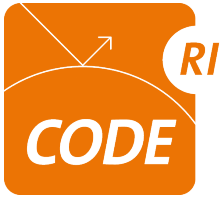
# BA/MA Market Place

CODE Team




Research Institute
Cyber Defence
Universität der Bundeswehr München

# CODE (1)

Universität der Bundeswehr München

- 2013 gegründet als Forschungszentrum “Cyber Operations and Defense”

- Ziel:
  - Experten aus verschiedenen wissenschaftlichen Disziplinen sowie Experten aus Wirtschaft und Verwaltung in der Forschung auf dem Gebiet der CIR (Cyber and Information Room) fakultätsübergreifend zusammen zu bringen.
  - CODE verfolgt das Ziel, innovative technische Innovationen und Konzepte zum Schutz von Daten, Software und Systemen ganzheitlich, integrativ und interdisziplinär unter Berücksichtigung rechtlicher und wirtschaftlicher Rahmenbedingungen umzusetzen.

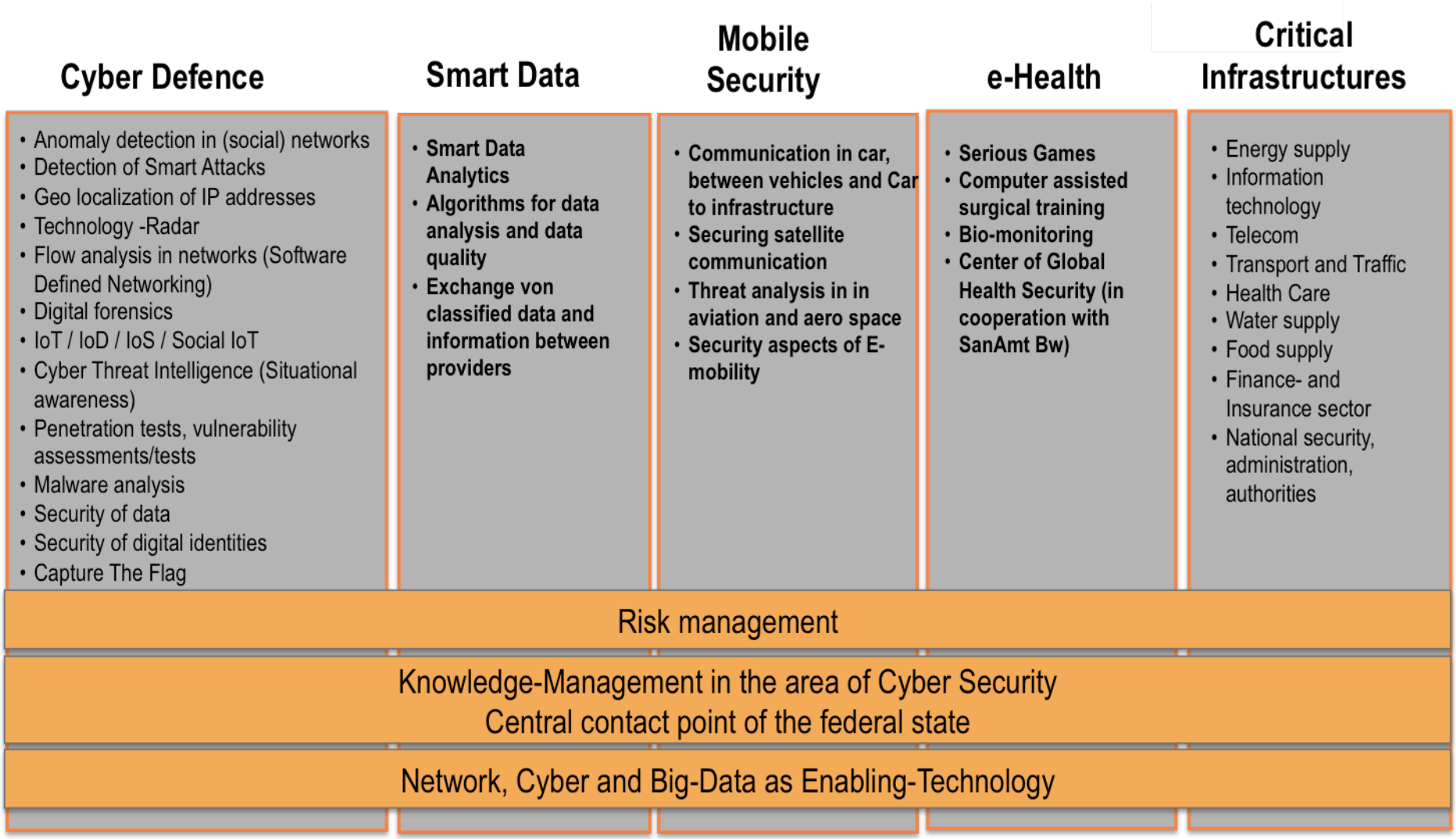
# CODE (2)

- 2017 Erweiterung zum "Forschungsinstitut für Cyber Defense und Smart Data der Bundeswehr und der Bundesregierung".
  - Die institutionelle Verbindung sollte zu einer wissenschaftlich fundierten Plattform für den Aufbau eines in Deutschland einzigartigen Cyber-Clusters führen.

- Infos
  - Lehre/stud. Arbeiten: https://www.unibw.de/code/lehre/lehre
  - Weitere Themen zu stud. Arbeiten gibt es auch auf den einzelnen Seiten zu den jeweiligen Professuren
  - Events: https://www.unibw.de/code/events-u/veranstaltungen

# CODE's Forschungsbereiche

Universität der Bundeswehr München

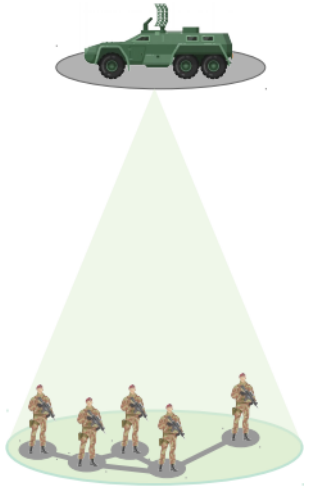


# Ziel heutiger Veranstaltung



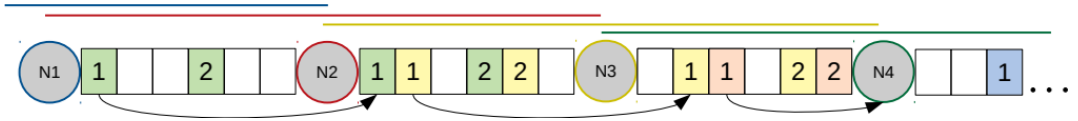
# Intelligent Slot Distribution in (SDN-assisted Tactical Mobile Networks)

Ansprechpartner: Klement Streit,
Florian Steuber
Emails: klement.streit@unibw.de
florian.steuber@unibw.de

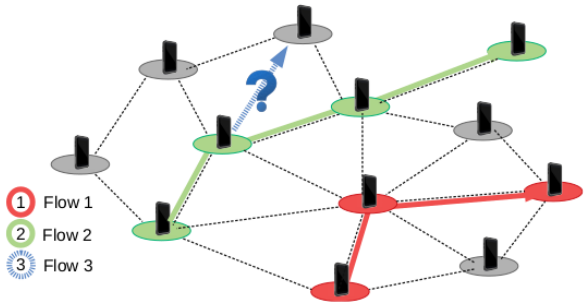


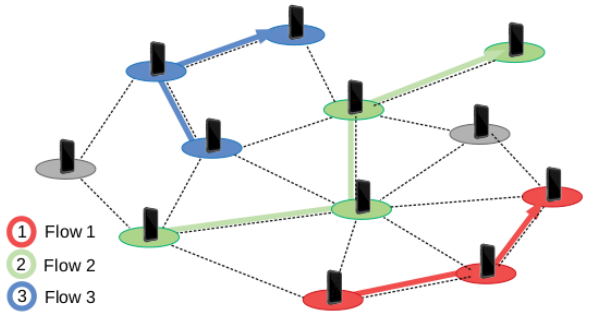
# Intelligent Slot Distribution

- Ziele:
  - Maximierung des Durchsatzes in Mobilen Wireless Networks
  - Übertragung der Frames mit Slot-basierter Paketweiterleitung (TDMA)
  - Einhaltung von QoS Requirements




- Aufgabenstellung:
  - Effiziente Slotaufteilung zwischen direkt verbundenen Knoten und darüber
  - Integrierung der QoS-Anforderungen in die Routenfindung



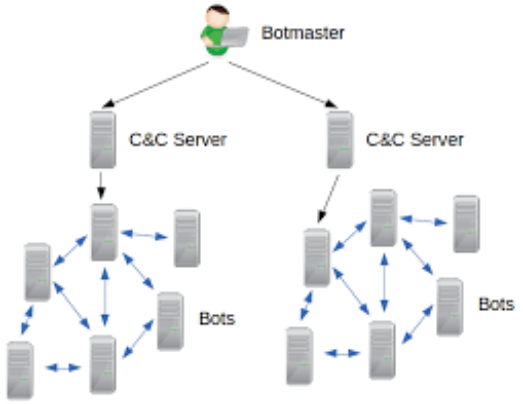





{klement.streit, florian.steuber}@unibw.de

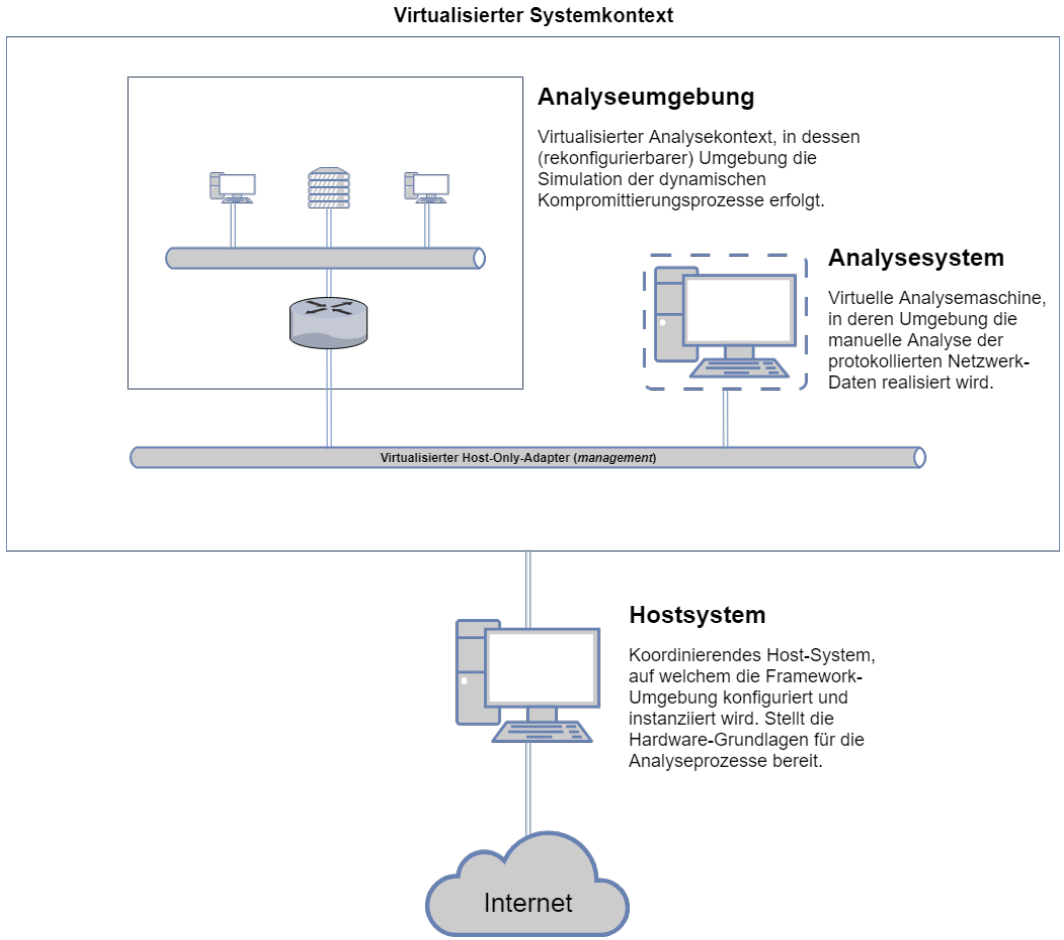
# Themengebiet Botnetze (Verhaltensanalyse & Früherkennung)

Ansprechpartner: Christian Dietz
Email: christian.dietz@unibw.de



# Botnetzverhaltensanalyse - Konzept

## Dynamic Botnet Evaluation Framework



# Dynamic Botnet Evaluation Framework

- Ziel: Dynamische **Verhaltensanalyse** von Botnetz Implementierungen in realitätsnaher Netzwerk-Simulationsumgebung.

- Bereits implementiert:
  - Automatisierte Erstellung und Isolation der Umgebung (Vagrant & VirtualBox)
  - Beispiel Szenarien (Mirai, WannaCry)
  - MITM Techniken
  - Emulation von realer Internet-Infrastruktur
  - Aufzeichnung von Log-Daten (PCAP, Netflow, … )
  - ….

- Mögliche Themenschwerpunkte
  1. [MA] Integration von SDN zur Vernetzung der Hosts (ONOS, Mininet, OpenFlow, …)
  2. [MA] Härtung des Frameworks gegen „Kontext-Checks“
  3. [MA/BA] MITM Techniken: Verschlüsselte C&C Kommunikation
  4. [BA] Visualisierung und Analyse von Ausbreitungscharakteristiken
  5. … Eigene Ideen/Interessen

# Härtung des Frameworks gegen „Kontext-Checks“ (MA)

Universität der Bundeswehr München

- Ziel: Verbergen, dass die Malware sich in einer virtualisierten (und isolierten) Analyseumgebung befindet.

- Bereits implementiert:
  - InetSim (Malware, kann beispielsweise die Internetverbindung testen)

- TODOs:
  - Allgemein:
    - State-of-the-Art Analyse
    - Identifikation relevanter/möglicher Kontext-Checks

  - Auf Netzseite:
    - Selektive Anbindung an das Internet (Whitelisting, …)

  - Im Host/Hypervisor:
    - Identifikation von Virtualisierungs- bzw. Sandboxartefakten
    - Untersuchung der Anpassbarkeit für identifizierte Artefakte
    - Proof-of-concept Implementierung der Äderungen

# MITM Techniken: Verschlüsselte C&C Kommunikation (MA/BA)



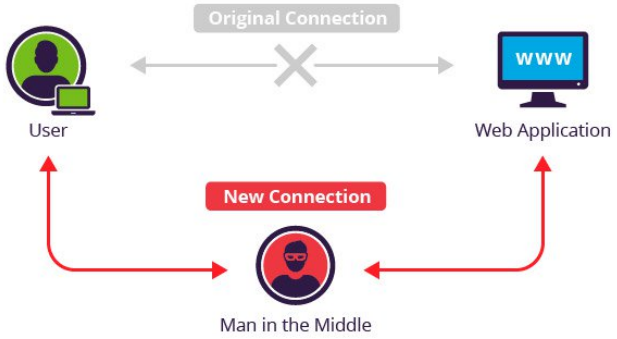
- Ziel: Ermöglichen der Analyse von Netzwerkmitschnitten trotz Einsatz von Verschlüsselung.

- Bereits implementiert:
  - Rudimentäre MITM Techniken

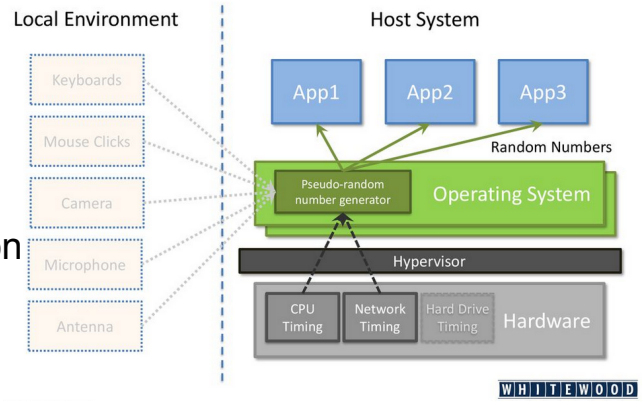
- TODOs:
  - Allgemein:
    - State-of-the-Art Analyse

  - Auf Netzseite:
    - Identifikation relevanter/möglicher Man-in-the-Middle Angriffe
    - Implementierung/Integration ausgewählter Angriffe/Tools

  - Im Host/Hypervisor:
    - Evaluation möglicher kryptografischer Angriffe durch Manipulation der Virtualisierungsumgebung.
    - Evaluation (und Implementierung) von Manipulationen von Entropie-Quellen für PRNG in virtuellen Umgebungen.




Quelle: https://medium.com/xcnotes/mitm-can-be-pretty-easy-with-mitmproxy-and-python-d5293f94d41




Quelle: https://pt.slideshare.net/WhitewoodOWASP/whitewood-entropy-and-random-numbers-owasp-austin-jan-2017-72698618

# Themengebiet Quantencomputing

Ansprechpartner: Prof. Dr. Stefan Brunthaler
Email: brunthaler@unibw.de

# Languages, compilers & runtimes

Universität der Bundeswehr München

Mehrere Themen aus dem Forschungsgebiet fuer geeignete BSc & MSc Studenten vorhanden.

Mögliche Themen:

- ***Compiler fingerprinting***: Identify which compiler & which set of optimizations produced a binary.
- ***JavaScript Profiler***: Use JitProf (Jalangi) to export profiling data to enable profile-based rewriting.
- ***RowHammer Case Study***: Analyze known RowHammer exploits.
- ***Fuzz-Testing State of the Art***: Analyze Random vs. Grammar-based Approaches on the same binaries.
- ***Adaptive Android Obfuscation***: Use profiling-data to obfuscate Android source code.
- ***Pascal compiler in Racket***: focus on instruction selection.

# Languages, compilers & runtimes



- **Offensive Tooling in Racket**:
  - Disassembling binaries
  - Finding ROP gadgets
  - Finding Spectre V1 vulnerabilities
  - Decompile to C/C++
- **Advanced COOP Attacks**: Manipulating only vtable Pointers.

# Themengebiet Softwaresicherheit

Ansprechpartner: Prof. Dr. Johannes Kinder
Email: johannes.kinder@unibw.de

# Android Forensik

- Ziel: Bestimmung welche API Funktionen eine Android-App aufruft, basierend auf System Calls
  - Voraussetzung z.B. für Malware Erkennung oder funktionale Einordnung

- Konzeptentwicklung:
  - Lernen von System Call-Mustern als Automaten
  - Probabilistische Zuordnung

- Implementierung:
  - Analyseplattform, basierend auf bestehenden Tools, z.B. “CopperDroid”
  - Datensatz an Testapplikationen mit bekannter Ground Truth
  - Experimentelle Validierung

# JavaScript Testing



- ExpoSE: Automatisches Testsystem für JavaScript
  - Basierend auf Symbolic Execution
  - Erzeugt systematisch Eingaben für Testabdeckung
  - Anbindung an Z3 Solver

- Projekt Regulärer Ausdrücke:
  - Erzeugen von positiven und negativen Beispielen für beliebige Regex
- Projekt Open-Source Trojaner:
  - KI-basiertes Warnsystem für Veränderungen in Bibliotheken
- Projekt Test-Umgebung:
  - Einbindung in bestehende Test-Umgebungen (z.B. Mocha) und End-to-End Erzeugung von Testfällen

# Automated Reverse Engineering



- Analyse von Binärcode
  - Malware, Schwachstellen
  - Ghidra: Vormals internes NSA-Tool, Open Source seit März 2019
  - Plugin und Scripting Interface in Java/Jython

- Projekt Deobfuscation:
  - Umwandlung von verschleiertem Binärcode in Klartext
  - Implementierung eines Algorithmus zur partiellen Auswertung von Pseudocode in Ghidra, und Einbindung in die Analyseumgebung

- Projekt Symbolic Execution:
  - Integration von Symbolic Execution zur Bestimmung von Pfadbedingungen
  - Anbindung eines Solvers und einer P-Code Semantik

# Themengebiet Cyber Range: Automated hostdiscovery and service enumeration

Ansprechpartner: Volker Eiseler/Tim Mittermeier
Email: volker.eiseler@unibw.de/tim.mittermeier@unibw.de

# Automated hostdiscovery

- Ziel:  Automatisiertes Scannen und Mappen von Netzen beliebiger Größe und Komplexität.
- Bereits implementiert:
  - Hardware Einrüstung
- Mögliche Themenschwerpunkte
  1. [BA] Entwurf und Aufbau eines teilvirtualisierten Testumgebung
  2. [BA] Praktische Evaluation von Scanning/Mapping Tools
  3. [MA/BA] Konzeption und Entwurf einer Softwareumgebung zum automatisierten Mappen von Netzwerken
  4. [MA/BA] Bewertung und Implementierung von Modulen
  5. … Eigene Ideen/Interessen

# Themengebiet Virtual Reality:
# Multi-user VR environment for data analysis

Ansprechpartner: Volker Eiseler/Tim Mittermeier
Email: volker.eiseler@unibw.de/tim.mittermeier@unibw.de

# Virtual Reality

- Ziel:  Aufbau einer VR-Testumgebung zur Darstellung und Verarbeitung großer Datenmengen im OSINT-Kontext

- Bereits implementiert:
  - Hardware Einrüstung

- Mögliche Themenschwerpunkte
  1. [BA] Implementierung eines room-scale multi user environments
  2. [BA] Entwurf von Darstellungsmöglichkeiten großer Datenmengen in VR
  3. [MA/BA] Implementierung eines Framework zur Aggregation und Darstellung großer Datenmengen in VR
  4. … Eigene Ideen/Interessen

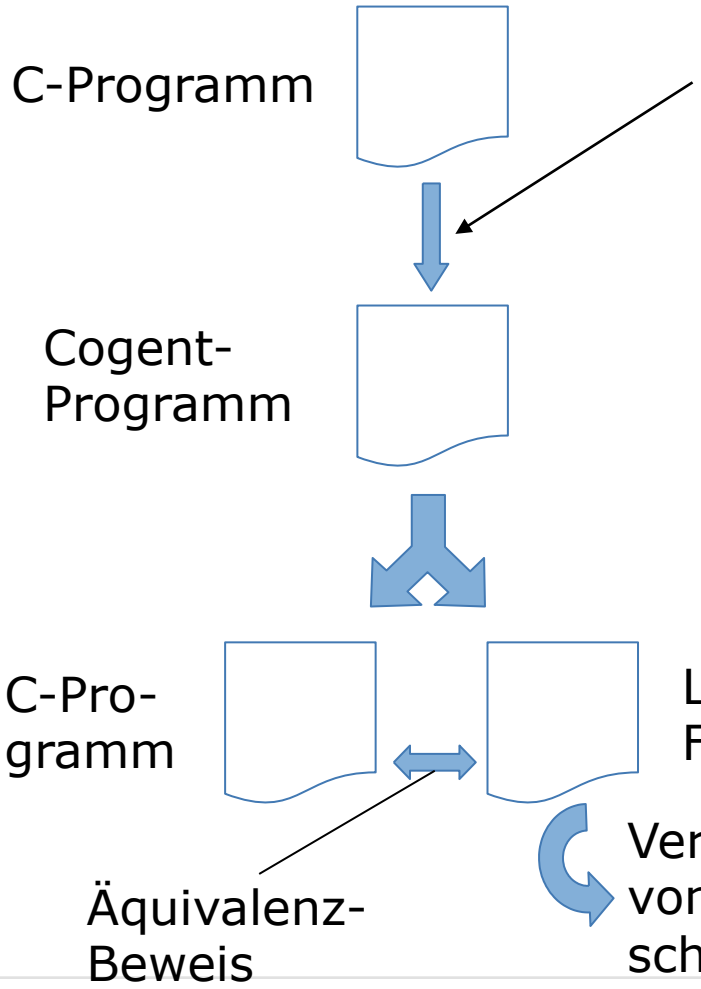
# Themengebiet Programmverifikation

Ansprechpartner: Prof. Gunnar Teege
Email: gunnar.teege@unibw.de

# Bachelor-Arbeiten im Code-Projekt HoBit

Universität der Bundeswehr München

(hochsicheres Betriebssytem für embedded IT)




BA/MA-Arbeiten

- Übersetzung von C-Code (imperativ) nach Cogent (funktional)
- Unterstützung durch Werkzeug (Übersetzung von Typdefinitionen und Deklarationen)
- Anleitung zum Vorgehen
- Ergebnis-Test durch Cogent-Syntaxprüfung

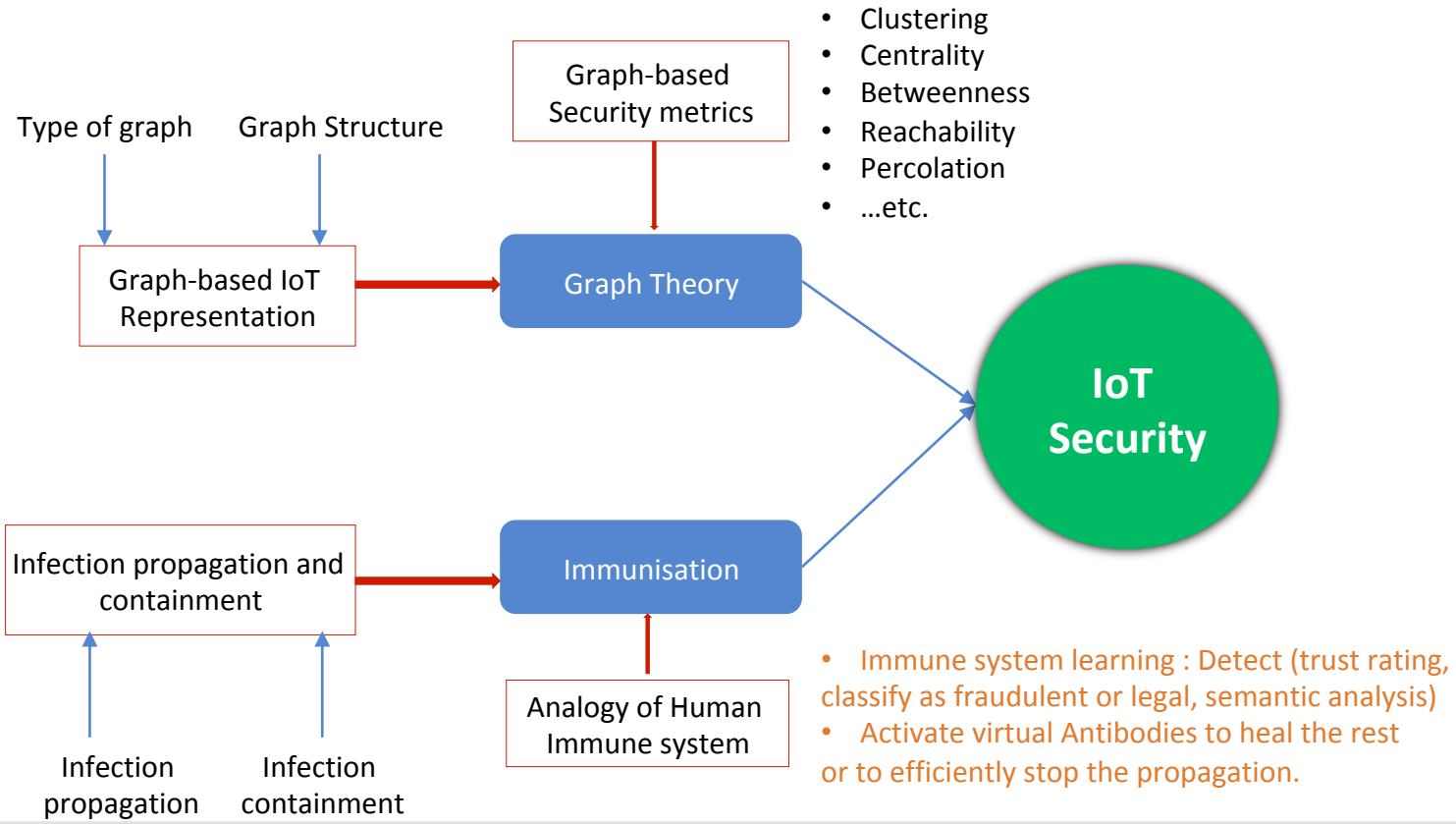
# Security of the Internet of Things

Ansprechpartner: Farell Folly
Emails: folly.farell@unibw.de

*"Since we can never produce a 100% secure general system or network, we need methods to mitigate the spread of damage."*

# Our Approach

- Minimize exposure factors(s)
- Control how threats spread
- Design an efficient patch or vaccines distribution mechanism



# Challenges to face (1)



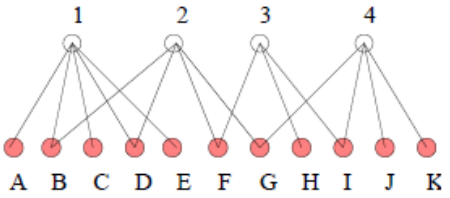
- Epidemic process: Susceptible-Infected-Recovered
  - How fast does an infection spread?
  - What is the threat strategy?
  - What os tje IoT network topology?
  - How resistant are the nodes/clusters?

# Challenges to face (2)

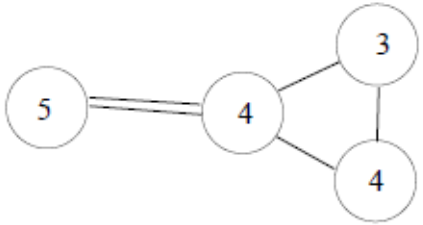
- Graph: clustering, groupings and simplifications

Apps

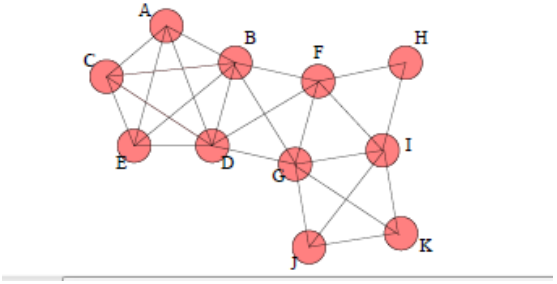
Devices



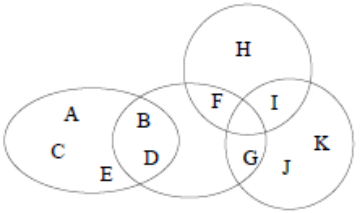

Original graph topology




Final compressed graph




Devices interconnection (Abstraction of used Apps)




Forming cliques

# Thesis Proposal (MA)



- Objective: Using Machine Learning to detect best communies (groups) to vaccinate first in order to efficiently mitigate infection propagation in large-scale networks.

- Programming Language:
  - Python + Networks Library for Graphs

- TODOs:
  - Build algorithms to summarise a graph with millions of nodes
  - Detect communities in large scale networks
  - Given a vaccine budget and using appropriate metrics, distribute vaccines to groups that will help efficient mitigate ongoing infection

# Themengebiet
# Sichere Aeronautische Kommunikation

Ansprechpartner: Dr. Corinna Schmitt, Nils Mäurer
Email: corinna.schmitt@unibw.de, nils.maeurer@dlr.de

# Security Architecture for LDACS

Universität der Bundeswehr München

## LDACS: L-band Digital Aeronautical Communications System

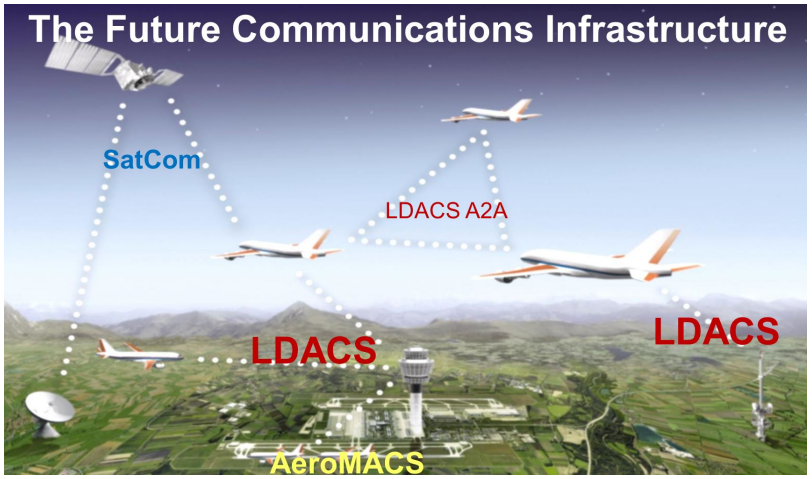
- LDACS is the **terrestrial data link** of the **Future Communications Infrastructure (FCI)**

## LDACS Communication Functionality

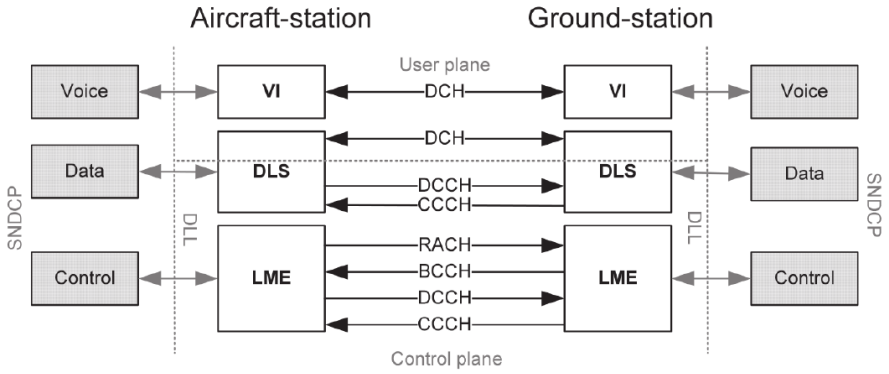
- LDACS enables secure data link
- Net data rate: 550 kbit/s – 2,6 Mbit/s (50xVDLm2)

**Extension Towards Navigation (APNT)**

**Extension Towards Aircraft Connectivity**




## LDACS Control Channel Security




## User Data Plane with Security Additions

- How to add security onto small channels?
- How to add security with limited resources?
- How to add security while maintaining interoperability?

**→ DLR offers a Master Thesis at DLR OP**

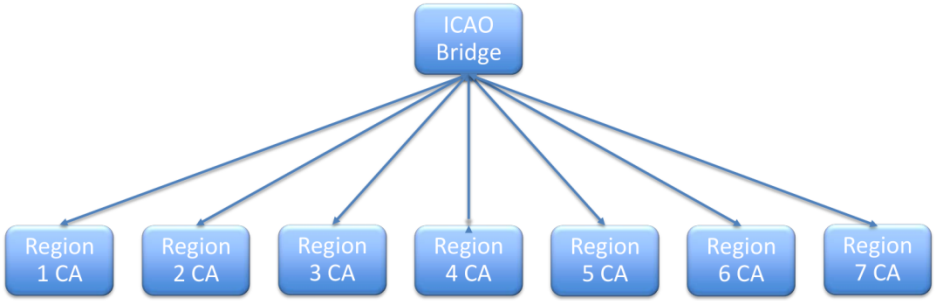
**→ Are you up for the challenge?**

# Distributed Trust in Mobile Environments for Digital Aeronautical Communications

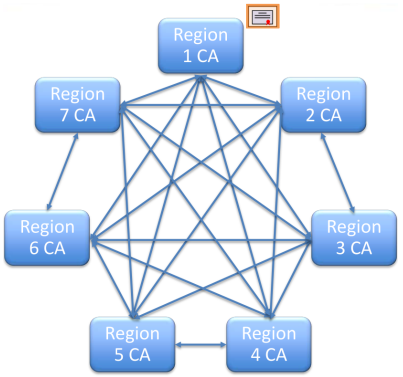
Universität der Bundeswehr München

- How to establish trust in a highly mobile, distributed system?

**PKI – ICAO trust bridge**




**PKI – Regional Cross Certification**



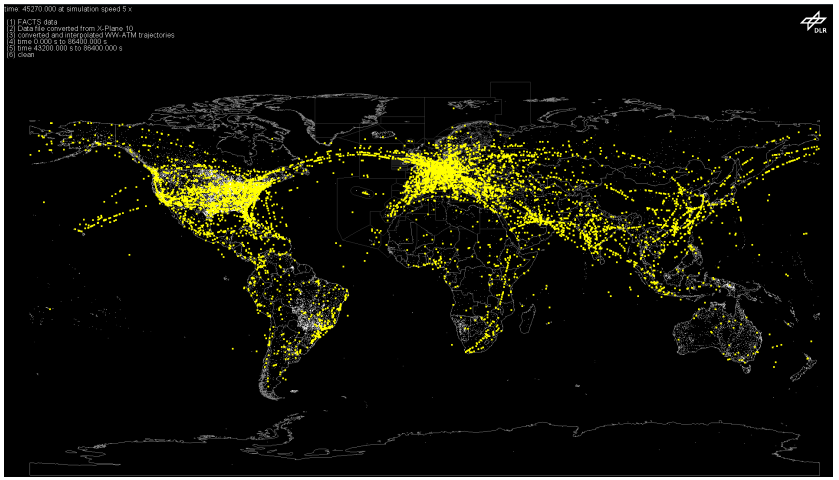

1. Evaluate trust measurement techniques
2. Investigate decentralized trust solutions
3. Apply distributed trust solutions on mobile environments

- Are there options beyond a PKI?

→ **DLR offers a Master Thesis at DLR OP**

→ **Are you up for the challenge?**

**FACTS2 – Simulation Environment at DLR**



# Themengebiet Quantencomputing

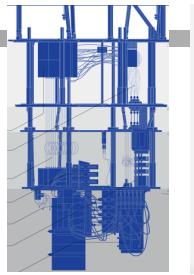
Ansprechpartner: Prof. Dr. Udo Helmbrecht, Dr. Wolfgang Gehrke
Email: udo.helmbrecht@unibw.de, wolfgang.gehrke@unibw.de

# IBM Q Hub @ FI CODE



**Kooperationspartner:**

- Leibniz Supercomputing Center
  - LMU
  - TU München
  - Hochschule München
- DLR
- Forschungszentrum Jülich
- ZITiS
- Giesecke + Devrient
- secunet
- Siemens
- ...




**Forschungsschwerpunkte:**

**Theorie: Quantum Computing**

- Vorlesung und Praktikum Quantum Computing

**Optimierung Quantum Computing**

- Optimierung von Quantenalgorithmen
- Einsatz des Quantum Computing in Geoinformatik

**Post Quantum Cryptography**

- Forschungsprojekt: Post Quantum Cryptography (Infineon Technologies)

## IBM Q Hubs

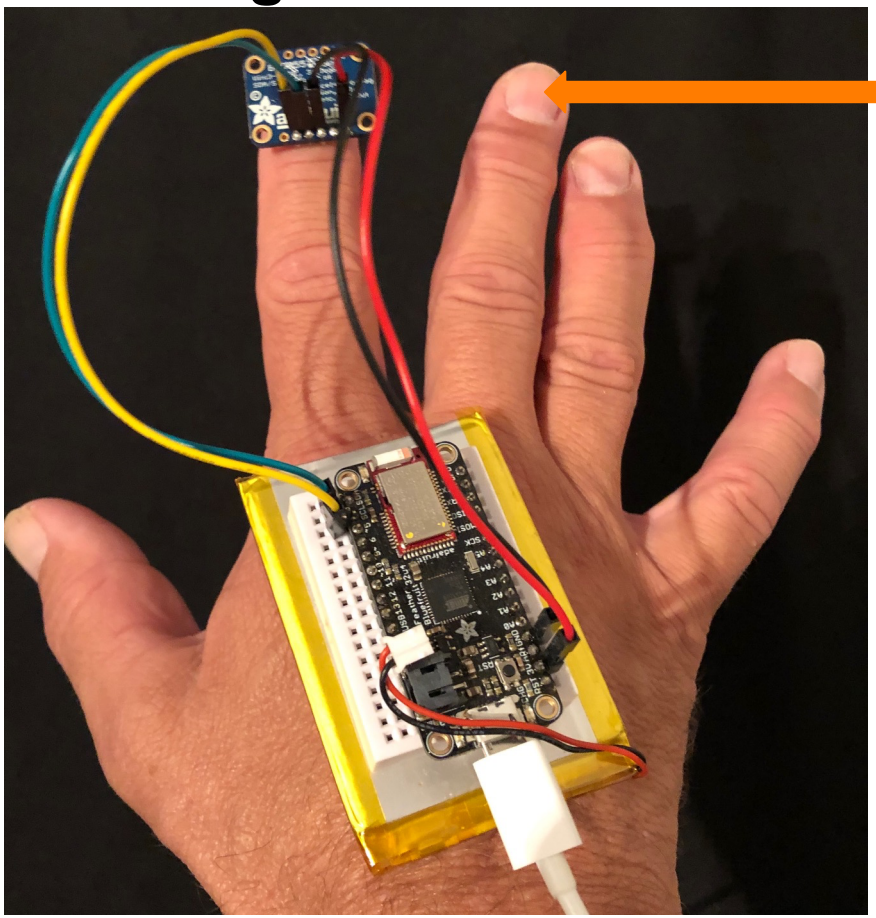
# Themengebiet IoT & VR

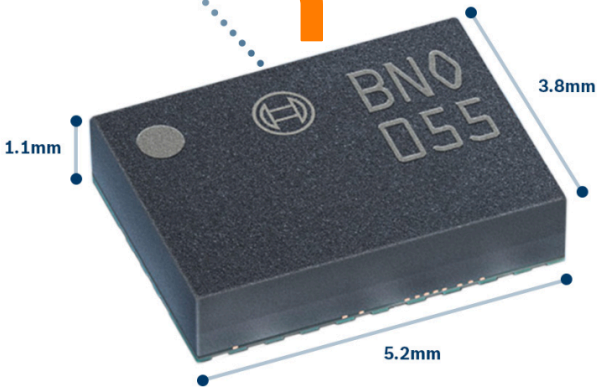
Ansprechpartner: Prof. Dr. Udo Helmbrecht, Dr. Ken Pfeuffer
Email: udo.helmbrecht@unibw.de, ken.pfeuffer@unibw.de

# Absolute Orientation IMU



## Challenge: miniaturization 4 x 5 mm on a fingernail






### Main features

**Absolute Orientation**
Integrates accelerometer, gyroscope and magnetometer

**Accelerometer**
Detects linear motion and gravitational forces

**Gyroscope**
Measures the rate of rotation in space (roll, pitch, yaw)

**Magnetometer**
Measures the terrestrial earth's magnetic fields

**Software**
Intelligently fuses raw data from multiple sensors

# Usable Security and Privacy Group

Ansprechpartner: Prof. Dr. Florian Alt
Email: florian.alt@unibw.de

https://www.unibw.de/usable-security-and-privacy/lehre/ studentische-arbeiten

# Usable Security





**We are looking at the role of humans in different types of security-critical systems.**


# Kontakt zu uns

- Email direkt an Themensteller
- Infos:

  Lehre/stud. Arbeiten: https://www.unibw.de/code/lehre/lehre

  Individuelle Professur- und Mitarbeiterseiten

- Kommt vorbei mit eigenen Ideen.
  Bei einer guten Tasse Kaffee/Tee vorbei!

# Making Multi-Variant Execution Practical in the Real World

Stijn Volckaert, Katholische Universität Leuven

Multi-Variant Execution Environments (MVEEs) have shown great promise as a mechanism to defend against the exploitation of software vulnerabilities. Their core idea is to run multiple versions (or diversified variants) of the same program in tandem on top of a small and efficient hypervisor that distributes program inputs, compares outputs, and terminates the variants when their outputs diverge. With properly constructed variants, one can guarantee that any exploitation attempt will trigger a divergence and, hence, termination before the exploit succeeds.

Unfortunately, MVEEs have seen virtually no adoption outside of military settings. In this talk, I will give an overview of the biggest hurdles that stand in the way of greater adoption. I will also discuss some preliminary research towards overcoming these hurdles and suggest future research directions.