaking keys

Charybdis – The Whirlpool of Apps

- Business and customers are innovative
- Technologies used in ways they were not designed for
  - Credit cards designed for ‘customer present’ transactions
  - Today one of the main payment modes in the internet
- How can you be secure by design if you do not know what you are designing for?

Defending the Unknown

- Disruptive Technologies [Christensen]
- Cheap and simple technologies, do not meet requirements of sophisticated users, but are adopted by a wider public
- When the new technology acquires advanced features, it takes over the entire market
- Problem for security: security features may not be required by the applications the new technology was designed for; when it turns into a platform for sensitive applications, re-integrating security becomes difficult

Disruptive Technology #1 – PC

- In the 1980s there were workstations and PCs
- Workstations for professionals, powerful, fancy graphics, serious machines for serious people
- PCs for amateurs, basic operating system, crude graphics

Disruptive Technology #1 – PC

- In the 1980s there were workstations and PCs
- Workstations for professionals, powerful, fancy graphics, serious machines for serious people
- PCs for amateurs, basic operating system, crude graphics

“1984”
Apple Macintosh
commercial
Superbowl XVIII

- There were many more amateurs than professionals

Demise of the Workstation

- Computing and graphics capabilities of PC got better
  - Anything good for visualization in engineering is good for visualization in computer games
- What happened to Apollo, DEC, Silicon Graphics, Sun?
- Workstation security:
  - Designed for engineering applications; issues like access control were considered
  - Top security researchers at DEC (Butler Lampson, Turing Award 1992)
- PC: single user stand-alone system; security is redundant
- End of story: systems 'insecure by design' (not their fault!) had squeezed out the more secure professional solutions

Disruptive Technology #2 – Internet

- Once upon a time there were telephone networks providing real time connections
- Once upon a time IBM had a network architecture (SNA) with robust protocols guaranteeing message integrity
  `https://www.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.znetwork/znetwork_151.htm`
- Packet-switched networks were scavenging spare capacities in the telephone network
  - IP as a best effort protocol: no security, no reliability
  - Killer application of the internet: email
- Industrial strength professional system competing against an experimental research network

Disruptive Technology #2 – Internet

- And the winner is

Disruptive Technology #2 – Internet

- And the winner is the internet

Disruptive Technology #2 – Internet

- And the winner is the internet
- A sigh of desperation from IBM, mid 1990s:
  “Our customers are switching over to TCP/IP, start from scratch to get back to where they already had been with our solutions”
- Telco operators first competed in offering cheap flat rates for internet users, and then complained that Apple and Google were earning all the money
- Public administration in Hamburg has just moved to VoIP

Disruptive Technology #1 + #2

- When the internet was released to the public, PCs at home and in the office got connected to the world at large
- When the internet was released to the public, it became a platform for e-commerce
- Devices insecure by design become terminals for commercial transactions
- This is a very generous invitation . . .

Disruptive Technology #1 + #2: Reaction

- Insecure legacy devices protected by firewalls
- Secure SSL/TLS tunnels for e-commerce
- Better software security in operating systems (DEP, ASLR) came after some delay

Disruptive Technology #1 + #2: Reaction

- Insecure legacy devices protected by firewalls
- Secure SSL/TLS tunnels for e-commerce
- Better software security in operating systems (DEP, ASLR) came after some delay

- Attacks moved into web pages, browsers (SQLI, XSS)
- Even perfect O/S security wouldn't stop these attacks

Security by Design is an Oxymoron

Oxymoron

An apparent juxtaposition of opposites

Making promises that can't be kept
is a dangerous long term strategy

Security by Design???

- Security means ‘no surprises’

Security by Design???

- Security means ‘no surprises’
- The bad news
  - There will always be surprises
  - Side channel attacks were a surprise to crypto in the 1990s

Security by Design???

- Security means ‘no surprises’
- The bad news
  - There will always be surprises
  - Side channel attacks were a surprise to crypto in the 1990s
- The good news
  - There will always be surprises
  - Surprises create problems $\rightarrow$ challenges $\rightarrow$ opportunities

Security by Design??

- What do we (security professionals, security researchers) mean by ‘security by design’?

Security by Design??

- What do we (security professionals, security researchers) mean by ‘security by design’?

- Defences against ‘zero days’, ‘APT’, . . . ?
  - Turn fortune telling into an engineering discipline?
  - We’d be in good company; Newton worked on astrology

Security by Design??

- What do we (security professionals, security researchers) mean by ‘security by design’?
- Defences against ‘zero days’, ‘APT’, . . . ?
  - Turn fortune telling into an engineering discipline?
  - We’d be in good company; Newton worked on astrology
- Avoiding unforgivable vulnerabilities?
  - This is first a matter of education
  - In research, keep pushing the boundary of ‘unforgivable’

Security by Design??

- What do we (security professionals, security researchers) mean by ‘security by design’?
- Defences against ‘zero days’, ‘APT’, . . . ?
  - Turn fortune telling into an engineering discipline?
  - We’d be in good company; Newton worked on astrology
- Avoiding unforgivable vulnerabilities?
  - This is first a matter of education
  - In research, keep pushing the boundary of ‘unforgivable’
- The next boundary: software security
  - Software is everywhere!
  - Still scope for fundamental research, but more a matter of industrial practice and research on industrial practice

Final Thoughts – The Modern Car

Final Thoughts – The Modern Car

Final Thoughts – The Modern Car

+

Final Thoughts – The Modern Car

car of the future: a smartphone on wheels

Final Thoughts – The Modern Car

car of the future: a smartphone on wheels

Which surprises lie in store?

Thank you very much for your attention!

Questions?