about the
DistriNet Master Thesis

Wouter Joosen
Overview in light of 2017-2018

Distributed Software - Software Security – Software Engineering
Overview - Guide

Part I: What can we offer?
- High-level overview of the research space
- Sorts and types of MsC theses

Part II: Who is supervising the thesis?

Part III: Illustrations (a selection(!) of thesis topics)

Part IV: Some final advise
PART I
What can we offer?

Research **Domains**, Collaborations & partnerships, **Trends** that drive the MsC. program
In a Nutshell

Distributed Software

- Autonomic, self-management of distributed systems (e.g. in traffic, in factories)
- Configuration and management of networks, infrastructures, cloud platforms (DevOps)
- Dynamic and runtime modification of the software systems in the Internet (Adaptation)

Secure Software

- Secure Programming Languages
- Software Verification and Certification (formal systems)
- Engineering for Privacy
- Security Analytics (ML)
- Security Services: Audit, Access Control...
- Web and Mobile security, IoT
- Network and system-level Security

Software Engineering

- Programming Languages, Verification
- Requirements Engineering, Architecture
- Modeling and Automation
Secure Software

- Programming languages
- System level languages
- Architectures and patterns
- Methodology
- Middleware
- Network and mobile security
- Specific requirements: Privacy, ...

Distributed Software

- Adaptability in middleware
- Service Customization
- Configuration
- Deployment
- Decentralization
- Autonomic systems

Software Engineering (SWEBOK all)
Background: a Project centric organization

- Typically about 25-30 funded projects (1):
  - Fundamental Research at the Core
    e.g. C1 TENSE: Secure Software for embedded Systems; GOA ADDIS: Adaptive Distributed Software
  - Strategic basic research or industry
    applying the above in cloud settings, in IoT environments, …
  - Applied research
    often with industry
  - Contract research

- Spectrum ranging from theory to practice (2), possibly/often applications

- A note on collaboration with companies: welcome!
A full spectrum of research activities

- Demand-driven research in synergy with fundamental, basic, and collaborative research
- Up to the offering of value-added services
  - to sense needs in the market and spot market opportunities
  - to understand and monetize valorization potential of internal expertise
  - test sustainability of specific services
What Does it Mean?

- Demand-driven research in synergy with fundamental, basic, and collaborative research

Possible areas of an MsC thesis, Always research oriented!
Colaboration with industry and with the public sector: some names
Applied Research ...

- Applications domains addressing essential themes for modern society:
  - Smart City
  - Smart Crowds
  - e-Health
  - Logistics and Traffic, Industry 4.0
  - Financial services and FinTech
  - New media,…

- Applied by making new concepts and innovative theoretical research practical in tangible prototypes
  - e.g. implementation of new web browser technology, browser extensions,
  - …
1. Content: which subdomain(s) are of interest to you? (complex)
   A. Security, Distributed Software and Software Engineering
   B. but also subdomains
   C. and also orthogonal themes in other “clusters”:
      e.g. Programming Languages, …

2. Type of work
   A. Theoretical, applied or both?
   B. Innovative ideas: how are these evaluated?
   C. Driven by a real application (domain)?

3. Options:
   A. (optionally) with industry?
   B. (optionally) interdisciplinary? – e.g. business or legal aspects…
      -- also technical CS aspects such as Machine Learning
TRENDS – Secure Software

- Focus on mobile devices!
- Client-side security (including privacy): from web clients (browser security) to app-security
- Hybrid solutions that make the trade-off between hard- and software
- Privacy (EU: GDPR: obligatory as of 2018!)
- Security in programming languages (secure compilation, object capabilities, interplay with FP)
- Cyber-security & cyber-crime:
  - Including systematic observation and analysis of threats, vulnerabilities and malware
- System and middleware security in cloud, IoT and automotive
TRENDS – Distributed Software

additional and/or emerging complexity in adaptive systems...

1. Cloud Computing (tenant and service provider)
2. Federated & Hybrid Data Stores, e.g. supporting Big Data
3. Support for Business Processes (Work flow based applications)
4. IoT Platforms for robust applications, embracing new network technologies (e.g. LoRa)

And (already mentioned)...
A. Adaptive systems
B. Autonomic systems
C. DevOps: from system and software development to management, configuration and system administration
TRENDS – Software Engineering

- Automated *code verification* maturing to become applicable real world applications.

- Property *analysis* at the level of high-level artifacts: software architecture.

- Prediction of properties based on practical *machine-learning* solutions.

- Domain Specific Languages!
  - Sub domain of *programming language research*
  - Examples: drivers for embedded devices, policy languages for secure deployment,....
PART II
Who offers the topics?

10 Faculty members (SEE PART III)
8 Research Experts/Managers, >10 Postdocs
See  https://distrinet.cs.kuleuven.be/people  !!!!!!!!
DistriNet Faculty Members

Bart De Decker
• Anonymity
• Pseudonymity
• Privacy Protection

Danny Hughes
• IoT
• Middleware
• Low-level Networking

Bart Jacobs
• Software Verification

Eric Steegmans
• Model Driven Software engineering
• early stages of the Software Life Cycle

Bruno Crispo
• Behavioural Biometrics
• Mobile App Security
• Malware Detection
• Real-time embedded systems security

Frank Piessens
• Security Architectures
• End-to-end Security
• ..

Tom Holvoet
• UAVs (Drones)
• AGVs
• Smart Power Grids
• Logistics

Wouter Joosen
• Cloud Computing Platforms
• Software Architecture
• Software Security

Yolande Berbers
• Mobile Cloud Applications
• Context-Aware Computing
DistriNet Faculty Members
@ other KU Leuven locations

Vincent Naessens
(Technologiecampussen Gent en Aalst)

Jeroen Boydens
(Technologiecampus Oostende)

Danny Weyns
(Campus Kulak Kortrijk)
PART III
Illustrations

Message from the promoters …
& examples of thesis topics
Focus on **mobile cloud applications**: applications that run partially on mobile devices and partially in the cloud

**Context-aware computing:**
- in band interpretation of context information to deliver custom solutions
- Context: environment, device(s) or history and other data in the back-end (cloud)
Autonomic Systems
• UAVs(*), AGVs, Smart Power Grids, Logistics
• Key aspects:
  → software engineering
    • of autonomous behavior
    • of virtual environment for sensor fusion
  → algorithmic
    • routing, task allocation, …

Game Theory & Security

(*) Drones!
The creation of distributed software systems that allow for **sensing of the physical world** and **control over physical processes**

Based upon tiny embedded devices - the Internet of Things

Interests range from the middleware to low-level networking
Driver: Sam Michiels

115 Optimised software deployment for the IoT
126 A Deep Packet Firewall for LoRa
Prof. Bruno Crispo - Themes

Behavioural Biometrics
How to autenticates to devices that do not have a keyboard? Shall we ever manage to get rid of passwords and pins?

Mobile App Security
Analysis of legitimate applications and detection of potential dangerous ones

Malware Detection
How to prevent zero-day attacks?

Real-time embedded systems security
Small, Fast yet Secure
One theme: **security architecture for the IoT** i.e. robust execution of trusted code in an untrusted environment

Another theme: **end-to-end security for multi-tier applications** (e.g. in the Tearless project)

Further: **App Security & Secure compilation** (language technology)
Sample Topics:
Secure Software for Control Systems

105 Sancus @ vatiCAN: Improving Software Security in Automotive Bus Systems
110 Secure Trust Assessment for the Internet of Things
107 Static Verification of Sancus Modules

Driver: Jan-Tobias Mühlberg
Focus: **Anonymity, Pseudonymity & Privacy protection**

- Crypto building blocks ➔ privacy protecting (sub)systems
  - Identity Management
  - Access Control
  - Reputation, Rewards, …
- Support ➔ Software Developer
  - Middleware
Sample Topics: Anonymity, Pseudonymity & Privacy Protection

- Security of IoT Devices: using virtualization to create a Software “Root of Trust”
- Design and Development of Secure Middleware in Real-time
One Theme: **Cloud Computing Platforms**
- Access control for Google-scale applications (security)
- Automating the rollout of BigData NoSQL systems
- Adaptability of SaaS-environments (DevOps)

Another Theme: **Software Architecture & Security** (security in early stages)
- Vulnerability prediction, leveraging on machine learning and data mining
- Automating the selection of patterns during requirements engineering and software architecture and design
Sample Topics:
Adaptive performance isolation of multi-tenant SaaS by means of container orchestration

- Support for adaptive performance isolation of multi-tenant SaaS by means of container orchestration
- SLA management for stateful applications using container orchestration
- Design and implementation of a generic feature toggle management system

**Driver:** Eddy Truyen
Sample Topics: Multi-tenancy & Multi-cloud

- Smart Multi-tenant Webserver with Webframework for Saas in the Cloud
- Multi-tenancy Support voor Webapp Devs
- Multi-cloud Decentralization of Large-scale Data Queries and Data Analysis

Driver: Bert Lagaisse
Sample Topics: Security Policies, Authentication & Authorization

- Security Policies for ad hoc Federations
- Adversarial machine learning for behavioral authentication
- Authorization as a Workflow in the Context of Healthcare Systems

**Driver: Davy Preuveneers**
Sample Topics: Web Security

- Automated discovery of timing attacks in web browsers
- Patch it like it's hot - exploring online patching practices
- Leveraging collaborative security to thwart cross-site attacks
Software Verification for safety, security and robustness

- Verifying the FreeRTOS real-time OS
  - FreeRTOS is een open source embedded real-time operating system
- Automatic Generation of Loop Invariants
- Verification of floating point computations
Sample Topics: Software Verification

101 Formal verification of floating-point code
102 Formal verification of cryptographic computations in OpenSSL
106 Verifying Entry and Exit (-Stubs to Sancus Modules)
107 Static Verification of Sancus Modules
108 Verified FreeRTOS: Case Studies in Software Verification
Software Engineering research

- Model driven software engineering
- Early stages of the software life cycle: requirements engineering, models and architectures
PART IV – some final advise

Talk to supervisors and coaches, do not hesitate to propose a thesis topic if you wish…
Decisions and choices

1. Content: which subdomain(s) are of interest to you? (complex)
   A. Security, Distributed Software and Software Engineering
   B. but also subdomains
   C. and also orthogonal; clusters: e.g. Programming Languages, …

2. Type of work?
   A. Theoretical, applied or both?
   B. Innovative ideas: how are these evaluated?
   C. Driven by a real application (domain)?

3. Optionally:
   A. with industry?
   B. interdisciplinary? (also outside the scope of DistriNet!!!)
      - e.g. business or legal aspects…
      - e.g. AI aspects such as Machine Learning
Important!

Note 1: many of the proposed themes may not be covered in the set of online published subjects, yet 😊.

Note 2: you can always contact one of the promoters, research managers or research experts for a direct dialogue.
One more: this may really affect your career!

*(inside or outside of the research world of KU Leuven)*
Thank You!

Questions?