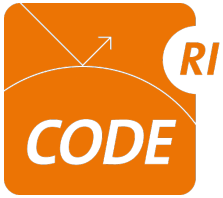
BA/MA Market Place

CODE Team



Research Institute
Cyber Defence
Universität der Bundeswehr München

Über Uns

Universität der Bundeswehr München

2013 - Gründung als Forschungszentrum

Ziel der gemeinsamen Forschungsarbeit mit Experten anderer Fachrichtungen und Experten aus Behörden und der Wirtschaft

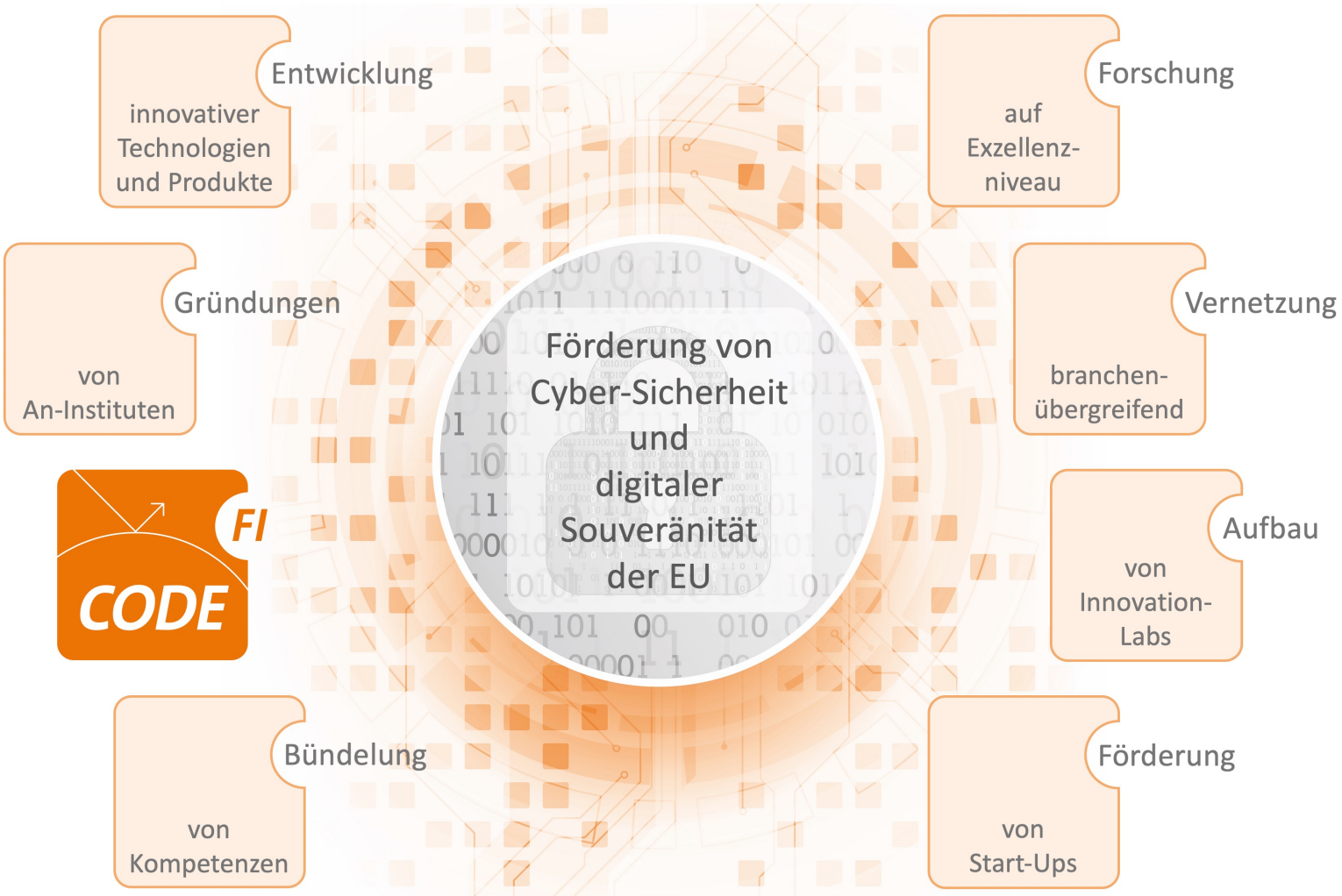
2017 - Ausbau zum Forschungsinstitut

Ministerielle Entscheidung zum Forschungsinstitut für Cyber Defence und Smart Data der Bundeswehr und des Bundes

Entwicklung eines bundesweit einzigartigen Cyber-Clusters

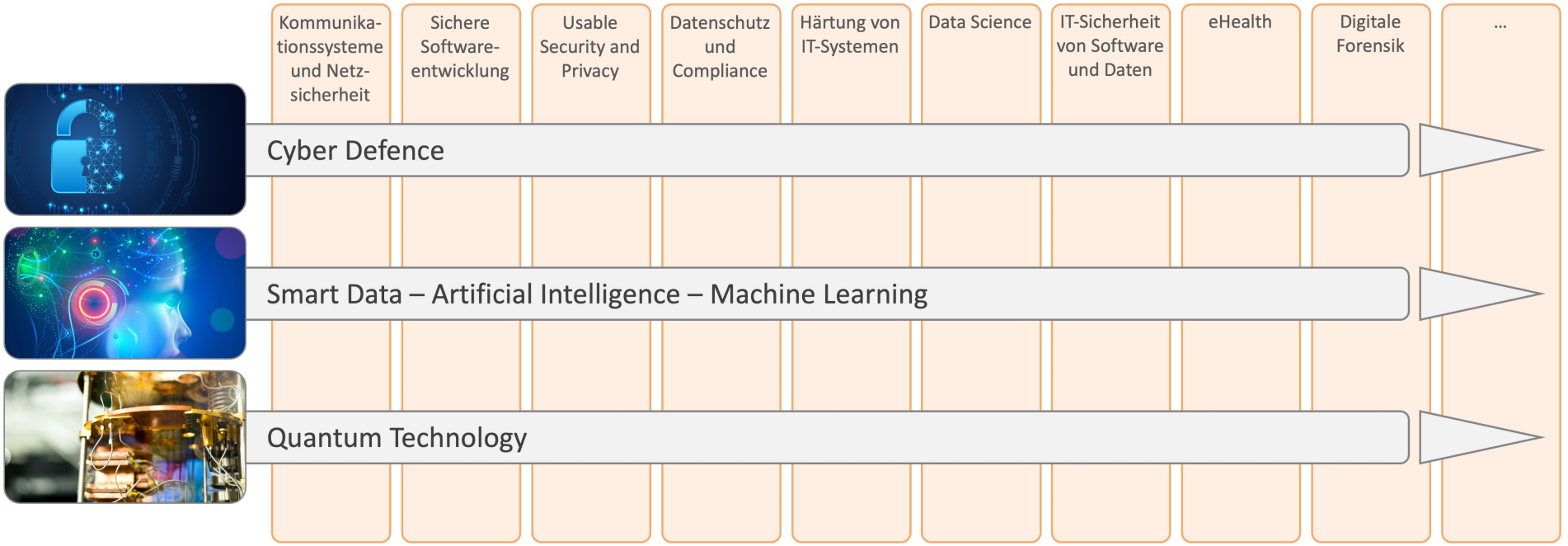
Etablierung von Aus- und Fortbildungsmöglichkeiten sowie einer wissenschaftsbasierten Plattform

Unsere Mission



CODE's Forschungsbereiche

der Bundeswehr Universität München



Aktuelle Abschlußarbeiten

https://www.unibw.de/network-security/lehre/ausschreibungen

Alle Arbeiten können entsprechend desgewählten Arbeitstyps (BA/MA) vom Umfang her angepasst und individualisiert werden!

Kontext zu QKD und zum Projekt MuQuaNet

Universität der Bundeswehr München

Kontext

Quantencomputer bedrohen die Sicherheit der etablierten Kryptografie, insbesondere die asymmetrischen Verfahren. Lösungsansätze, die am FI CODE untersucht werden:

- Post-Quantum Cryptography (PQC): Verschlüsselungsmethoden auf Basis mathematischer Verfahren, die (noch) nicht effizient durch Quantencomputer gelöst warden können
- Quantum Key Distribution (QKD): Nutzung der physikalischen Prinzipien der Quantenphysik, um sichere Schlüssel zu erzeugen

Projektinhalt MuQuaNet

Untersuchung von Quantum-Key-Distribution insbesondere aus Sicht IT-Sicherheit

- Aufbau einer Infrastruktur zur Quantenkommunikation im Großraum München bis 2024 mit ersten Pilotstrecken in 2021
- Untersuchung von Konzepten, Protokollen und Architekturen zur Schlüsselverteilung
- Durchführung von Sicherheitsanalysen
- Demonstration von Use Cases

Kontakt: Nils g. Felde, Hedwig Koerfgen

Authentifizierung in QKD-Netzwerken

Universität der Bundeswehr München

Fragestellung	• Die Sicherheit von Quantum Key Distribution liegt darin, dass aufgrund der physikalischen Gesetzmäßigkeiten ein Abhören des Quantenkanals bemerkt würde • Neben dem Quantenkanal ist allerdings die Kommunikation über einen authentifizierten “klassischer Kanal” erforderlich, um QKD-Protokolle zu realisieren. • Solche Authentifizierungsverfahren sollen untersucht und bewertet werden
Mögliche Inhalte der Arbeit	• Vergleich und Bewertung verschiedener Authentisierungsverfahren • Theoretische und praktische Untersuchung des Authentisierungsverfahrens der bei MuQuaNet vorhandenen QKD-Laborgeräte • Implementierung eines Proof of Concept für ein Authentisierungsverfahren
Voraussetzungen	• Methodische und systematische Arbeitsweise für die Entwicklung eines nachvollziehbaren Bewertungsschemas • Programmierkenntnisse von Vorteil (Sprache beliebig)

Kontakt: Nils g. Felde, Hedwig Koerfgen

Anomalieerkennung bei QKD-Geräten

Fragestellung	• Die Sicherheit von Quantum Key Distribution liegt darin, dass aufgrund der physikalischen Gesetzmäßigkeiten ein Abhören des Quantenkanals bemerkt würde. • Umwelteinflüsse haben allerdings einen großen Einfluss auf Quantentechnologien. • Untersuchungsgegenstand der Arbeit ist die Unterscheidbarkeit zwischen Umwelteinflüssen und Manipulationen
Mögliche Inhalte der Arbeit	• Auswertung der bei MuQuaNet vorhandenen QKD-Laborgeräte im Hinblick auf Korrelationen zwischen Performance und externen Einflüssen • Entwicklung beispielhafter Denial-of-Service-Attacken
Voraussetzungen	• Erste Erfahrung / Interesse an Datenanalyse (z.B. Machine Learning-Verfahren) • Erste Erfahrung / Interesse mit linuxbasierten Systemen • Interesse, sich in die Funktionsweise von QKD-Geräten einzuarbeiten

Kontakt: Nils g. Felde, Hedwig Koerfgen

Seitenkanalangriffe auf QKD-Geräte

Universität der Bundeswehr München

Fragestellung

- Die Sicherheit von Quantum Key Distribution liegt darin, dass aufgrund der physikalischen Gesetzmäßigkeiten ein Abhören des Quantenkanals bemerkt würde
- Neben dem Quantenkanal gibt es allerdings weitere Systembestandteile, die auf mögliche Angriffsvektoren untersucht werden sollen

Mögliche Inhalte der Arbeit

- Ermittlung und Klassifizierung möglicher Angriffsvektoren für QKD allgemein und die bei MuQuaNet verwendeten Geräte im Speziellen
- Praktische Durchführung exemplarischer Angriffsvektoren auf Datenverkehr, Firmware o.ä.

Voraussetzungen

- Kenntnisse im Bereich Rechnernetze
- Erste Erfahrung / Interesse mit linuxbasierten Systemen
- Interesse, sich in die Funktionsweise von QKD-Geräten einzuarbeiten

Kontakt: Nils g. Felde, Hedwig Koerfgen

Simulation von Quantenkommunikationsnetzen

Universität der Bundeswehr München

Fragestellung	• Quantum Key Distribution lässt sich aufgrund der speziellen Protokolle nicht mit klassischen Tools zur Netzwerksimulation abbilden • Da QKD-Infrastruktur teuer ist, sind Simulationen wichtig für die Validierung von neuen Konzepten und Protokollen für große Netzwerk • Untersuchungsgegenstand ist die Simulation des MuQuaNet-Netzes und die Bewertung verfügbarer Simulationstools
Mögliche Inhalte der Arbeit	• Anforderungsanalyse für Simulationen der MuQuaNet-Infrastruktur • Recherche und Bewertung möglicher Simulationstools • Durchführung von Simulationen zur Quantenschlüsselverteilung • Erweiterung bestehender Simulatoren um die spezifischen MuQuaNet-Anforderungen (z.B. verwendete Protokolle)
Voraussetzungen	• Kenntnisse im Bereich Rechnernetze • Vorerfahrungen mit Netzwerksimulationen von Vorteil • Interesse, sich in die spezifischen Anforderungen von Quantenkommunikation einzuarbeiten

Kontakt: Nils g. Felde, Hedwig Koerfgen

Mehrbenutzerkommunikation mit QKD

Universität der Bundeswehr München

Fragestellung

- Die Sicherheit von Quantum Key Distribution liegt darin, dass aufgrund der physikalischen Gesetzmäßigkeiten ein Abhören des Quantenkanals bemerkt würde
- Das gleiche Prinzip bewirkt allerdings auch, dass Quantenschlüssel nur auf Punkt-zu-Punkt-Verbindungen ausgetauscht werden können, nicht im ganzen Netz
- Für Mehrbenutzerszenarien müssen entsprechende Konzepte zur Schlüselverteilung untersucht und implementiert werden

Mögliche Inhalte der Arbeit

- Erweiterung einer bestehenden Demonstratorapplikation (Punk-zu-Punkt-Verbindung) für ein Mehrbenutzerszenario mit drei Kommunikationsknoten
- Untersuchung, Vergleich und Implementierung möglicher Protokolle für die Verteilung und Nutzung von Quantenschlüsseln

Voraussetzungen

- Kenntnisse im Bereich Kryptografie
- Erste Programmierkenntnisse, Erfahrung mit Python und Shell-Skripten von Vorteil
- Erfahrung mit REST-APIs von Vorteil

Kontakt: Nils g. Felde, Hedwig Koerfgen

Moving Target Defense approach in P4

- Moving Target Defense (MTD) is about shifting continuously the variables of the environment in such a way that is more complex for an attacker to be successful.
- Network-level MTD examples include IP shuffling or Port Hopping.
- This work will investigate the migration of existing approaches into the next generation programming language P4, which is directly executed on the network interface itself.
- **Goal**: The goal of this master thesis is to implement existing MTD approaches in the P4 networking language.

Kontakt: Nils Rodday & Raphael Labaca Castro

Evaluierung von automatisierten Netzverkehr-Generatoren

Universität der Bundeswehr München

- Ziel: Evaluierung von Lösungen zur Generierung von automatisiertem und realitätsnahem Netzverkehr, sowie deren Verwendung in einer Cyber Range

- TODOs:
  - Entwicklung einer geeigneten Metrik für die Bewertung von Ansätzen zur Generierung von realitätsnahem Netzverkehr
  - Darauf basierend: Betrachtung und Bewertung verfügbarer Lösungen
  - Evaluierung, wie eine geeignete Lösung in einer Cyber Range Umgebung eingesetzt werden könnte

- Themenschwerpunkte (u.a.):
  - Generieren und Einspielen von Netzwerkverkehr
  - Komposition von realem und Realitätsgrad von synthetischem Netzverkehr
  - Anpassungsmöglichkeiten des generierten Verkehrs an bestehende Netzstrukturen (IP-Adressen, Services, ...)

Kontakt: Marcus Knüpfer/Matthias Schopp/Christoph Steininger

Dynamische Ontologieerstellung für Daten Streams

Universität der Bundeswehr München

- Ziel: Erstellung einer dynamischen Ontologie durch Erweiterung einer bestehenden Ontologie wie bspw. DBpedia

- TODOs:
  - Einarbeitung in eine bestehende Ontologie (z.B**. DBpedia)**
  - Darauf basierend: Erweiterung durch eigenes Modul zur dynamischen Integration von weiteren Einträgen (Daten Stream und Named Entity Recognition sind bereits exemplarisch vorhanden)
  - **Quantitative E**valuierung der Erweiterung und Integration in die Data Engineering Pipeline

- Themenschwerpunkte (u.a.):
  - Dynamische Ontologien
  - Wissensgraphen
  - Named Entity Recognition

Kontakt: Sabine Ullrich, Tim Mittermeier & Matthias Frank

Kontextsensitive multimodale Interfaces zur Datenanalyse

Universität der Bundeswehr München

- Ziel: Entwurf eines multimodalen User Interfaces zur kontextsensitiven Generierung von Suchanfragen.

- TODOs:
  - Literaturrecherche
  - Entwurf und Implementierung eines User Interfaces mit mindestens zwei Eingabemodalitäten (Spracherkennung & Gaze Tracking)
  - **Evaluation des Interfaces in Form einer Nutzerstudie**

- Themenschwerpunkte (u.a.):
  - Multimodale Interfaces
  - Spracherkennung
  - Gaze Tracking

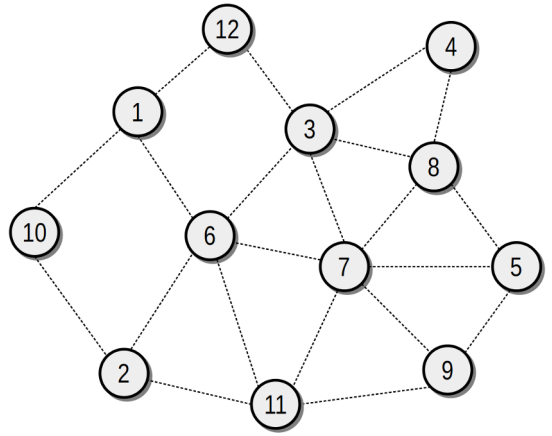
Kontakt: Tim Mittermeier, Sabine Ullrich & Matthias Frank

Partial Topology Update in MANETs

- Mobile Ad-Hoc Netze sind selbstorganisierende Netze, deren sich bewegende Teilnehmer über einen kabellosen Kanal miteinander verbunden sind.
- Herausforderung: Routenfindung basierend auf einer aktuellen Netztopologie.

- Aufgaben:
  - Erweiterung eines existierenden Topologie Update Algorithmus
  - Implementierung und Auswertung der Erweiterung

- Anforderungen an den Algorithmus:
  - Geringer Routingoverhead
  - Topologierepresentation muss aktuell sein

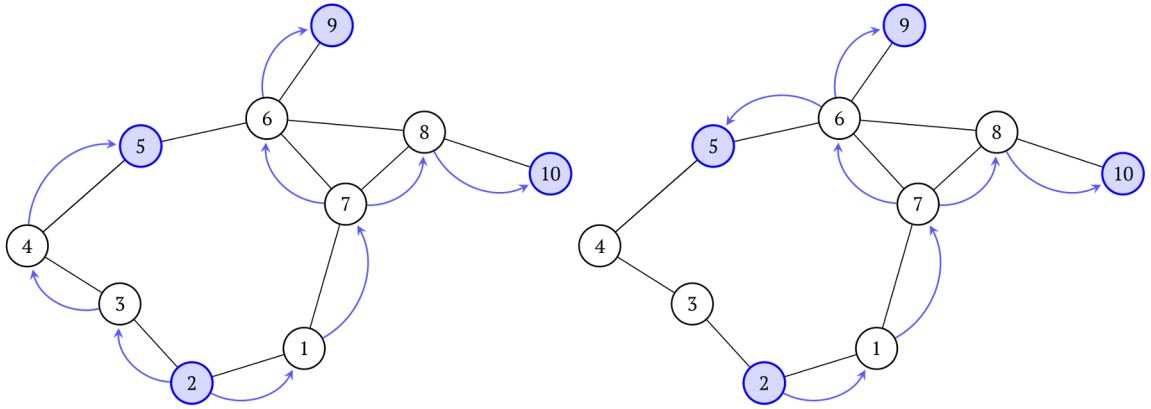


Kontakt: Klement Streit

Multicast Data Delivery in MANETs

- Ziel: Berechnung von Multicast Routen in MANETs
  - Möglichst kurze Multicast-Routen
  - Hohe Überlappung an “shared-links”

- Vorgehensweise:
  - Einarbeitung in MANET-Framework (java)
  - Literaturrecherche
  - Implementierung und Auswertung



Kontakt: Klement Streit

Generating a RPKI groundtruth dataset in Omnett++ and evaluating ROV methodologies

- The Border Gateway Protocol (BGP) is used to communicate routing information between Autonomous Systems on the Internet, e.g. AT&T and Telekom.
- Since BGP is insecure, the Resource Public Key Infrastructure (RPKI) was developed to provide Origin Validation and prevent BGP Hijacking. Every announcement can be validated via a cryptographic chain using RPKI validators.
- Different Route Origin Validation measurement methods exist, but they cannot be evaluated against each other as there is no ground truth (who is actually using RPKI?).

- **Goal**: Your job is to create an Internet-like topology using the simulation software Omnett++. Once established, you will deploy RPKI filtering on selected nodes. As a last step, existing ROV measurement methodologies will be used to infer RPKI filtering and results between different approaches can be compared.

Kontakt: Nils Rodday

Validating RIPE Atlas probe information

- RIPE Atlas is a well known distributed measurement platform. Thousands of Arduino-like devices are installed in different networks around the world and can be remotely used for measurements (e.g. traceroutes to debug networking issues).
- Meta information about the probes is available, but sometimes inaccurate (e.g. IP addresses, NAT information, etc.).

- **Goal**: Find inconsistencies in probes meta info and update accordingly.

- **Method**: You will be using RIPE Atlas to send traceroutes against a server that you control. The payload contains unique identifiers such that you are able to tell if a probe actually reached your control server. You can compare probes meta info and actual information accordingly.

Kontakt: Nils Rodday

Default Route Measurement extension

Universität der Bundeswehr München

- **Problem:** Default Routes provide connectivity although no route entry exists in the routing table of an Autonomous System. We implemented two identification methodologies in previous work that allow us to infer default routes. Results can be found at: defaultroutes.net
- However, visibility is limited as the number of RIPE Atlas vantage points covers only 3700 (out of 72.000) Autonomous Systems.

- **Goal**: Extend coverage by incorporating more vantage points (e.g. PlanetLab) into the measurements.

Kontakt: Nils Rodday

A Graph-theoretical Approach For Mitigating Infections Spread in Large-scale Networks

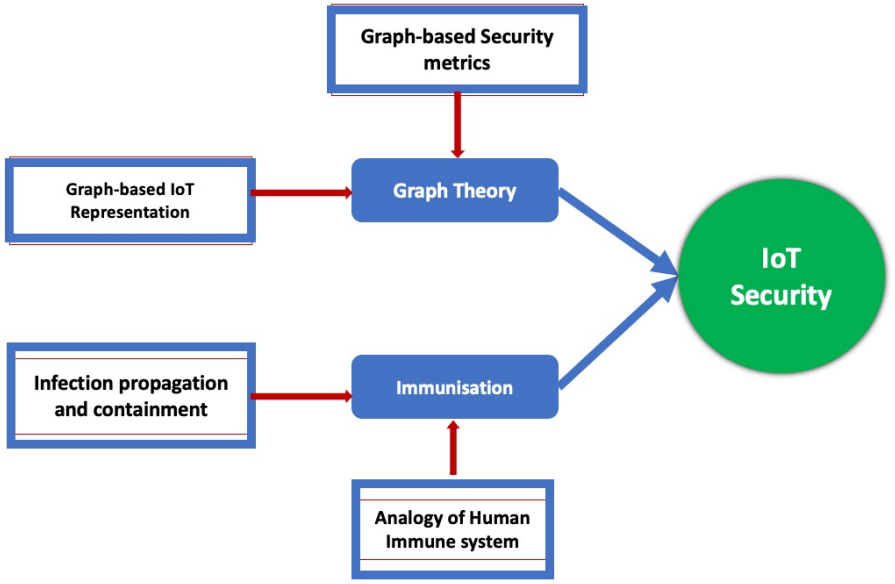
Kontakt: folly.farell@unibw.de

Problem Statement

- The Internet today, mainly the IoT comprises of Billions of nodes characterised by:
  - Heterogeneity
  - Dynamic
  - Number
- No systematic security approach for IoT, most devices lack strong security measures
- Infecting a few nodes could lead to a worldwide chaos (usually a DDoS, money lost)
- Intractability of Algorithms

Investigations

- Application areas:
  - Social networks
  - Email networks
  - Web of Things



- Use nodes' security-relevant features to build up pertinent metrics to study infections propagation
- Build an efficient algorithm to group nodes based on the identified features
- Design an efficient node removal mechanism to mitigate the attack propagation.

Topic Proposals

- Using Machine Learning to identify what features play a significant role during an infection propagation, and determine how to use them to build groups that could help isolate or contain attacks efficiently in large-scale networks.

- **Programme Language**:
  - Python + Networks Library for Graphs

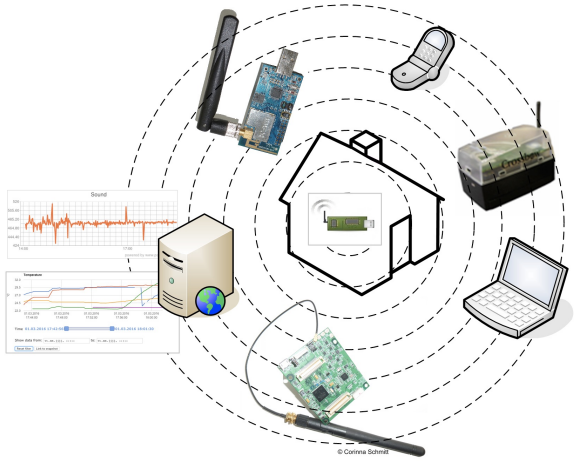
- **TODOs**:
  - Build algorithms to summarise a graph with millions of nodes, based on security-relevant features
  - Explore how infections spread among groups of nodes and identify what features characterise the big spreaders.

Sicherheitsprotokolle

- Ziel: Gesicherte Kommunikation zwischen Knoten und Gateway
- Plattformen: OpenMote - Knoten mit RIOT OS

- Möglichkeiten u.a.:
  - Pre-shared Ansatz
  - Elliptic Curve Cryptography
  - DTLS und zertifikatbasiert

- ToDos:
  - Konzeptentwicklung
  - Implementierung und Integration in bestehendes System
  - Evaluation (u.a. Ressourcenverbrauch)



Kontakt: Corinna Schmitt

Indoor Lokalization

- Große & versteckte Deployments von Knoten
- Vergesslichkeit der Eigentümer

- Ziel: Indoor Lokalisierung

- ToDos:
  - Evaluation von Lokalisierungsmethoden
  - Konzeptentwicklung unter Verwendung von RIOT OS-basierten Knoten
  - Implementierung und Integrierung in bestehendes System
  - Evaluation

Kontakt: Corinna Schmitt

Weitere Abschlußarbeiten

In den Bereichen genannten Bereichen, sowie u.a. in

- Social Engineering
- Bot(s)
- Identification Mechanisms

https://www.unibw.de/network-security
https://www.unibw.de/network-security/team → Kontaktdaten
https://www.unibw.de/network-security/lehre/ausschreibungen