Matchmaking event artificiële intelligentie (AI) & cybersecurity (CS)

9 maart 2020 - Lamot Mechelen

Vlaanderen
is ondernemen

AGENTSCHAP
INNOVEREN & ONDERNEMEN

ICON DiskMan: A testimonial on identity management and authentication

Davy Preuveneers

KU Leuven

AGENTSCHAP
INNOVEREN & ONDERNEMEN

DistriNet

ICON DiskMan: A testimonial on identity management and authentication

Davy Preuveneers

Davy.Preuveneers@cs.kuleuven.be

DistriNet

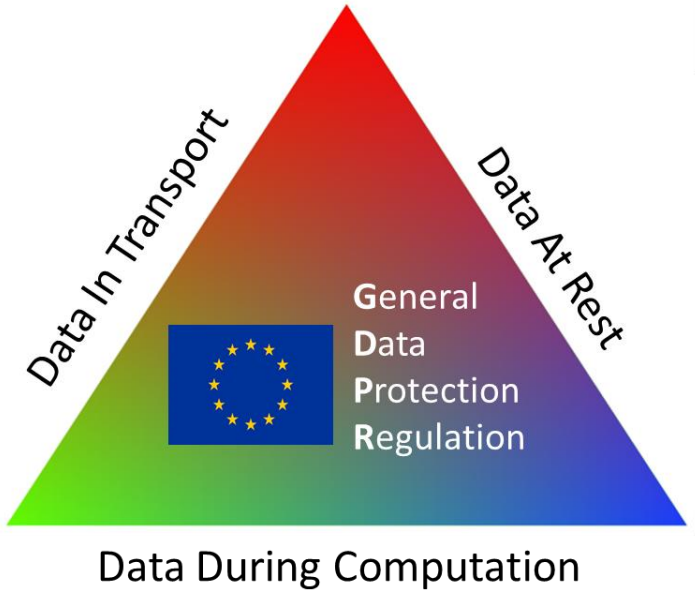
Lamot, March 9, Mechelen

ICON DiskMan: Scope within cybersecurity program

TRACK 02

Security Services

- Reusable security specific building blocks
  - **Identity and authentication**
  - Authorization and audit
- Secure data processing
- Policy and regulation



ICON DiskMan: Authentication is critical security layer

› Low-friction and near real-time authentication experience for mobile consumers

› Conference systems with multi-level access control and stronger guarantees for remote participants/interpreters

› Tailored solutions on top of reusable IAM platform for its customers in need of mobile identity management

ICON DiskMan: The solution

SONY

televic conference

Multi-factor

Device-to-Device authentication

Context, risks and trust models

DistriNet

COSIC

Mobile Access Middleware

- User context
- Behavioral fingerprints
- Trust delegation
- Lightweight / threshold crypto

User-friendly collaborative user authentication

SONY

Protect access to consumer content

Extend OpenID Connect / OpenUMA
Privacy preserving authentication

IS4U identity & access management

DistriNet

Enhanced IAM

- Collaborative, multi-factor
- Dynamic, risk-adaptive

Base IAM system

- User provisioning
- Policy-based access control

televic conference

Protect access to online services and enterprise assets

DistriNet

Mission for identity management and authentication

Secure identity management and authentication solutions that *increase transparency and privacy* while *limiting user friction*

- **Focus:**
  - Reduce security risks: multiple authentication factors, behaviometrics
  - Manage security/usability trade-offs: continuous and context-based authentication factors, e.g. location, proximity
  - Privacy-by-design approach and privacy analysis of existing IAM

Thank you!

https://distrinet.cs.kuleuven.be/

DataBlinder data protection middleware: An application-level, distributed middleware for flexible data protection

Bert Lagaisse

Industrial research manager

KU Leuven

AGENTSCHAP
INNOVEREN & ONDERNEMEN

DistriNet

KU LEUVEN

DataBlinder data protection middleware:

An application-level, distributed middleware for flexible data protection

Bert Lagaisse,
Industrial research manager

DistriNet, KU Leuven

Outsourcing data and computation on data to the cloud ?
Attacker model: “Cloud provider is honest …but curious”

→ Or curious third parties …

SPIEGEL ONLINE SPIEGEL+ Sign in

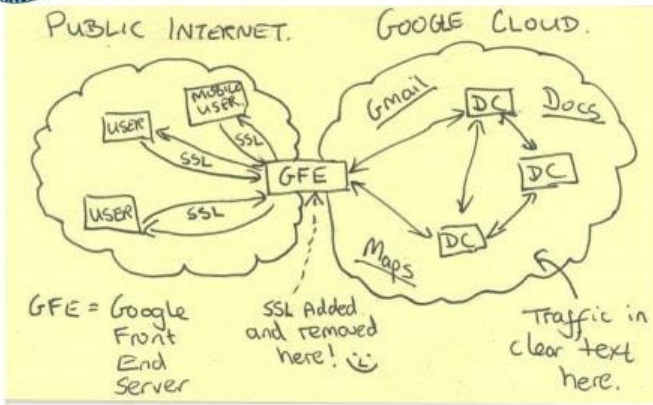
Belgacom Attack

Britain's GCHQ Hacked Belgian Telecoms Firm

A cyber attack on Belgacom raised considerable attention last week. Documents leaked by Edward Snowden and seen by SPIEGEL indicate that Britain's GCHQ intelligence agency was responsible for the attack.

TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

KU LEUVEN

State of practice vs state of the art in crypto

State of practice (AES, RSA)

- Data encryption at rest/transmission
- No search or computation on encrypted data

Foreshadow: Extracting the Keys to the Intel SGX Kingdom

Challenging examples …

- Find patient admitted on 12/05/2012
- Find patient's oncology visits in date range
- Average heart rate of patient
- Number of refills of doxycycline on a patient

State of the art: operate on encrypted data

- Searchable encryption (SSE, …)
  - Search in encrypted text, secure indexes
- Property preserving encryption
  - OPE, ORE, … (order for range queries)
- Homomorphic encryption (x , +)
  - Paillier, ElGamal, SHE, FHE, BGV, TFHE,

Trade-off: no one-size fits-all

KU LEUVEN

ICON-Seclosed contributions to DataBlinder

Crypto agility: There is no one-size-fits-all protection tactic

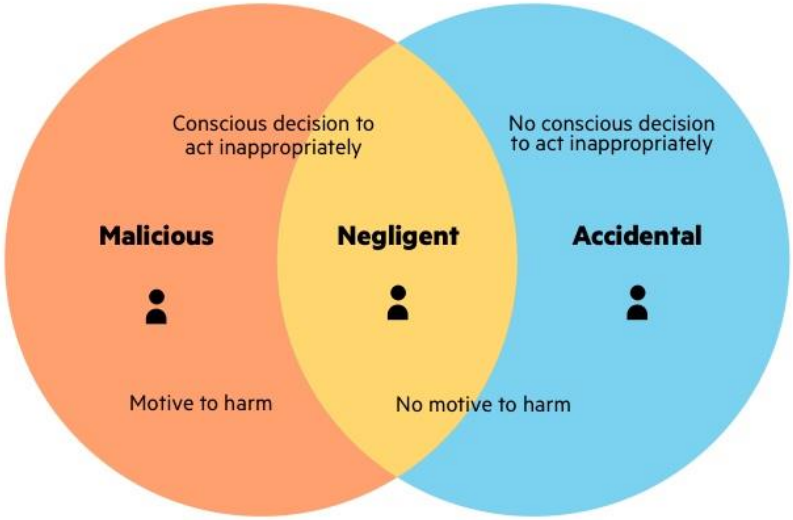
- Configurable per field on a (semi)-structured data item (document)
- Trade-off support: function vs performance vs level of data protection
- Evolvability of cryptographic tactics (attacks and research progress)

Bridge between cryptographic developers and application

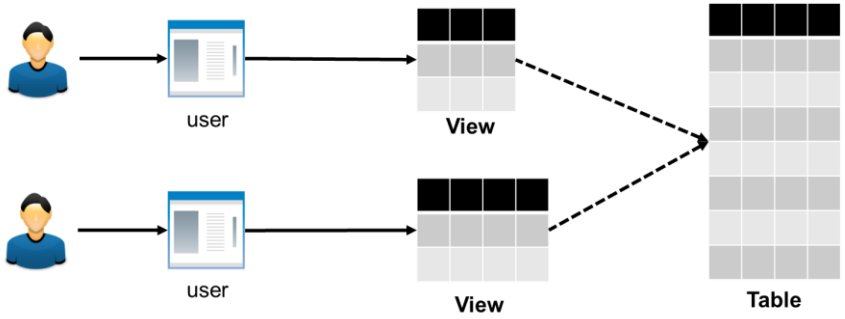
- Right level of Abstraction: Cryptographic implementations are complex and error prone
- Implementation support: to develop distributed cryptographic tactics and protocols
- Pluggability: Hard to develop and integrate in an existing application software stack

Data protections vs Insider threat

Malicious, negligent or accidental

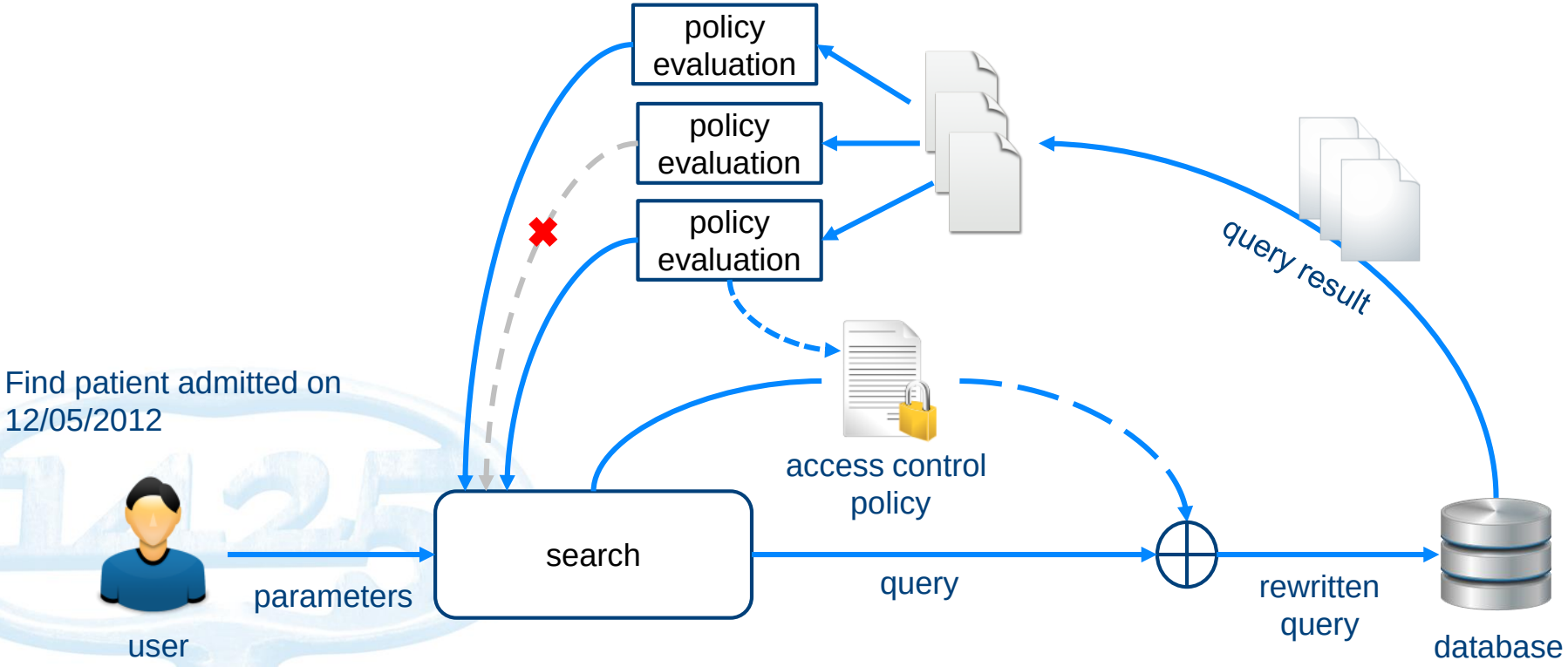


In-database access control models too limited



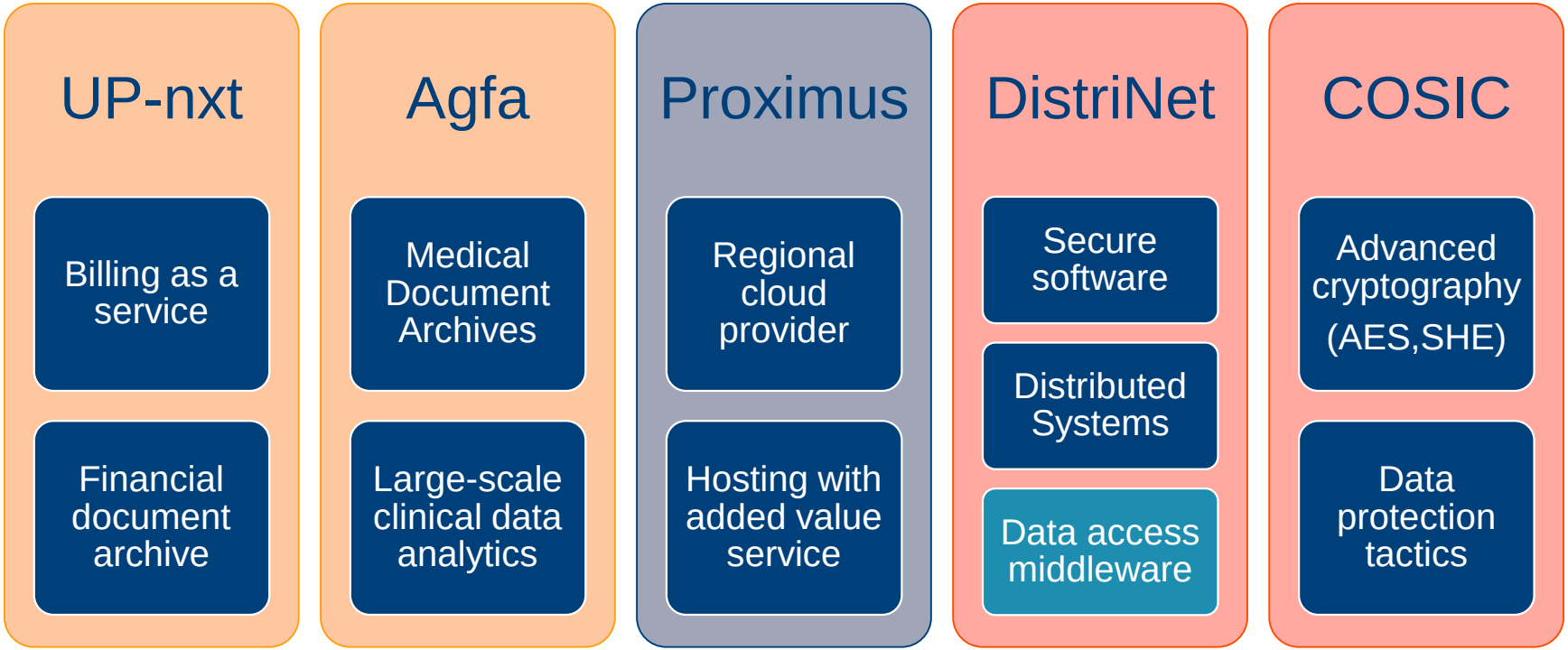
KU LEUVEN

ICON-Sequoia Approach: ABAC, Policy-based access control & query rewriting



KU LEUVEN

Example consortium:
Common tech problem, multiple application cases



Secure Development Lifecycle (SDL)

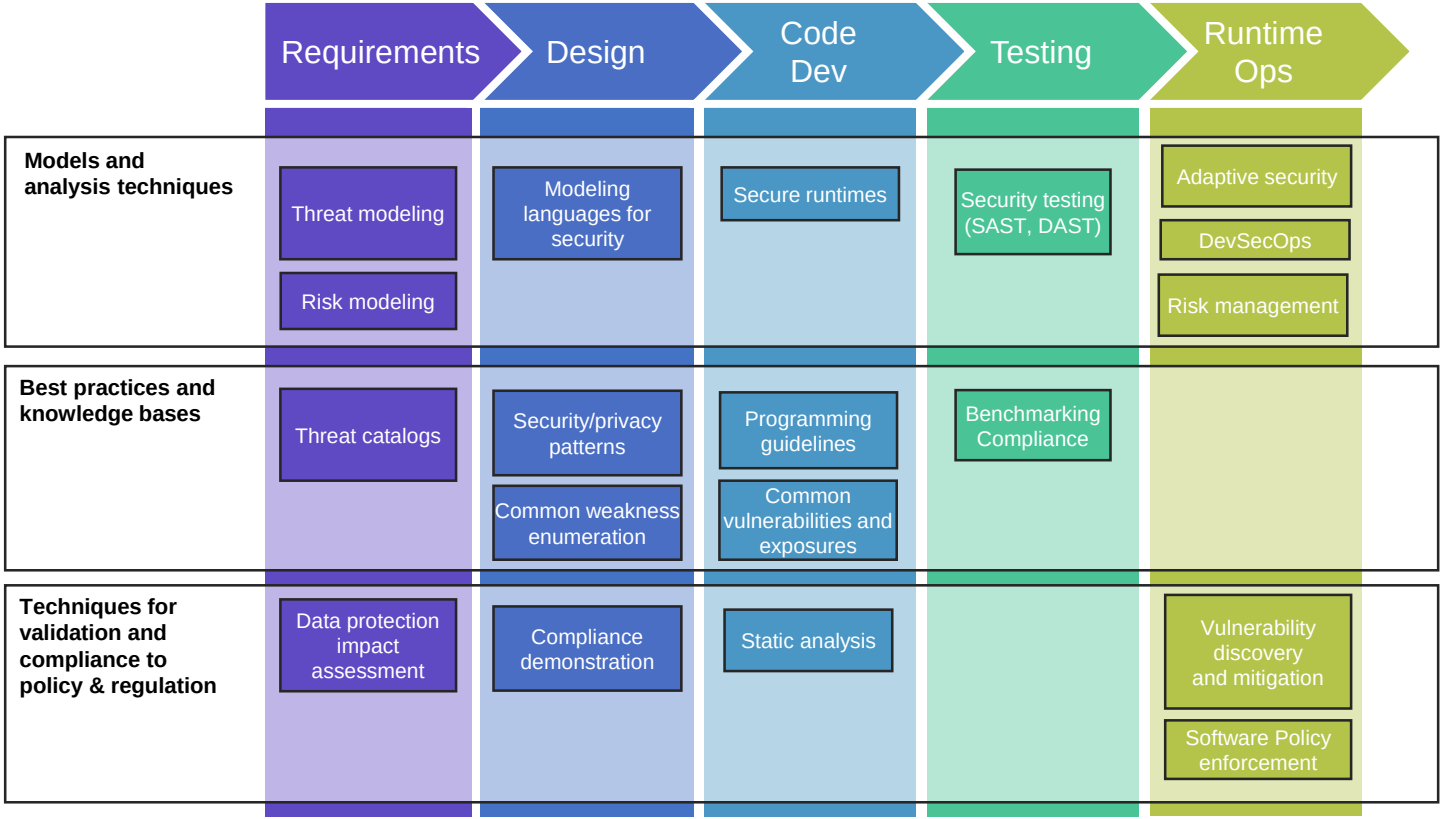
Dimitri Van Landuyt, PhD

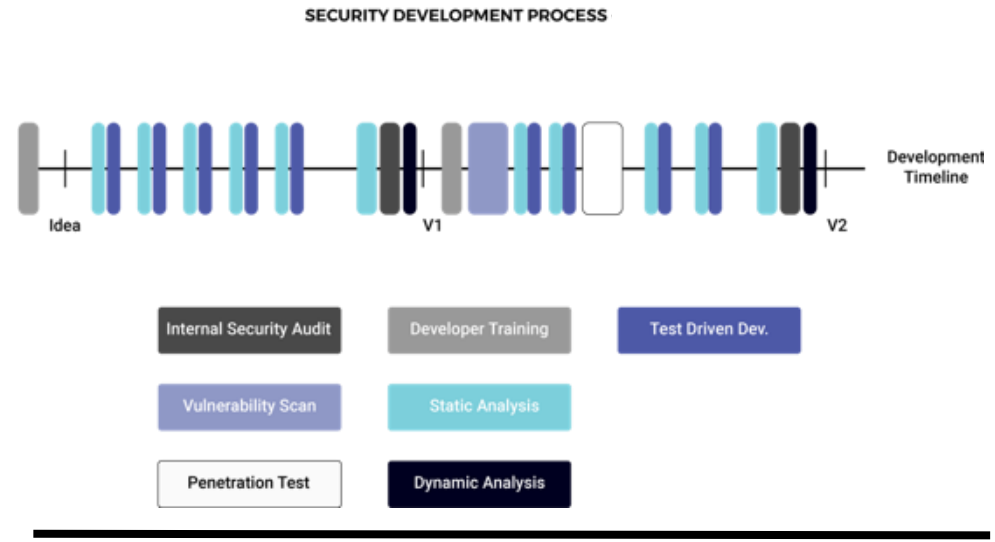
Research Manager in Software Engineering

imec-DistriNet, KU Leuven

AGENTSCHAP
INNOVEREN & ONDERNEMEN

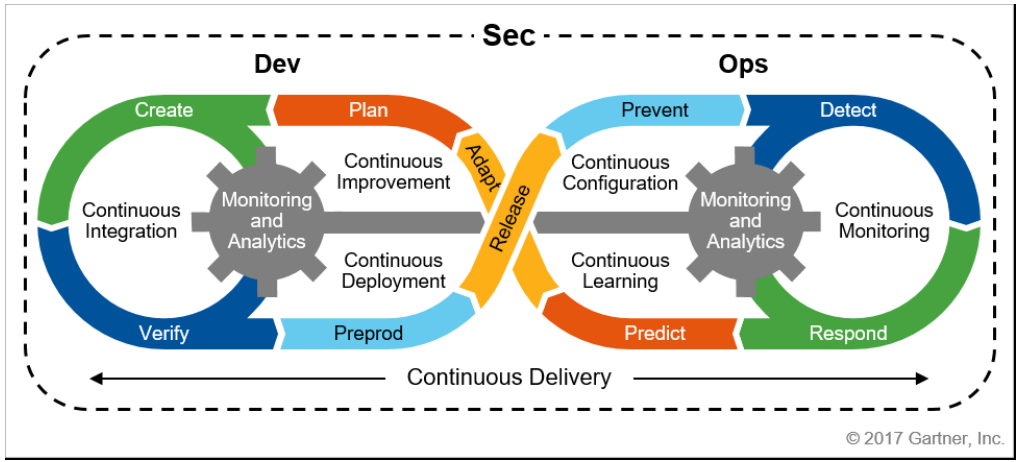
Secure Development Lifecycle (SDL)





[current security process]

- All security investments focus on active development
- Rigorous process involving established practices
- Outcome of security testing presents a snapshot in time



[evolved security process]

- Operational context strongly influences next development cycles
- Security testing no longer results in a “still-frame view” but a live video feed; verify, detect and continuous monitoring

Continuous monitoring/continuous security testing

- Integration of operational aspects into development context + vice versa
- Model-supported analysis activities, focus on automation
- Risk and assurance based
- Adaptive aspects of security

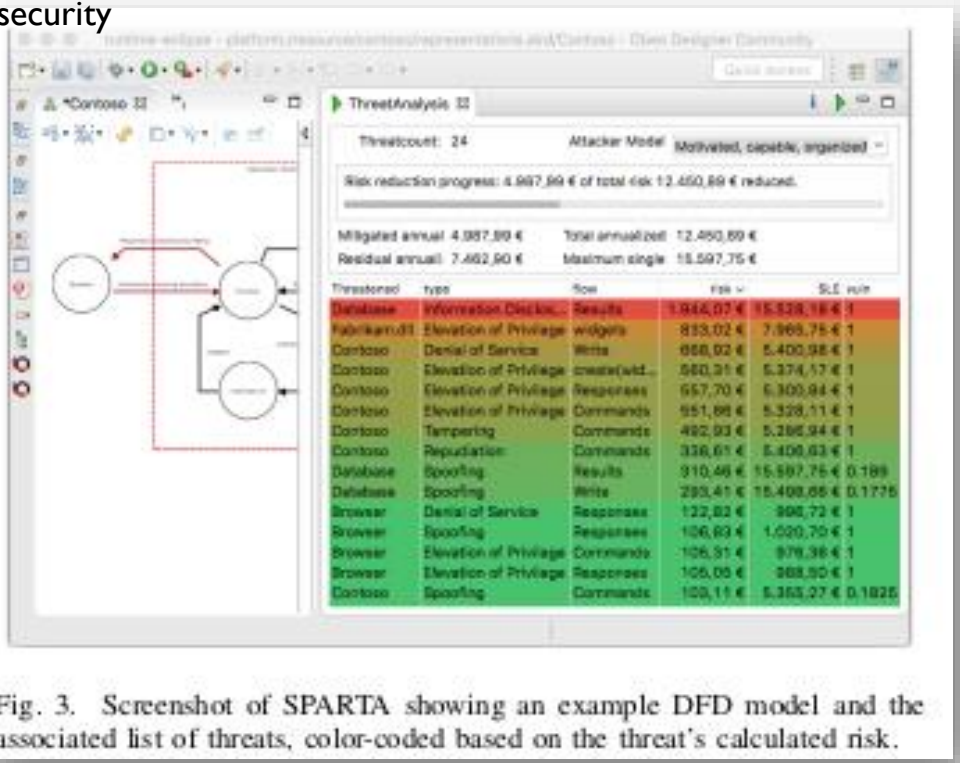
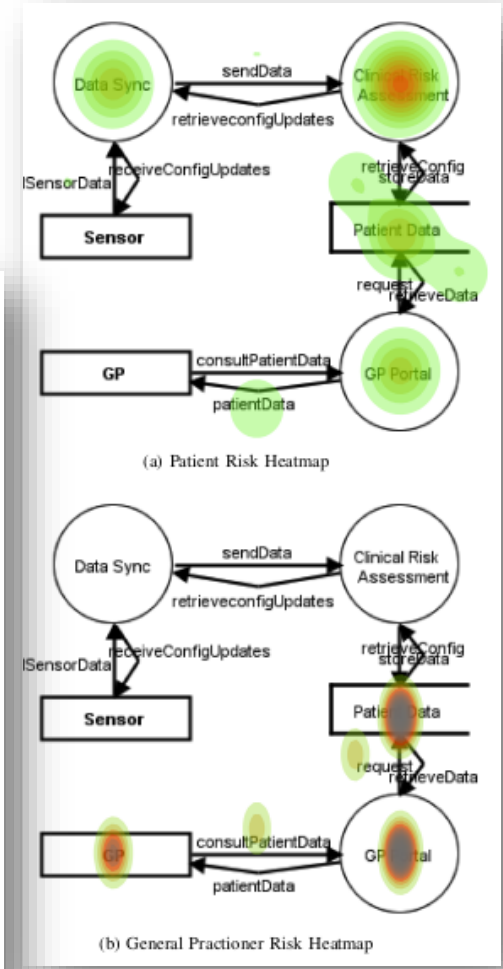


Fig. 3. Screenshot of SPARTA showing an example DFD model and the associated list of threats, color-coded based on the threat's calculated risk.



Data protection /privacy risk

Securing Software at the Application Level

Florian Myter

Business Developer

Software Languages Lab / VUB

AGENTSCHAP
INNOVEREN & ONDERNEMEN

Static Application Security Testing

Dynamic Application Security Testing

Run-time Application Security Protection

Run-time Complex Event Detection

VUB

SOFTWARE LANGUAGES LAB

Florian Myter
fmyter@vub.be

Security and safety enhanced co-design of tomorrows cyber-physical control systems!

Klaas Gadeyne
Research Fellow
Flanders' Make

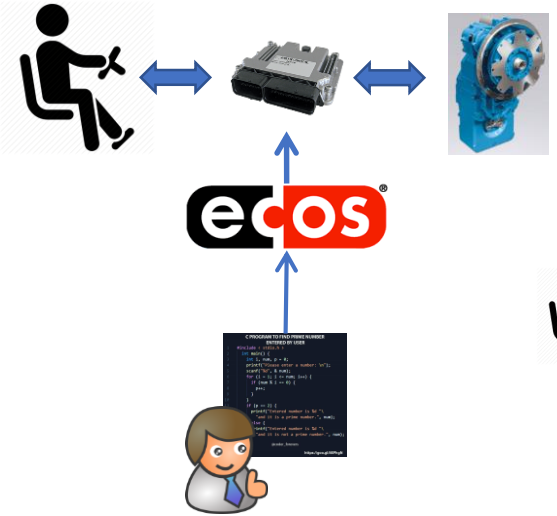
AGENTSCHAP
INNOVEREN & ONDERNEMEN

FLANDERS MAKE
MANUFACTURING INNOVATION NETWORK

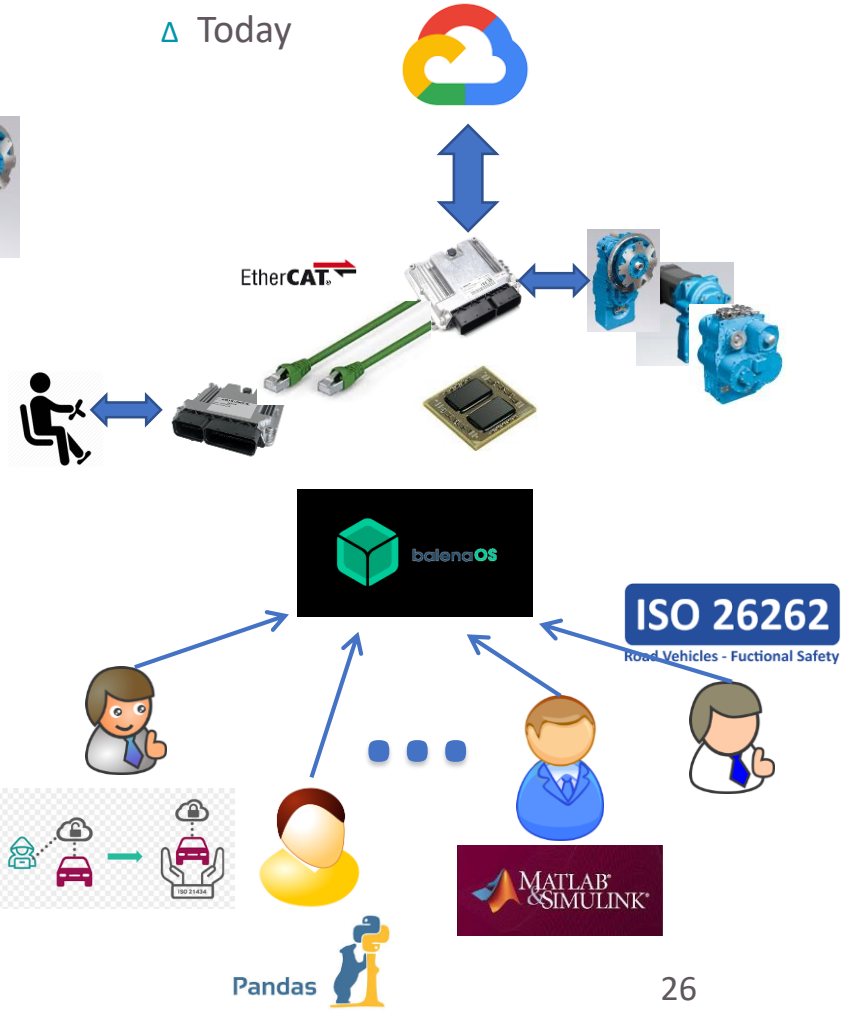
SECURITY AND SAFETY ENHANCED CO-DESIGN OF TOMORROWS CYBER-PHYSICAL CONTROL SYSTEMS!

KLAAS GADEYNE

- Back then



- Today



- How to further improve the **co-design** of todays hypercomplex cyber-physical control systems taking into account safety and security

IoT device security

Michael Dieudonne

Keysight Technologies Belgium

AGENTSCHAP
INNOVEREN & ONDERNEMEN

A Brief History of Keysight

1939–1998: Hewlett-Packard years

A company founded on electronic measurement innovation

1999–2013: Agilent Technologies years

Spun off from HP, Agilent became the World's Premier Measurement Company

In September 2013, it announced the spinoff of its electronic measurement business

2014+: Keysight years

On November 1, Keysight became an independent company focused on the electronic measurement industry

IoT devices security

- IoT applicaties hebben 2 gezichten:
  - Goedkoop en niet belangrijk systeem => I don’t care
  - Duur en/of belangrijk systeem => I do care
- Als het belangrijk is, wil je ‘zeker’ zijn dat het niet kan aangevallen worden
- Security test is niet simpel… (Pen test, side Chanel…) kan het simpeler gemaakt worden? Kan het toegankelijker gemaakt worden voor niet experten?
- Project zou methodologieën onderzoeken om IoT security test te vergemakkelijken en te automatiseren.
  Kan het zo simpel worden dat het voor alle IoT devices gebruikt kan worden?
- Wie zoeken we: bedrijven die in het IoT security interesse hebben, van device maker tot system integrators.

Contact

- Michael Dieudonné
  Keysight Technologies Belgium
  michael_dieudonne@keysight.com

Voorstelling bedrijven in de zaal

AGENTSCHAP
INNOVEREN & ONDERNEMEN

Ronde tafels

Tafel 1 Secure Software & Applications
Tafel 2 Security Services
Tafel 3 System & infrastructure security
Tafel 4 Security building blocks & secure hardware

AGENTSCHAP
INNOVEREN & ONDERNEMEN