Engineering Security
(Professional Master in Information Security)

PRO.M.IS
security built in

Tony Gorschek
(tony.gorschek@bth.se)

agenda

- Pre-emptive Security through “secure” engineering
  Short on area and Introduction Course

- PROMIS general information
- Courses
- How to apply

(how we see) “security”

How you “build” security into products n services

Engineering

- secure architectures
- security testing
- ”agile” n. security
- secure engineering
- compliance n. regulation
- security n. emergent properties

…

Operations and evolution of prod./services in use

Operation

- monitoring, detection
- forensics
- evolution n. maintenance
- data analytics
- tools/methodology
- input to engineering of next gen. prod./services

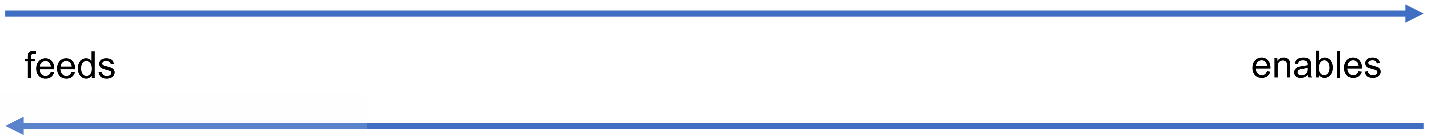
…

Invention of new tech. used to achieve security

Technology

- new protocols
- languages
- algorithms
- standards

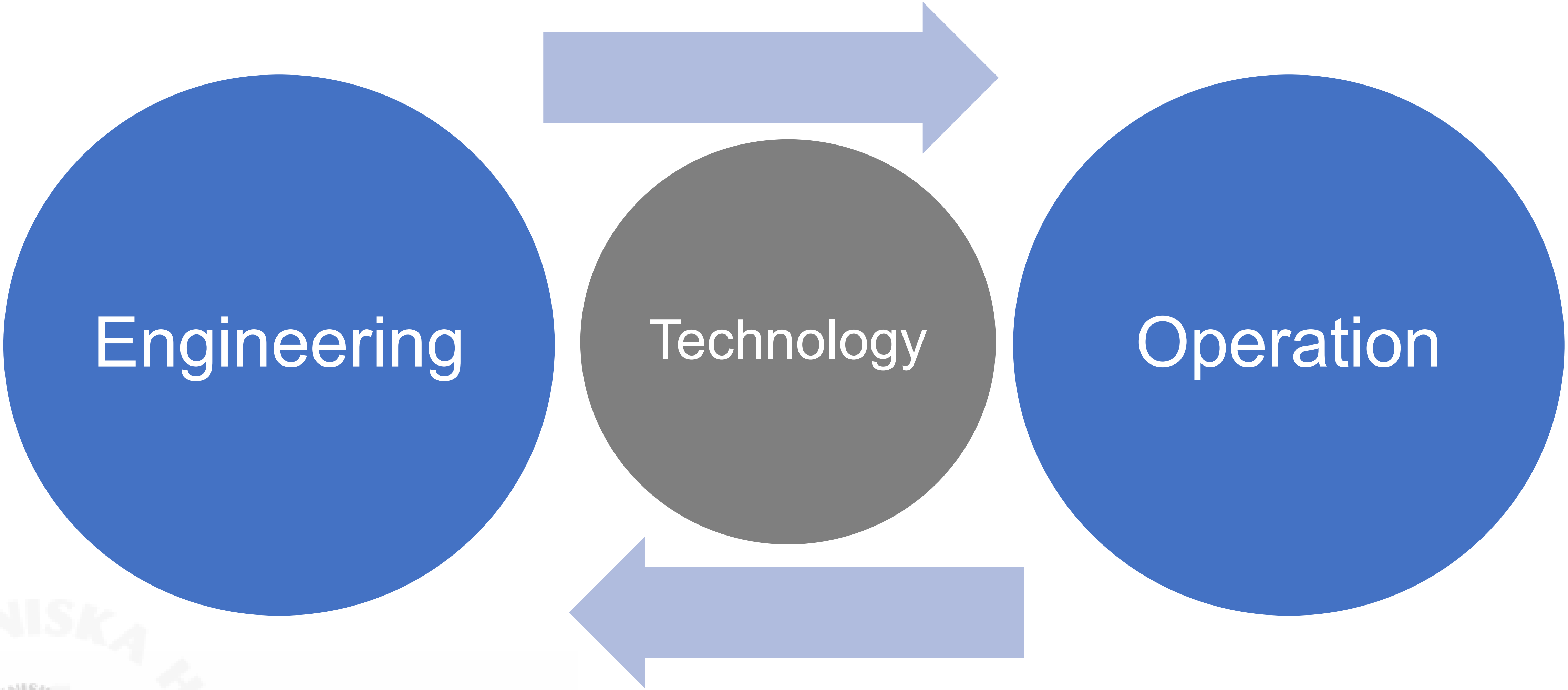
…



feeds

enables

(how we see) “security” (2)



(how we see) “security” (3)

Privacy

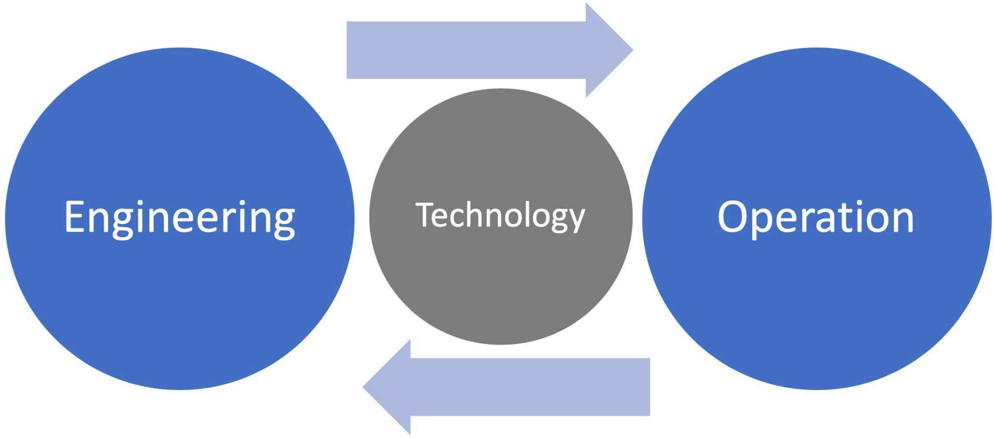
Integrity

Safety

…other

NON-FUNCTIONAL ASPECTS of a SYSTEM

iso-iec-ieee-29148-2011



…other

hardware

law

social engineering

design

human aspects

algorithms

processes

networks

architectures

modeling

automation

ai

tools

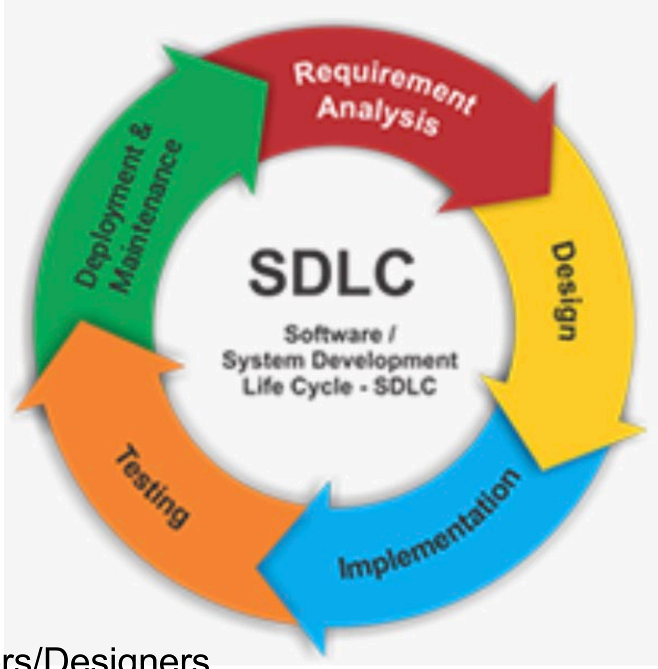
ml

interweb

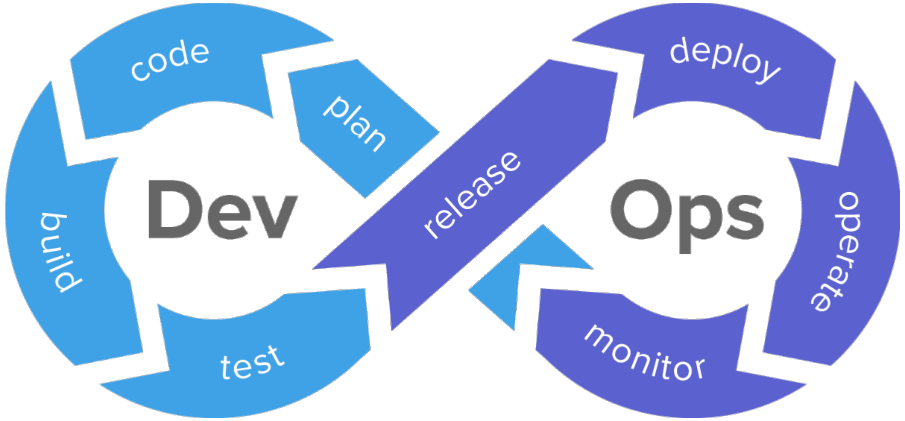
signal processing

so what is “engineering security”?
(the area)

Engineering… (security “built in”…)



…



TARGET GROUP:

- Developers/Testers/Designers…
- Managers
- (semi-) non-technical (e.g. decision makers)

Security in Software-Intensive product and service development

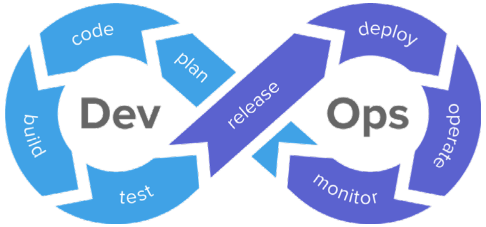
(course) ***introduction*** to “pre-emptive”/”engineering security into a product/service”/security for software engineers…

- Intro to “security” (Engineering – Operative – Technology (or equiv.))
- Security and why critical (how a software engineer convinces a manager to care)
- Security analysis (risk, trade-off, cost, trade-off different non-functional aspects)
- Security and “How to”:
  - Security and “requirements”
  - Use patterns, standards, practices to achieve (more) secure products/services
  - Security and design
  - Security and architectures
  - Security and coding…
  - Security and testing (and automation)

  - SDLC and Security
    - ”Agile” and Security

  - Security and technology (relates to architectures): e.g. intro to cloud based and other “infrastructure” choices and how this affects how the system is designed, developed and deployed…

Requirement Analysis
Design
Implementation
Testing
Deployment & Maintenance
SDLC
Software / System Development Life Cycle - SDLC

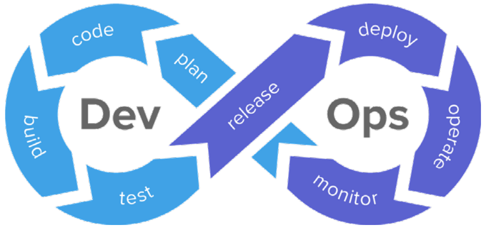


TARGET GROUP:

- Developers
- Managers
- (semi-) non-technical

Security in Software-Intensive product and service development

Requirement Analysis
Design
Implementation
Testing
Deployment & Maintenance
SDLC
Software / System Development Life Cycle - SDLC



TARGET GROUP:

- Developers
- Managers
- (semi-) non-technical

Introduction: MS SDL and OWASP (irt to security) (owast.org)

(requirements/metrics/compliance, tools, testing, design…)

Risk assessment: OWAST (base)

(rating, likelihood, impact, model…)

Threat modeling: overview

(types and tools…)

Third party security implications: overview

(components, in supply chain…)

Security testing: overview

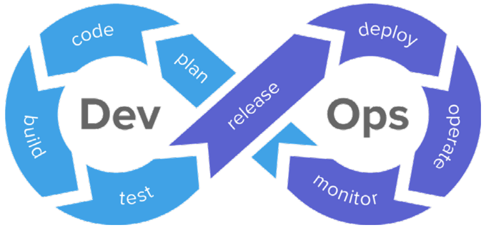
(static, dynamic, pen-test… utilization of machine learning)

Security in Software-Intensive product and service development

Secure programming: Introduction and practice

(
Users/privileges
Files and processes
Session management
Buffer/Numeric overflow…
…)
((demo java, C++))

Requirement Analysis
Design
Implementation
Testing
Deployment & Maintenance
SDLC
Software / System Development Life Cycle - SDLC



Incident response: post release: overview

(planning for operations…)

TARGET GROUP:

- Developers
- Managers
- (semi-) non-technical

Does this sound interesting?

PROMIS (Professional Master in Information Security)

GENERAL FORMAT

Active industrials studying and working at the same time

- *University grade **COURSES for professionals**!*
- *Extend current competence in **an area ("security")***
- Case-based pedagogy (bring your own problems!)
- On-line collaborative didactics
- Distance capability overall incl. lab and tools

Courses under development with input from companies

- Keep relevant and right level (companies advise us)
- <u>**DO YOU want to be part of the companies advising on courses?**</u>
    - CONTACT: Anna Eriksson aes@bth.se

BALLOU
VI ÄR EXPERTER PÅ DRIFT - ÄR NI?
citynetwork
ERICSSON
CYBERCOM GROUP
Outpost24
PROMESTRA
telenor
TRUESEC
advenica
factor10
MaxKompetens
HELP AT WORK

more to come

Courses (3 thus far)

PROMIS (Professional Master in Information Security)

https://promisedu.se/

BALLOU
CITYNETWORK
ERICSSON
CYBERCOM GROUP
Outpost24
PROMESTRA
TRUESEC
telenor
advenica
factor 10
MaxKompetens HELP AT WORK

Software Security (DV2595)
https://www.bth.se/eng/courses/D5816/20202/
Course responsible: Dragos Ilie dragos.ilie@bth.se

- The ability to understand how attackers exploit risky programming practices
- The ability to detect risky programming practices
- The ability to understand and reason about efficiency and limitations in existing software security mechanisms
- The ability to to compare and weight the benefits and costs associated with binary analysis and instrumentation techniques

more to come

Courses (3 thus far)

PROMIS (Professional Master in Information Security)

https://promisedu.se/

Web System Security (DV2596)
https://www.bth.se/eng/courses/D5816/20202/
Course responsible: Anders Carlsson anders.carlsson@bth.se

- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to describe the Common Vulnerability Scoring System (CVSS)
- be able to explain web protocols based on known vulnerabilities and weaknesses
- be able to explain the security aspects when using languages and framework, eg. PHP, JavaScript, and SQL
- be able to explain authentication mechanisms and counter techniques to bypass authentication
- understand Cross-site scripting (XSS) attacks and SQL injections
- be able to explain impacts of one or more combined vulnerabilities that limit or extend the damage given
- be able to install and configure the web server for high security independently
- be able to use and search open vulnerability databases (Common Vulnerability databases CV -DB)
to prevent and find security problems
- be able to use best practice of known design patterns for secure web applications
- be able to utilize OWASP where applicable
- be able to conduct internal and external penetration testing of web applications and related infrastructure)

more to come

Courses (3 thus far)

PROMIS (Professional Master in Information Security)

https://promisedu.se/

Security in Software-intensive products and service development (PA2582)
https://www.bth.se/eng/courses/D5818/20202/
Course responsible: Tony Gorschek
tony.gorschek@bth.se
(actual experts: Alexander Adamov
Volodymyr Tkach

- The ability to understand the technology, operational aspects, and engineering aspects of security - albeit the focus on the course is on "engineering security"
- The ability to plan for "pre-emptive" security in the planning and development of products and services
- The ability to do a risk assessment and take ROI into account
- The ability to develop and use secure architectures that allows for a more stable base for products and services
- The ability to compare and weigh the benefits and costs of non-functional aspects in combination to security
- The ability to estimate how security aspects impact, and are impacted on quality-/non-functional aspects such as usability, performance and maintainability of a product

more to come

PROMIS

HOW TO APPLY

https://promisedu.se/

Spread information about courses @ your company

Entry Requirements

PROMIS courses requires at least 120 credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

Even if you don’t have the formal academic merits, you might be qualified for the course through validation (reell kompetens)! **ASK US!**

Application open until 31st August!

Apply for course:

1. **Create a user account at antagning.se / universityadmission.se**
2. **Search for PROMIS courses by the name Fill in and send in your application**
3. **Upload your required documents (employer’s certificate)**
4. **Reply to any offers of admission**

Questions about the course: contact course responsible(s)
Questions about applying and validation (reell kompetens): : anna.eriksson@bth.se
Visit promisedu.se for more info about courses, application and template for employer’s certificate

further reading

https://dl.acm.org/doi/abs/10.1145/3239235.3267426

https://www.sciencedirect.com/science/article/pii/S0167404818303043

https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1700

https://ieeexplore.ieee.org/abstract/document/7774522

https://ieeexplore.ieee.org/abstract/document/8920644

https://ieeexplore.ieee.org/abstract/document/8543389

https://dl.acm.org/doi/abs/10.1145/2857546.2857552

https://ieeexplore.ieee.org/abstract/document/8993081

https://www.sciencedirect.com/science/article/abs/pii/S0920548916301155

https://aisel.aisnet.org/jise/vol13/iss3/3/

https://ieeexplore.ieee.org/abstract/document/7516832

https://www.amazon.com/Secure-Software-Design-Theodor-Richardson/dp/1449626327

Q*n*A