How to develop secure (systems that contain) software?

Lessons of the past 20 years

Erik Poll

Digital Security Group

Radboud University Nijmegen

Radboud Universiteit

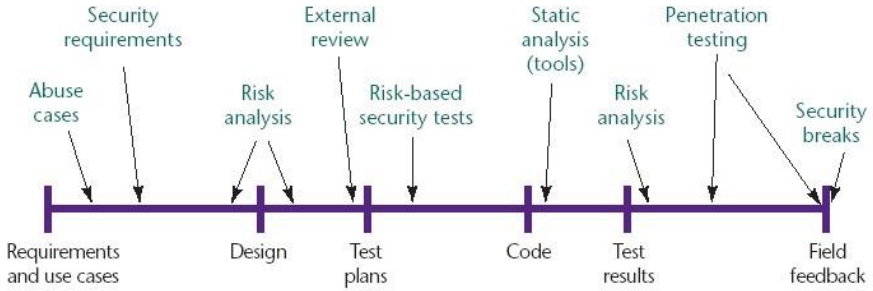
INTERSCT.

“What we should change in 5 to 10 years from now in design, development, etc. of IoT products to be able to deliver products that are more cyber resilient with less human intervention ?”

What has the software industry changed in the past 20 years in terms of design, development, etc. to deliver products that are more secure?

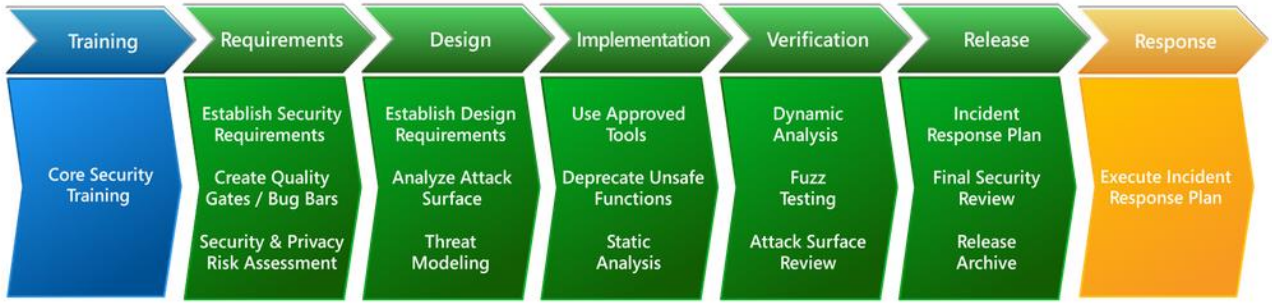
NB ‘resilient’ is just a confusing synonym for ‘secure’

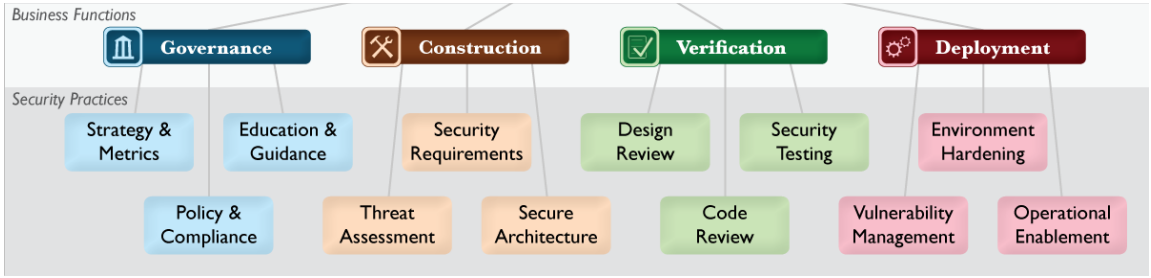
Security: 1) the process – *'methodologies'*



McGraw's Building Security In aka Cigital Touchpoints

Microsoft SDL





OWASP SAMM

Attention to security *throughout* the SLDC
All of these subsume Security by Design, Privacy ~, ~ by Default

Security: 2) the product – *'guidelines'*

OWASP TOP10

MOST DANGEROUS Top 25 CWE SOFTWARE WEAKNESSES

OWASP Application Security Verification Standard (ASVS)

OWASP Standard SCVS Software Component Verification Standard

NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:

Recommendations for Mitigating the Risk of Software Vulnerabilities

CIP centrum informatiebeveiliging en privacybescherming

Grip op Secure Software Development (SSD) Beveiligingseisen

SSDF draws on BSA FSS, BSIMM, CNCF FSSCP, EO14028, IDA SOAR, IR8397, MS SDL, NIST CSF , NIST LABEL, OWASP ASVS, OWAPS SCVS, PCI SSLC, SC AGILE, SC FSSD, SC SIC, SC TPC, SP800-52, SP800-160, SP800-161, SP800-181

What's new?

- Methodologies haven't really changed for 2 decades
  Organisations still struggle to introduce them & then shift left
  - Rise in Agile & DevOps increases need to shift left
  - More acronyms: SAST, DAST, IAST, RASP
  - Shifting *down* is a good way to shift left
- Many many many more security guidelines & requirements
  with OpenCRE as effort to compare/relate them
- More security worries due to 1) increased *code* reuse
  hence SBOMs and SCA (Software Composition Analysis)
  and 2) increased *service* reuse (aka SaaS/cloud APIs/micro-services)
  hence SAST tools for secret scanning
- Improvements in some of the SDLC security steps
  eg fuzzing to test input handling and - shifting left - LangSec to get input handling right from start

What's new?

More regulatory pressure

Sept 2022

May 2023

What's different about IoT ?

- More heterogeneity
  - in platforms, tech stacks, applications, industry traditions, and scale
    - eg. fridge vs nuclear powerplant vs national infrastructures
  - less capable platforms when it comes to security
    - incl. security controls, security monitoring, support for updating, ...

- Clash in engineering traditions
  - Getting used to becoming a software company &
    beginning with introducing secure software methodology