OWASP
Open Web Application Security Project

Tell me stories about your appsec, let's skip the pentest

timur@owasp.org

@timurxyz

- Timur ‘x’ Khrotko, PhD
- x@secmachine.net
- timur@owasp.org
- linkedin.com/in/timurx

O.W.A.S.P.

OWASP
Open Web Application Security Project

- Open Web Application Security Project[s]
  - owasp.org, open-source, non-profit
  - AppSec evangelism
- OWASP ≠ Top 10 (which is an educational project!)
- for production:
  - ASVS V3 (Application Security Verification Standard)
  - SAMM (Software Assurance Maturity Model)
  - Testing Guide (TG)
  - SKF (Security Knowledge Framework)
  - (T10) Proactive Controls
  - ...

OWASP Proactive Controls

C1: Parameterize Queries

C2: Encode Data

C3: Validate All Inputs

C4: Implement Appropriate Access Controls

C5: Establish Identity and Authentication Controls

C6: Protect Data and Privacy

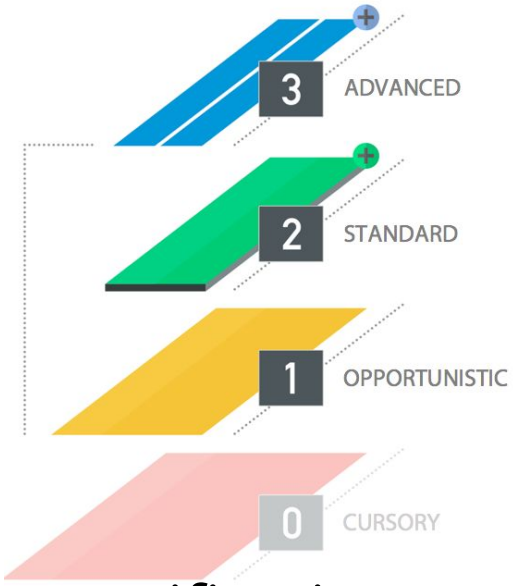
C7: Implement Logging, Error Handling and Intrusion Detection

C8: Leverage Security Features of Frameworks and Security Libraries

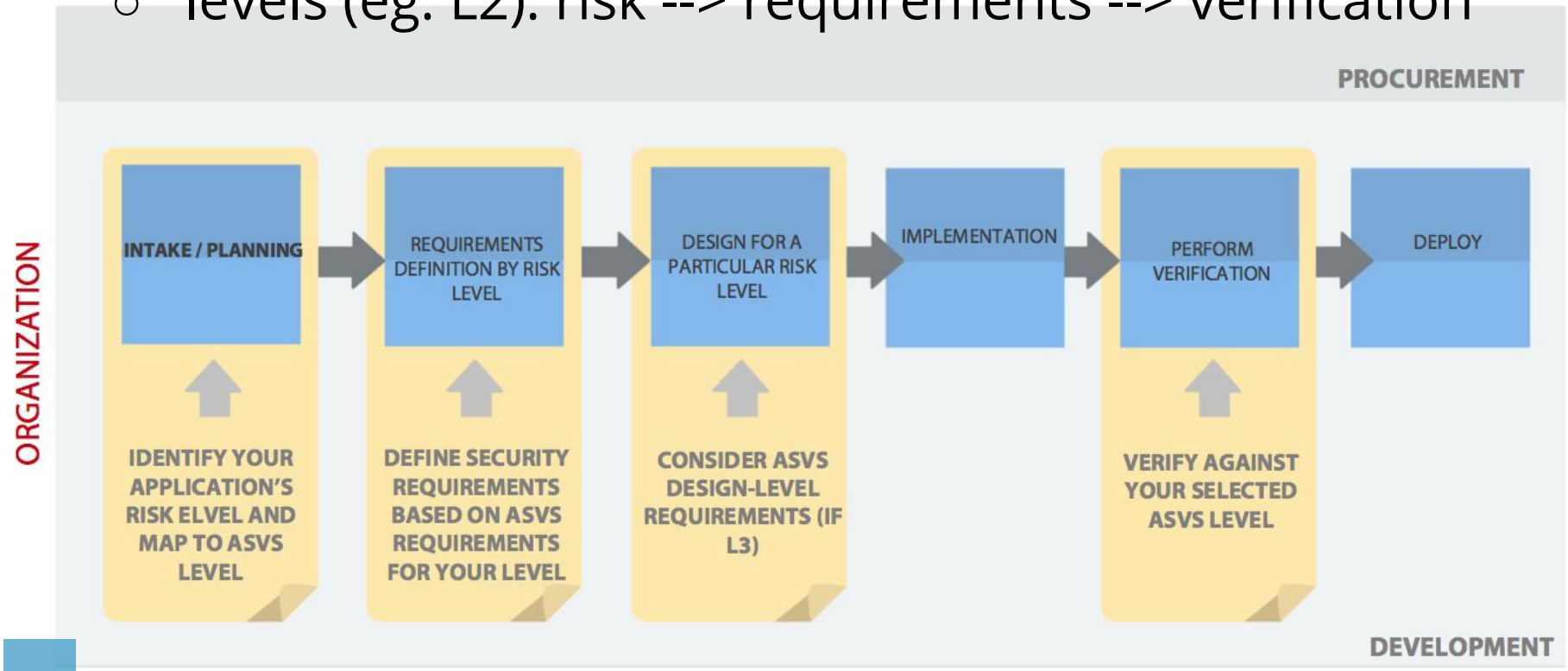
C9: Include Security-Specific Requirements

C10: Design and Architect Security In

OWASP ASVS



- AppSec Verification Standard
  - “security engineering checklist”
  - levels (eg. L2): risk --> requirements --> verification



#sec

- schneier.com/crypto-gram.html
  - “the conceptualism”
- pauldotcom.com (security weekly)
  - beer & cigars
- twit.tv/sn (security now)
  - your grandpas
- Jean Baudrillard: Passwords
- goo.gl/6GGzYq

appsec concepts

- AppSec = QA (**security QA**, SeQA)
  - product + production/dev + support + etc practices
- don't buy it w/o **threat modeling** (risk assessment)
- audit/**testing**
  - va, **vapt**, sast, dast, iast, **code review**, **ci** ...
- **S-SDLC** (SDL) + AS **policy**
  - design, code, configuration, controls, testing (**MS SDL**)
  - patch management, support agreement, sec SLA
- **countermeasures**: filter, isolate, monitor, respond
  - waf, sandboxing, dmz, log audit, id(p)s

untrustable quality

image: deviantart.com, by sefesoft

causes: complexity

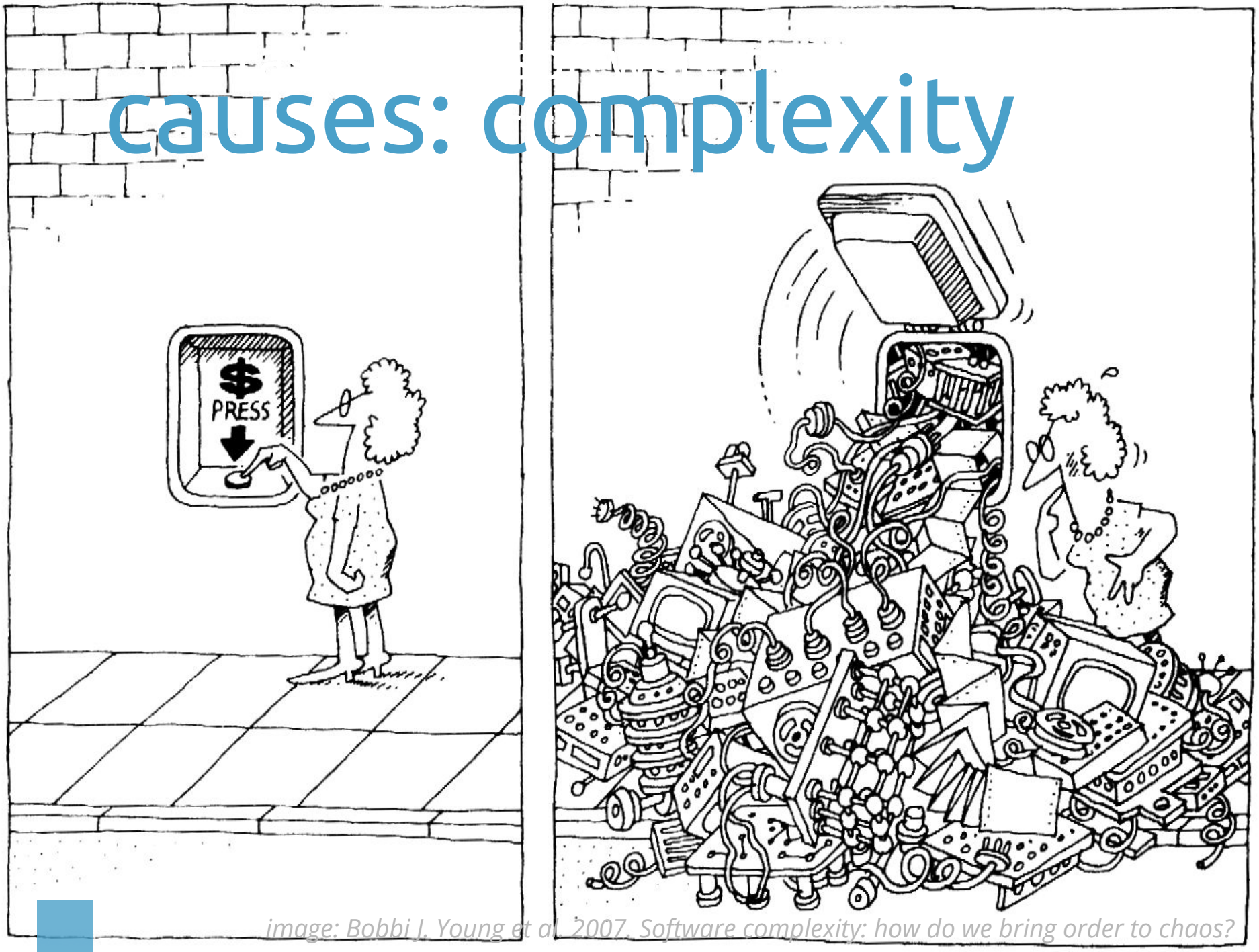


image: Bobbi J. Young et al. 2007. Software complexity: how do we bring order to chaos?

causes: dev culture

image: en.wikipedia, by Klean Denmark

causes: complicity

image: Thomas van de Weerd

causes: appsec mis-mgmt

causes: testing methodologies

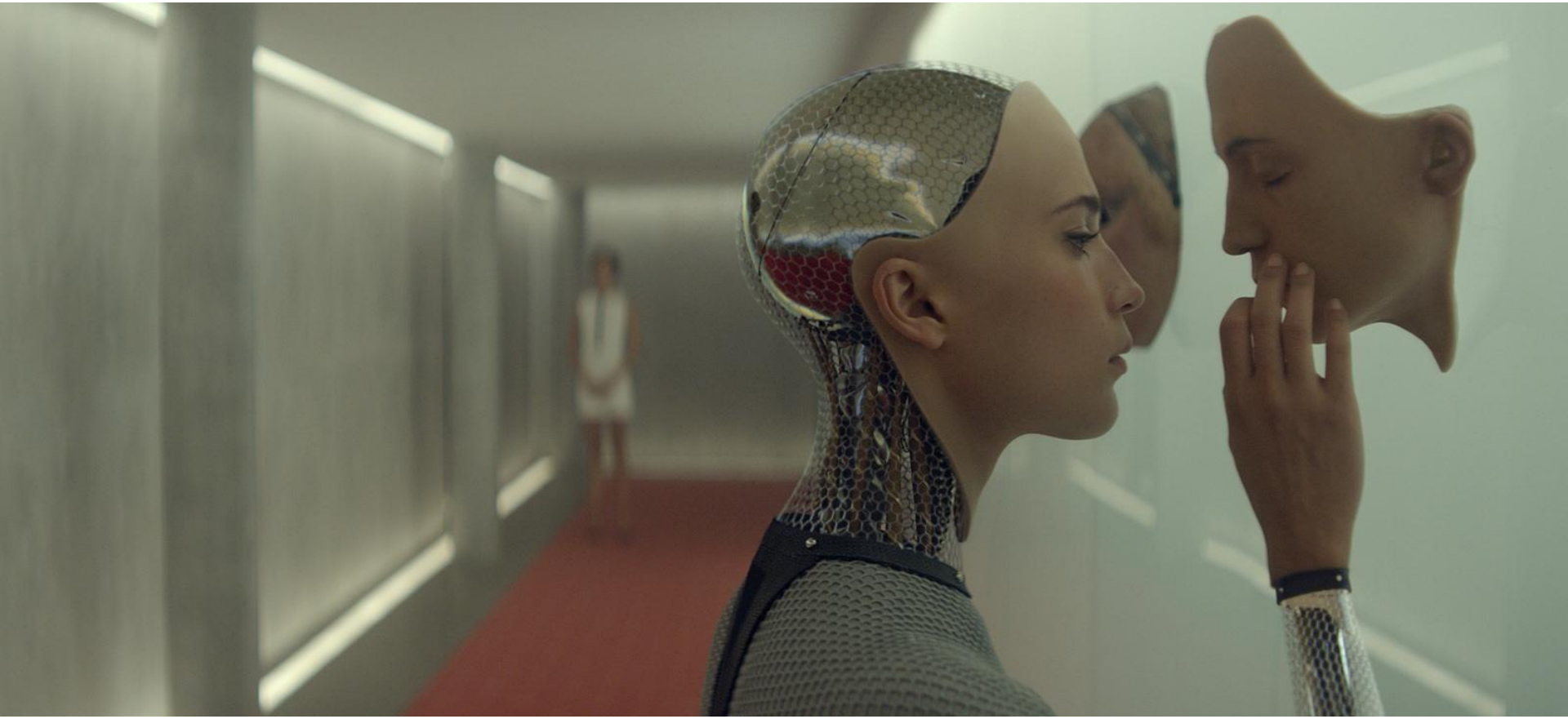


image: flickr.com/photos/bagogames/16153704398

causes: unhelpful eh

image: http://www.eccouncil.org/portals/0/Images/img/icons/ec-council-about-us-banner1.png

let’s skip the pentest/audit!
let’s do narrative interviewing!

why stories

- the root causes of application security
  - are mostly of organizational nature, not technical
- why blackbox/dynamic testing while ...
  - (while you can do static / code review?!)
  - while you can ask!
- testing the product you measure symptoms while ...
  - the roots are in the process
    - see S-SDLC, QA, policies, practices, conflicts
  - the roots are in the manufacturing unit (org)

narrative interview

- use the mature org dev methodology
  - see qualitative interview
- interview managers
  - with care
- interview workers (devs, devops)
- analyse the situation and interpret the findings
- propose changes
  - improving security (S-SDLC) is an iterative process
- speak Utlish

40-20-40

+design +testing

OWASP
Open Web Application
Security Project

did you threat-model?

OWASP
Open Web Application
Security Project

and secure coding course?

OWASP
Open Web Application
Security Project

be tested, trained, coached!

train secure coding

review with devs

audit, VAPT

+ respond to the incidents!

OWASP
Open Web Application
Security Project

resource: cut eh bdgt

- eh (ethical hacking incl webapp/mobile testing) is just another expensive social construct you subscribed to
  - eh culture is just as bad as that of the dev's
- relocate and spend more on:
  - trainings, **secure coding** courses
  - S-SDLC, AppSec policy/**rulebook** enforcement
  - **threat modeling** and IR
- find the **root causes (mostly organizational)**
- use appsec specialists with whom your devs can work constructively (eg. coaching)

resource for the smb-s

- involve a visiting appsec **specialist in critical moments**
- have a **visiting ciso**, at least rarely visiting
- make one resident member of the dev team **security champion** (see MS SDL)
- secure coding **courses**

soon: 16Q1

meetup.com/owasp-hu

twitter.com/owasp_hu

this prezo: goo.gl/6GGzYq