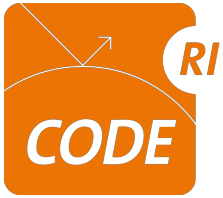
# BA/MA Market Place

CODE Team




Research Institute
Cyber Defence
Universität der Bundeswehr München

# CODE (1)



- 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)

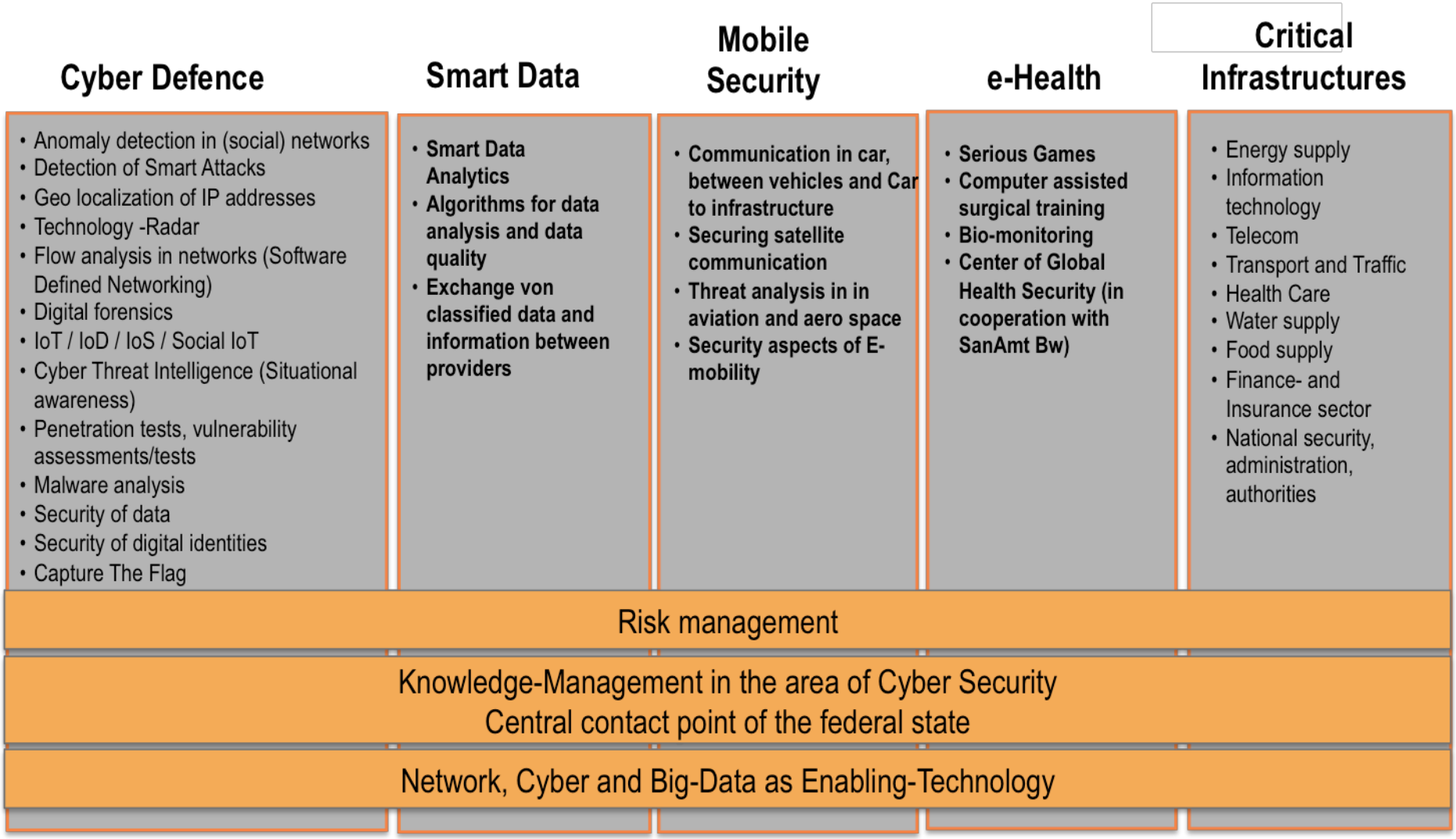
Universität der Bundeswehr München

- 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
  - Events: https://www.unibw.de/code/events-u/veranstaltungen

# CODE's Forschungsbereiche

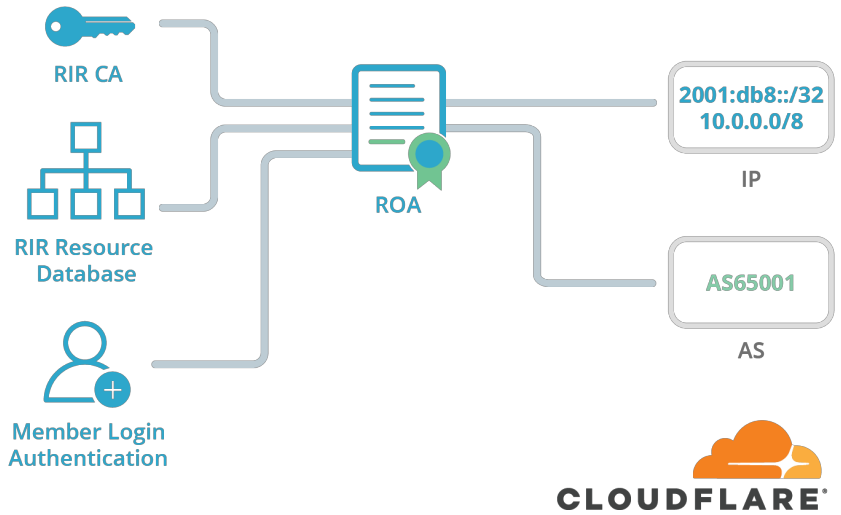
Universität der Bundeswehr München



# Ziel heutiger Veranstaltung



# RPKI Measurements




Ansprechpartner: Nils Rodday
Email: nils.rodday@unibw.de

# Resource Public Key Infrastructure (RPKI)



- Problem:
  - Routing in the Internet is based on BGP, but BGP announcements are not validated
    → BGP is insecure
  - BGP hijacking is a huge attack vector

- Solution:
  - Make sure that the originator of a BGP announcement is allowed to make such an announcement.
  - How? → By using a Public-Key-Infrastructure we make sure that every autonomous system that is receiving BGP announcements is able to validate those by using certificates.

- Our contribution as CODE:
  - Measure deployment and adoption rate of RPKI. RPKI is currently being deployed and the community needs to be able to monitor its success. → Hot topic!

- YOUR contribution as a student:
  1) Use Python to analyze huge datasets of BGP announcements on powerful machines
  2) Design and setup experiments in collaboration with PhD students
  3) Perform & validate experiments using the BGP Peering testbed and active traceroute measurements (PlanetLab / RIPE Atlas)

# CERTIFICATE VALIDATION STRATEGIES IN PUBLIC LEDGER-BASED SUPPLY CHAINS: APPLICATIONS IN MISSION CRITICAL SUPPLY CHAINS

**Problem**: In ledger supported supply chains, PKI makes an integral part; these PKIs can be based on existing infrastructures. The goal they serve can be mission critical in terms of scope and span of the partnership across the supply chain.

**Objective**: To determine certificate validation conditions in a deterministic way;

**To Do's**: Analyse supply chain flows; analyse the public ledger registrations; certificate validation paths; validation reporting; dependencies at the application level

*For more information: COD2 (Andreas Mitrakas)*

# P4 - Programming language for Software-Defined-Networking

Ansprechpartner: Nils Rodday / Klement Streit
Email: nils.rodday@unibw.de / klement.streit@unibw.de

# P4



- Why p4?
  - Advantage of SDN: Software-Defined, dynamic, agile
  - But: SLOW!
  - P4 is keeping the programmability but combines it with the execution on hardware that is specialized for such tasks → Combining software-defined programming with speed!

- Situation:
  - We currently have 2 Agilio CX 2x10GbE networking cards that are p4 capable and are available for this project.
  - Experiment setup: 2 PCs, each with one p4 card installed which are connected via fiber.

- Our contribution as CODE:
  - Accelerate the adoption of SDN products in commercial setups by providing examples of functioning use-cases and feasibility studies.

- YOUR contribution as a student:
  1) Design use-cases where p4 can be an improvement to the current state-of-the-art
  2) Implement the use-case in p4 and run experiments
  3) Validate experiments by comparing the results with prior research

-> p4 is currently picking up! – You will be working on next generation networking equipment!

# MTD – Moving Target Defense

Ansprechpartner: Nils Rodday / Raphael Labaca Castro
Email: nils.rodday@unibw.de / raphael.labaca@unibw.de

# Moving Target Defense

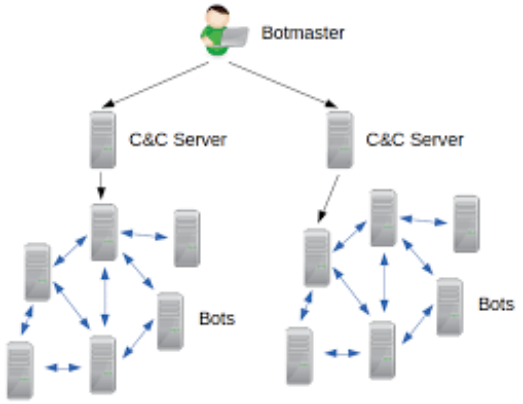
Universität der Bundeswehr München

- Problem:
  - Network-based attacks are still common and firewalls/IDS cannot entirely prevent them
- Approach:
  - MTD is trying to reduce the attack surface by “moving“ the target system.
  - Methods: IP-Address shuffling, port hopping, etc.
- Our contribution as CODE:
  - Improve current defense techniques and provide functioning examples to the industry and government as to how MTD can be used to mitigate threats.
- YOUR contribution as a student:
  1) Implement a MTD technique of your choice (e.g., using Python, JAVA, C)
  2) Build a use case for that MTD technique and the experiment setup (VM or real)
  3) Evaluate the MTD technique by running attack scenarios and measure the protection level

→ This topic also allows for a team of two or three to work together and evaluate their MTD implementations against each other!

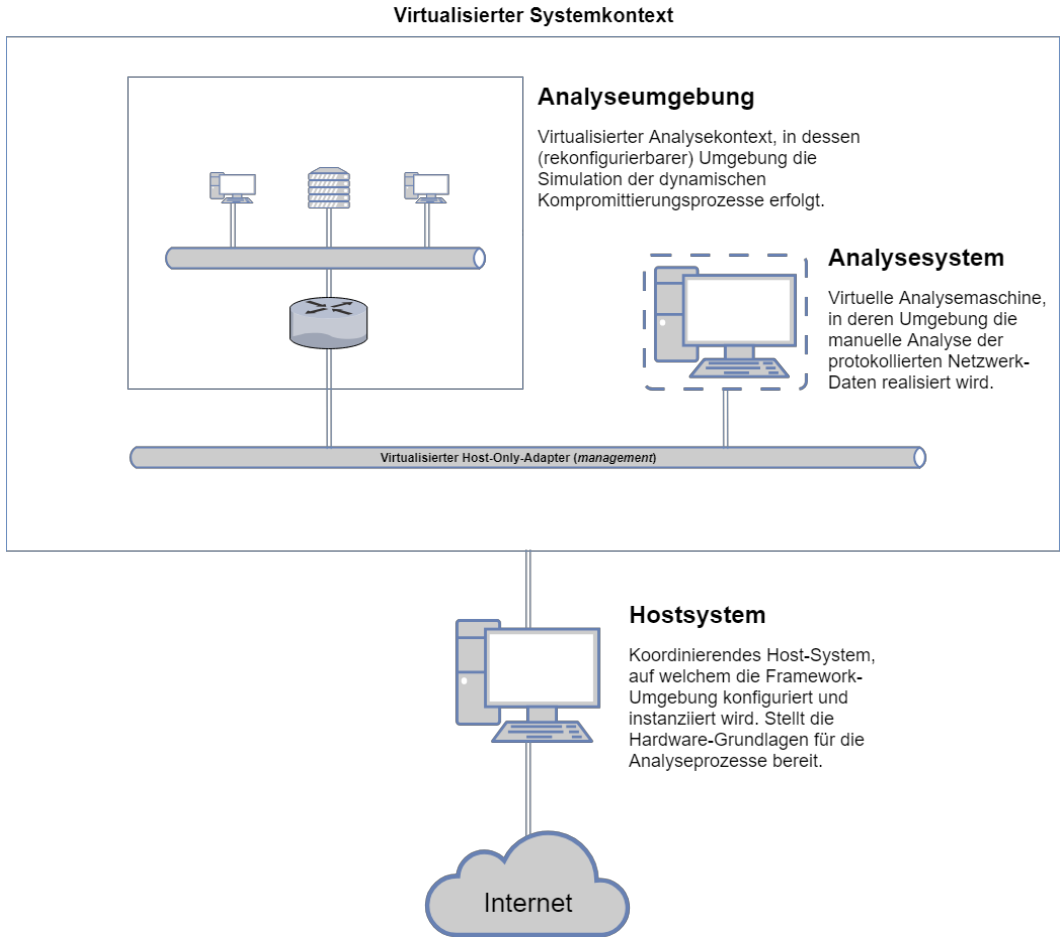
# Themengebiet Botnetze (Verhaltensanalyse & Früherkennung)

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)



- 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)



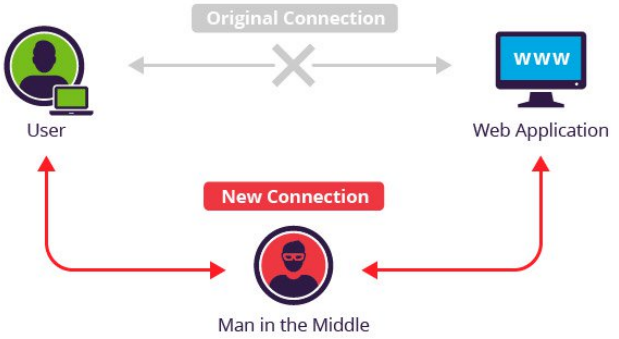
- Ziel: Ermöglichen der Analyse von Netzwerkmitschnitten trotz Einsatz von Verschlüsselung.

- Bereits implementiert:
  - Rudimentäre MITM Techniken

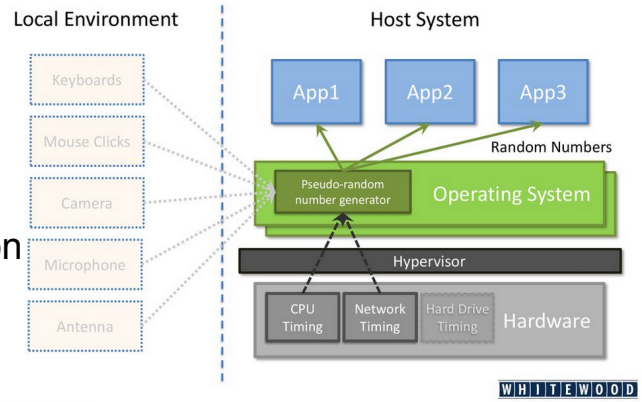
- TODOs:
  - Allgemein:
    - State-of-the-Art Analyse

  - 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

# SEARCHABLE ENCRYPTION

**Problem**: Perform search on encrypted data saved in the cloud,

**Objectives**: Allowing users to protect their data through encryption while at the same preserving search ability.

**To Do's**: Research on searchable encryption allowing users to protect encrypted data while at the same preserving search ability on the server side in situations where for example data is outsourced to the cloud.

*For more information: COD3 (Demosthenes Ikonomou)*

# CRYPTOGRAPHY

**Problem**: Preserving privacy and data protection in future applications such as car-2-car communications.

**Objectives**: By using cryptographic technologies as well as related techniques (e.g. blockchain) in different context than what is generally known for (for instance crypto currencies).

**To Do's**: Use of cryptography and related technologies (e.g. blockchain) in establishing privacy and data protection in car-2-car applications.

*For more information: COD3 (Demosthenes Ikonomou)*

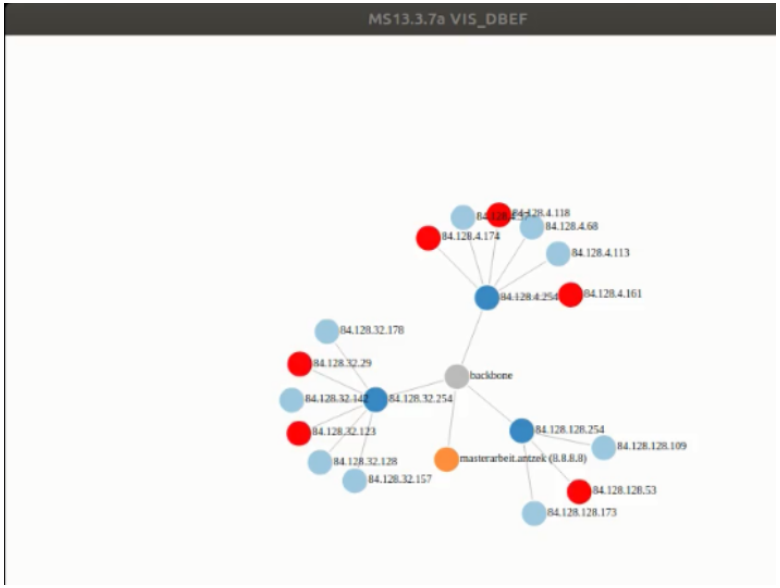
# Visualisierung und Analyse von Ausbreitungscharakteristiken (BA)

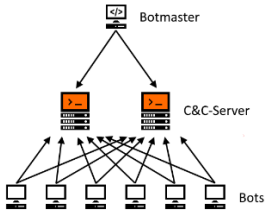


- Ziel: Struktur und Rollen (Relays, Controller, Bots, Dropping Server, etc. ) von Botnetz Instanzen erkennen.

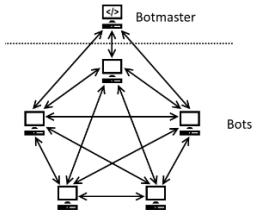
- Bereits implementiert:
  - D3.js basierter Prototyp (NetworkX)
  - Visualisierung der Topologie
  - Farbliche Markierung der Infizierten Hosts

- TODOs:
  - Konzeptentwicklung
  - Dashboard Entwurf
  - Visualisierung von Metriken
  - Integration von Live-Filter Möglichkeiten
  - Prototypische Implementierung
  - Evaluation in verschiedenen Szenarien

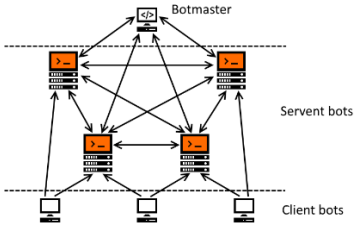


Zentralisierte Botnetz-Struktur



Dezentralisierte Botnetz-Struktur



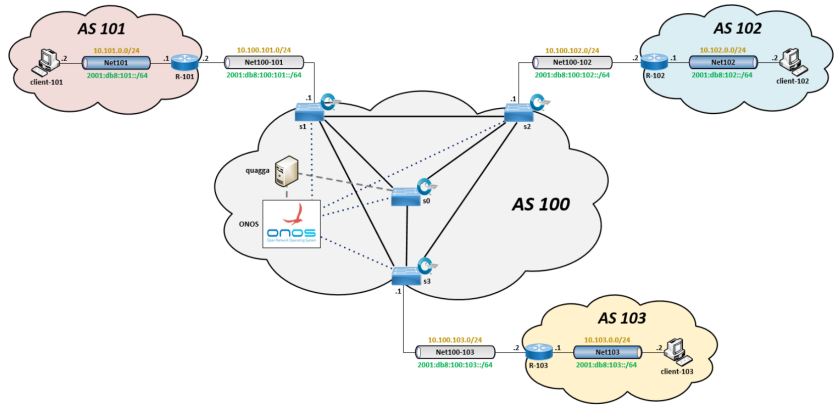
Hybride Botnetz-Struktur

# Integration von SDN zur Vernetzung der Hosts

- Ziel: Dynamische und skalierbare Netzstruktur.

- Bereits implementiert:
  - Routing auf Basis von VirtualBox Interfaces mit GNS3 (Dynamips)

- TODOs:
  - Konzeptentwicklung
  - Implementierung entsprechender Module für das Framework
  - Integration in das Framework
  - User Interaktion für Anpassungen im Live-Betrieb
  - Evaluation (z.B. verschiede Referenztopologien)

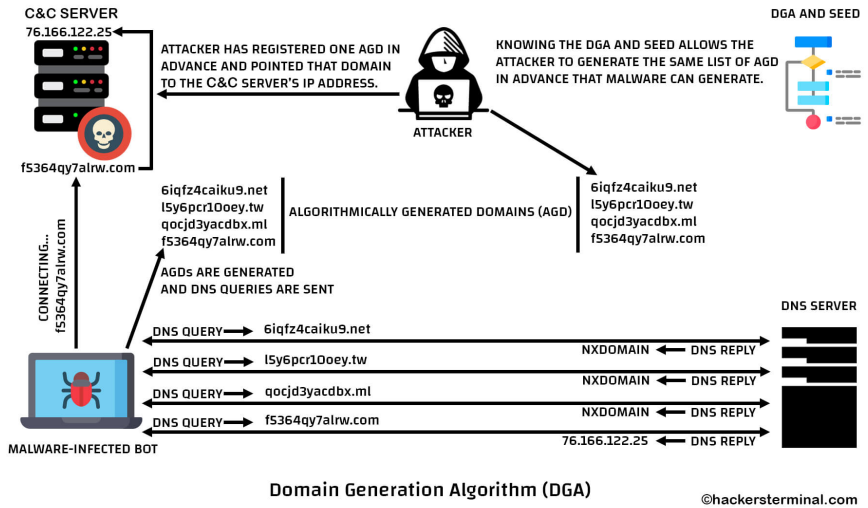



Quelle: http://oukas.info/?u=ONOS+Tutorial++SDN+Hub

# Vorhersage von Botnet Domains (MA)

- Ziel: Vorhersage von AGDs (Algorithmically Generated Domains) mit Neuronalen Netzen für verschiedene Botnetze.

- TODOs:
  1. Evaluation bestehender Ansätze
  2. Prototypische Implementierung ausgewählter Ansätze
  3. Generierung bzw. Aufbereitung von Trainingsdaten
  4. Evaluation (Erkennungsraten, ROC, …)




Quelle: https://hackersterminal.com/domain-generation-algorithm-dga-in-malware/

# 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 Usable Security and Privacy

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

Ansprechpartner 2: Dr. Ken Pfeuffer
Email: ken.pfeuffer@unibw.de

# Biometrische Verhaltensanalyse

der Bundeswehr Universität München

- Verhalten (Bewegung) messen
- Identifikation & Authentifizierung
- Full-body & Object motion tracking
- Verbindung von echter & virtueller Realität

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

Ansprechpartner 2: Dr. Ken Pfeuffer
Email: ken.pfeuffer@unibw.de

# Enhance immersion in VR

- Participant should be completely immersed in the environment.
- How can gaze and personal avatar enhance immersion?
- Explore visualization techniques in Multi-user VR environment

- Open Topic:  Social Gatherings in VR
- Radiah Rivu: sheikh.rivu@unibw.de

# Neue Authentifizierungskonzepte

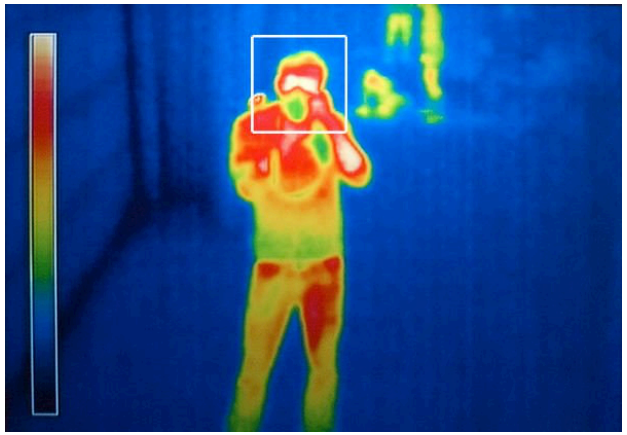
- Password / PIN / Pattern populär aber unsicher
- Trade-off zwischen Usability und Security
- Beispiele
  - Authentifizierung in AR mit der Microsoft Hololens
  - Bildbasierte Authentifizierung basierend auf Familiarity
  - Authentifizierung durch Blickbewegung

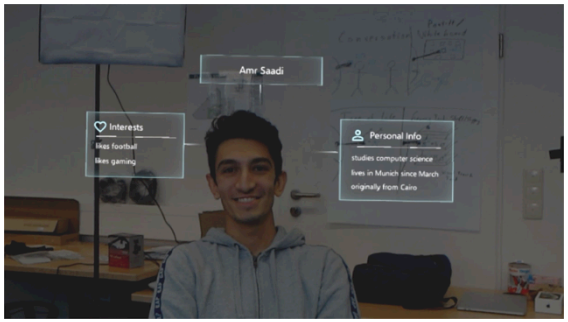
Ansprechpartner: Prof. Florian Alt
Email: florian.alt@unibw.de

Ansprechpartner 2: Dr. Ken Pfeuffer
Email: ken.pfeuffer@unibw.de

# Physiologische User Interfaces

- Thermal imaging
- Eye-tracking
- 3D UI (Augmented Reality, Virtual Reality)






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

Ansprechpartner 2: Dr. Ken Pfeuffer
Email: ken.pfeuffer@unibw.de

# Usable Security in Smart Homes

Universität der Bundeswehr München

- “smarte” Geräte halten zunehmend Einzug in das Zuhause von Nutzern
- “smarte” Geräte können zunehmend auf personenbezogene, sensitive Daten zugreifen
- trotzdem stellen sie oft unzureichende oder gar keine Sicherheits-/Authentifizierungs-Mechanismen zur Verfügung
- herkömmliche Mechanismen sind im smart Home schwer (d.h. nicht benutzerfreundlich) oder gar nicht anwendbar (z.B. keine Eingabemaske an einer Glühbirne)

- Open Topic: Privacy Mental Models of Smart Homes

Sarah Prange | sarah.prange@unibw.de

# Themengebiet Adversarial Learning for Malwaren Classification

Ansprechpartner: Raphael Labaca Castro
Email: raphael.labaca@unibw.de

# Adversarial Machine Learning against Malware Classifiers



- Adversarial examples have been extensively studied for image classification and partially in Android malware but more applications in the Windows malware domain are still needed.
- Adversarial learning is important in general to ensure AI safety because it forces the model to act in unexpected ways, which allows to observe its behavior under worst case input.

- **Goal**: Work on the implementation of a model (e.g.: Neural Network, Light GBM, etc.) in order to benchmark against existing proposals.

# A GLOBAL SECURITY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE

**Problem**: Artificial Intelligence (AI) involves a broad spectrum of technologies and has the potential to bring a paradigm shift in cybersecurity. On one hand, AI can serve as a tool to assist security operations and lead to enhanced threat intelligence. On the other hand, AI itself bears a series of novel risks that might hinder its widespread deployment and have adverse implications. The latter aspect is of particular importance, since there is currently a lack of global security frameworks for AI. Relying heavily on massive amounts of data and evolutionary and self-optimizing algorithms, AI necessitates security frameworks that go beyond existing well-established IT security ones. Whereas the particularities of different applications scenarios and context of use are important to take into account, the underlying principles of AI are pervasive and this further motivates the need for relevant security frameworks.

**Objective**: To frame the problem of AI cybersecurity using a methodological approach, based on both qualitative and quantitative metrics and taking into account the dynamic and self-evolving, unsupervised operation of AI technologies. This will assist in building a theoretical framework, based on which a generic and widely applicable security analysis of AI can be performed, which will furthermore allow to draw comparisons between different implementations.

**To Do's**: Desktop research of existing AI security frameworks and related work. Build a theoretical model (qualitative and quantitative) of AI cybersecurity. Build a security framework (threat model included) to address identified security challenges. Define general security measures that satisfy the global security framework (at a later stage these can be drilled down to specifics based on context of use).

*For more information: COD1 (Evangelos Ouzounis, Apostolos Malatras)*

# ARTIFICIAL INTELLIGENCE PROCESS CONTROL

**Problem**: In traditional data processing systems and relational databases, data subjects and data protection authorities can query databases and inspect processes and procedures to identify how data is processed. With Machine Learning processes operating as a 'black box' to the user, algorithms provide no explanation for their results. Thus, the lawfulness, fairness and transparency of personal data processing cannot be assessed.

**Objective**: To avoid misuse and undesirable outcomes from Artificial Intelligence algorithms, the introduction of controls will be required during its execution. AI algorithms can work autonomously and create machine-centred feedback mechanisms, hence the requirement of having a process to control and, when possible, validate the results avoiding the 'black box' effect.

**To Do's**: Research on a model that implements an AI process control.

*For more information: HSA (Marco Barros Lourenco)*

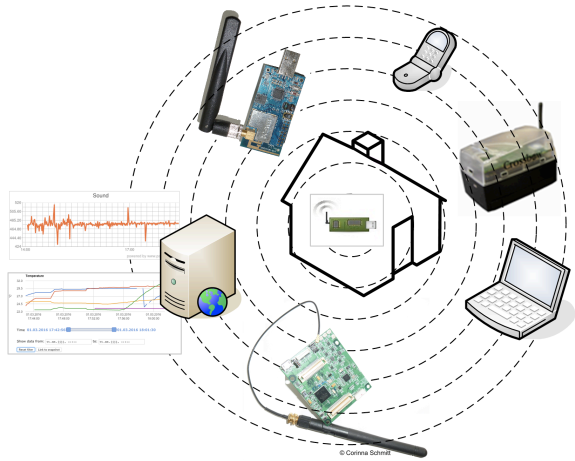
# Reverse-engineering Blackbox Malware Classifiers



- Black box malware classifiers rely mostly in security by obscurity, which means neural networks are unknown to the user.
- However, different attack approaches have been implemented to infer how the model is created and eventually being able to create a separate model with similar parameters.
- If a model can be ‘extracted’ and re-created, an attacker would be able to design specific attacks tailored to any targeted model.

- **Goal**: Implement an existing approach to reverse-engineer black-box models based on an existing state-of-the-art literature research from a *Seminararbeit*.

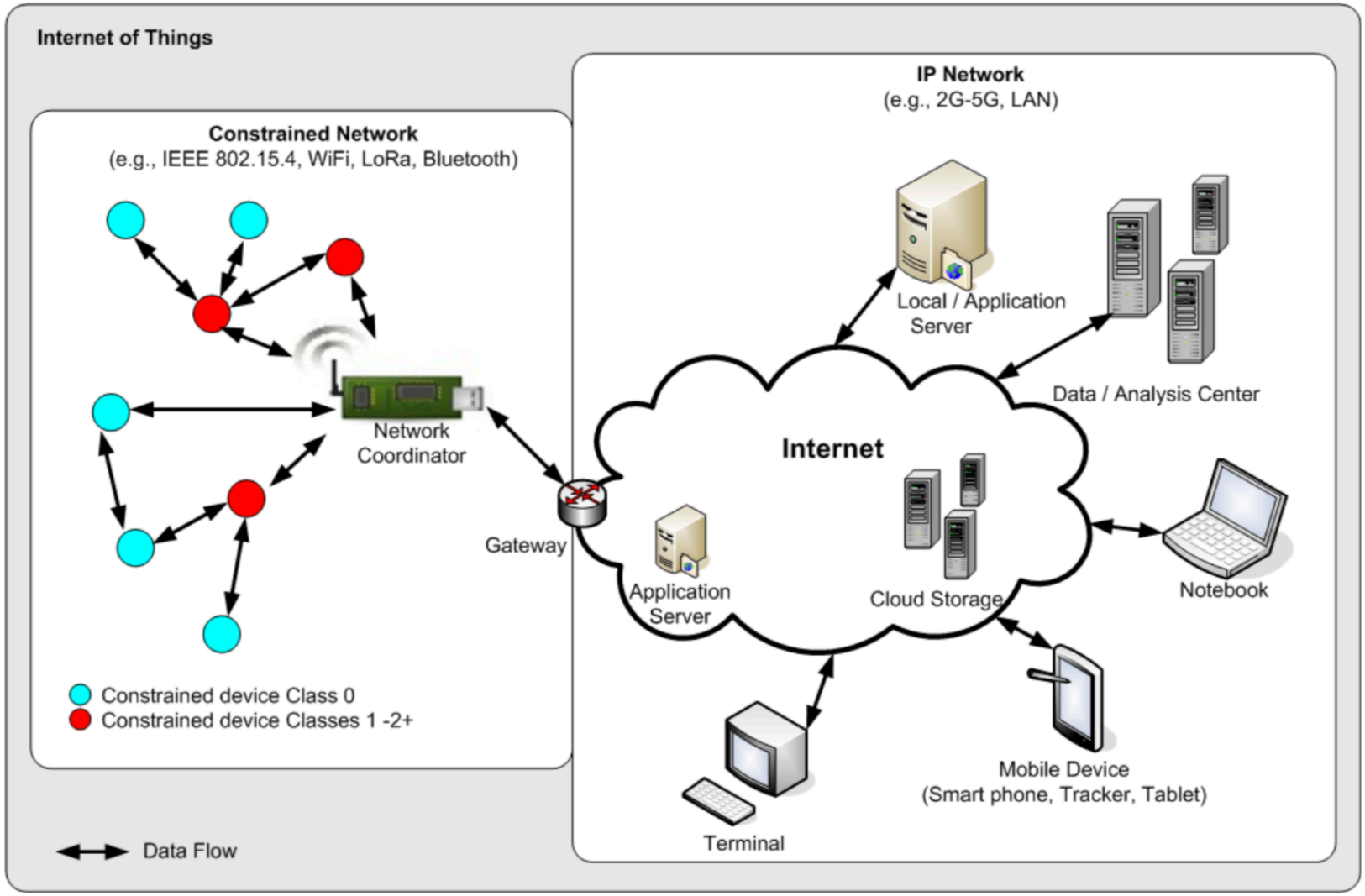
# Themengebiet Sensornetze (SecureWSN)



Ansprechpartner: Corinna Schmitt
Email: corinna.schmitt@unibw.de

Homepage: https://corinna-schmitt.de/securewsn.html

# SecureWSN - Konzept

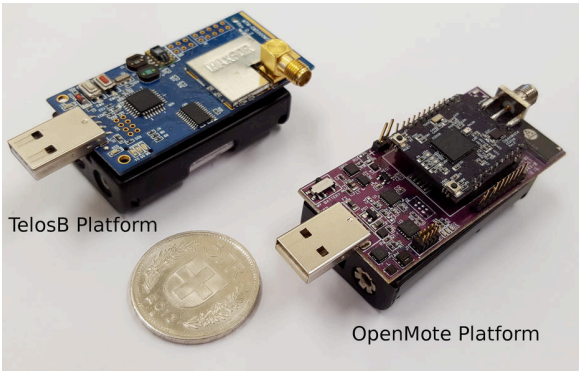


# Hardwareintegration



- Bereits angebunden:
  - OpenMote – OS Contiki
  - TelosB, IRIS, OPAL – OS TinyOS

- Ziel: Integration von Knoten mit RIOT OS als Betriebssystem
  - Auf dem Knoten:
    - Datenformat TinyIPFIX implementieren (RFC 8272)
    - Aggregationssupport
    - Pull-Support
  - Auf dem Gateway und im Backend
    - Gatewaysupport für RIOT OS (u.a. Konfiguration, Datenübersetzung)
    - Datentransfer zum Backend und Integration in Datenbank



# Sicherheitsprotokolle



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

- Möglichkeiten:
  - Pre-shared Ansatz*
  - Elliptic Curve Cryptography
  - DTLS und zertifikatbasiert

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

https://betanews.com/2013/11/12/qa-with-secure-communications-service-perzo/

* Nur für Knoten mit RIOT OS

# Alarmsystem



- Ziel: Netzeigentümer soll informiert werden, wenn Knoten Werte meldet, die vom „gewöhnlichen“ Verhalten (bspw. hohe Temperatur = Feuer) abweichen.

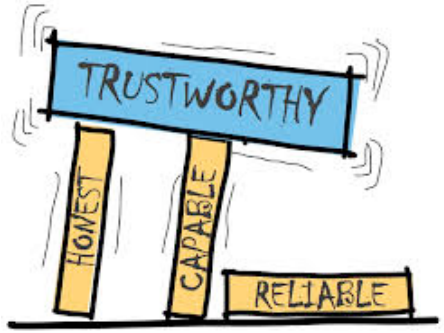
- ToDos:
  - Konzeptentwicklung
    - Analyse aktueller Daten vs. zuvor übermittelter Daten
    - Interaktion mit Netzeigentümer
  - Implementierung u.a.
    - Analyse von Daten
    - Visuelle Warnung im hinterlegten Raumplan
    - Elektronische Warnung (bspw. Mail)
    - Eintragung ins existierende Logging-System
  - Evaluation – „Proof of Concept“

# Test auf Vertrauenswürdigkeit



- Aktuelle Situation
  - Jeder Knoten darf in Richtung Gateway kommunizieren
- Problem
  - „Bösartiger“ Knoten kann Daten ins System übertragen, wenn gewählter Kommunikationskanal bekannt ist und entsprechende Applikation/Protokoll unterstützt wird.

  → Falsche Daten können ungewollte Reaktionen auslösen!
- Ziel: Integration einer „Trust-Checks“ im System
- ToDos:
  - Konzeptentwicklung und Hardwarespezifikation
  - Implementierung des Trust-Checks
  - Reporting im Logging-System & Warnung an Netzeigentümer
  - Evaluation – „Proof of Concept“



https://www.bepioneer.net/blog/are-you-trustworthy

# ESTABLISHING TRUST THROUGH REPUTATION BASED TECHNIQUES

**Problem**: Establishing privacy through trust and reputation based techniques and algorithms. Use reputations based techniques commonly used in the past in peer-2-peer architectures as alternatives in establishing privacy trust.

**Objectives**: Use reputations based techniques commonly used in the past in peer-2-peer architectures as alternatives in establishing privacy trust.

**To Do's**: Use reputations based techniques and technologies commonly used in the past in peer-2-peer architectures as alternatives in establishing privacy trust in a seamless manner.

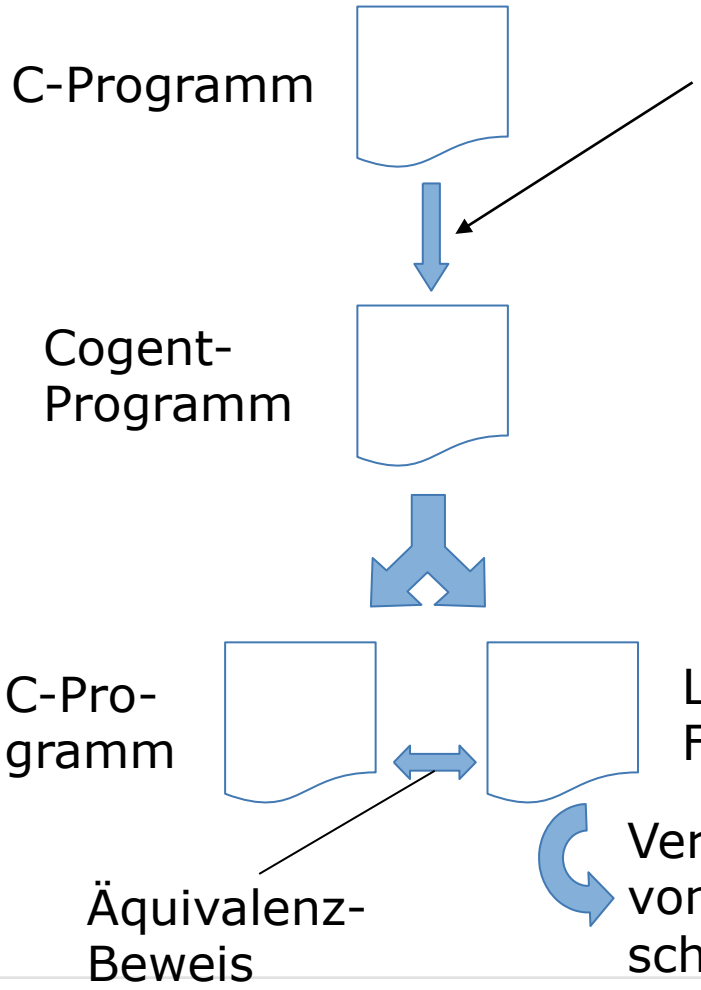
*For more information: COD3 (Demosthenes Ikonomou)*

# Themengebiet Programmverifikation

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

# Bachelor-Arbeiten im Code-Projekt HoBit

(hochsicheres Betriebssytem für embedded IT)




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

# QUANTITATIVE TECHNIQUES FOR SECURITY VERIFICATION OF CODE

**Problem:** Code is at the heart of all IT operations and systems and it is widely one of the last concerns when it comes to security. While there exists a series of secure software development lifecycle (SDLC) guidelines, whether they are used in practice and how can one validate this is a widely unexplored territory. The huge amounts of code being generated every day (big chunks of which are automatically generated by IDEs, evolutionary algorithms, software frameworks, etc.), the reuse of APIs and virtualization, are few of the challenges that make it difficult to verify the proper implementation of security of code. Moreover, the disparity in the definition of quantitative metrics to assess security verification of code further exacerbates relevant concerns.

**Objective:** Based on existing secure SDLC guidelines, devise a model of security features to assess their systematic application in code development. With the model at hand, define a series of quantitative metrics to evaluate at what degree the properties of the model are satisfied. Implement a web-based tool to automatically verify security of code snippets (focusing on one programming language, but designed to allow for generalization) using the aforementioned metrics.

**To Do's:** Desktop research and analysis of existing secure SDLC guidelines and related work. Build a theoretical model of security features for security verification of code. Define quantitative metrics to assess the extent to which the aforementioned security features have been implemented. Develop a web-based tool to automatically perform security verification of code based on said metrics and focusing on a particular programming language.

*For more information: COD1 (Evangelos Ouzounis, Apostolos Malatras)*

THE EU CYBERSECURITY AGENCY

# ADDITIONAL ENISA TOPICS

# SECURITY APPROACHES FOR RAPIDLY EVOLVING TECHNOLOGY

**Problem**: The rapid evolution of technologies (e.g. AI, quantum computing, hyper-connectivity, bio-inspired computing to name a few) is in general outpacing related security efforts. This has been illustrated in the case of the Internet of Things (IoT), where research and technology developments were initially made without considering the aspect of security. When security is not considered in the design phase, it is usually the case that significant efforts need to be placed to catch up and implement security a posteriori in an efficient and effective manner.

**Objective**: Devise a model of the lifecycle of evolution of technologies, focusing on latest examples that have rapidly emerged. Considering one case of a rapidly evolving technology, e.g. AI, devise a forecasting method (or adapt an existing one such as DELPHI) to include security-by-design considerations in the context of the evolution cycle. Develop an iterative methodology that considers the different stages of the aforementioned lifecycle and adapts the adopted security framework based on an evolving threat model.

**To Do's**: Desktop research and analysis of existing methods for forecasting of evolving technology and related security work. Design a security-by-design lifecycle model for rapidly evolving technology and integrate it into an existing forecasting method. Validate the method using a specific technology with rapid evolution features, e.g. AI, and identify good practices and shortcomings. Develop an iterative methodology to adapt the security framework of such technologies using a continuously changing threat model.

*For more information: COD1 (Evangelos Ouzounis, Apostolos Malatras)*

# CORRELATION BETWEEN CERTIFIED PRODUCTS AND VULNERABILITIES

**Problem**: Certification is a standardized process for acknowledging that products and services pass specific performance and quality assurance tests and/or meet specific criteria. In the cybersecurity domain, certification acts as proof that a product or service implements specific measures to mitigate cybersecurity risks. Measures and implementation criteria are usually outlined within the certification process. While certification processes provide a common ground for achieving a basic level of cybersecurity, still a growing number of certified products and services are found to be vulnerable to numerous threats.

**Objective**: Develop a report using open source intelligence, technical reports and available statistics and trends on vulnerabilities, with a focus on presenting potential correlations between certified products and detected vulnerabilities on some type of product (for all published versions). Aggregate vulnerability statistics for similar (both certified and non-certified) product types and services and analyse trends, both in terms of type and amount of vulnerabilities detected. Using the knowledge acquired, provide insight on: (i) whether certification processes aid products and services in lowering the number of critical vulnerabilities, (ii) differences between certified and non-certified products, based on the amount and criticality level of detected vulnerabilities, and (iii) specific types of products and groups of services where certification seems to have a greater (or smaller) impact.

**To Dos**: Desktop research and analysis of existing open source intelligence, technical reports and available statistics and trends on vulnerabilities for the past years; both from the industry, university labs and government publications. Develop a statistical report of vulnerabilities per type of device/service. Define products and services with the highest and lowest amount vulnerabilities. Aggregate and correlate findings to produce useful insight on the effect of certification on products and services per type of product/service and per type of vulnerability

*For more information: COD1 (Evangelos Ouzounis, Apostolos Malatras)*

# ROBOTS IN THE DOCK WITH CRIMINALS: AI AND THE GENEVA CONVENTIONS CONCERNING WAR CRIMES

**Problem**: Unmanned systems have been used to carry out lethal missions

**Objective** To determine the limits of human intervention and control over unmanned systems in a cybersecure operational environment.

**To Do's:** Analyse the key areas of algorithmic processing; analyse key data sources; analyse control features; analyse cybersecurity for control features; determine the discretion margins of the AI agent; determine the time and spatial limits of control; determine the deltas of human intervention; analyse the provisions of war crimes; determine the crimes that come in scope

*For more information: COD2 (Andreas Mitrakas)*

# DATA ORCHESTRATION UNDER THE EDGE COMPUTING PARADIGM

**Problem**: Edge computing is supposed to help dealing with a deluge of data coming from sensors, phones, cars, IoT devices and such. Processing data near where it is collected will help with issues of latency and the challenges of moving large datasets back to the cloud. The movement of this data may pose serious threats to the protection of user privacy and data and the operation of complex systems that depend on this data to deliver critical services.

**Objective**: Developers need to build a strategy for orchestrating and securing the movement of data for their applications assuring its integrity and availability in edge and fog architectures.

**To Do's**: Research on a model for Data Orchestration under the Edge Computing paradigm.

*For more information: HSA (Marco Barros Lourenco)*

# IDENTIFYING ABUSIVE BEHAVIOR IN DIGITAL PLATFORMS

**Problem**: A major technical challenge for operators of digital platforms such as social media is to develop sentiment analysis algorithms capable of detecting abusive and anti-social behavior such as hate speech, offensive language, trolling and cyber bulling without crossing the line of censorships. There is simply too much content on these platforms and too many people with motives to deceive and manipulate.

**Objectives**: From the analysis of large datasets and user content, identify patterns of abusive behavior and fake profiles that may incur in malicious actions.

**To Do's**: Research on the development of a model capable of identifying abusive behavior in Digital Platforms from the analysis of large data sets without crossing the line of censorship, invading user privacy, compromising performance and user experience.

*For more information: HSA (Marco Barros Lourenco)*

# SECURE CODE DEVELOPMENT

**Problem**: As systems (e.g. communication neteworks) tend to become more complex and are the result of 'contributions' by multiple vendors the need for secure and reliable code becomes imperative.

**Objectives**: Secure code development especially in the context of supply chains of multiple different vendors is a topic that especially in the last year has attracted considerable attention.

**To Do's**: Use techniques developed in other field (e.g. PC S/W development) of secure code development especially in the context of supply chains in the context of complex systems supported by multiple vendors.

*For more information: COD3 (Demosthenes Ikonomou)*

# ADDITIONAL SUGGESTIONS

Hands-on proposals:

- Set up a matrix.org instance that could be maintained by ENISA staff and could be used for testing in the CNW.
- Include an assessment of the strong/weak points but unlike the study that was done, base this on the actual findings from deploying it and running it.
- Have somebody create/code something that could serve as a dashboard in the CNW portal and uses data from either sitreps (technical and situational) and/or Cyber Weather data
- This could be integrated with or even based the OpenCSAM search engine from ENISA
- Certificate-based (SMIME/A) e-mail encryption via DNSSEC

*For more information: CR (Andrea Dufkova)*

# Weitere Themenbereiche

Universität der Bundeswehr München

- Social Media – Florian Steuber, florian.steuber@unibw.de
- SDN – MANET – Klement Streit, klement.streit@unibw.de
- Und vieles mehr!

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

# Kontakt zu uns

- Email direkt an Themensteller
- Infos:

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

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