Projektseminare

WS 2021/22

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Universität Regensburg

Universität Regensburg

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Erweiterung einer Analyseumgebung um eine inhaltsbasierte Untersuchung von digitalen Beweisen

- **Beschreibung:**
  - Es wurde ein Prototyp für eine IT-forensische Rekonstruierung von Arbeitsabläufen (Geschäftsprozesse) geschaffen
  - Dieser Prototyp soll um die Fähigkeit der Analyse von bestimmten Merkmalen innerhalb der wiederhergestellten Dateien erweitert werden

- **Ziele:**
  - Definition relevanter Merkmale (wie z.B. Metadaten, Zeitangaben und Verweise auf weitere Verzeichnisse und Daten)
  - Eine prototypische Umsetzung zur Extraktion dieser Merkmale

- **Voraussetzungen:**
  - Gute Programmierkenntnisse in Java, nodeJS, bash oder Python
  - Grundkenntnisse in Linux sind vorteilhaft aber nicht notwendig

- **Mögliche Bearbeiter:** 2 Personen (max.) – als Team!
- **Betreuer:** Ludwig Englbrecht (ludwig.englbrecht@ur.de)

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Datenanalyse von MISP-basierter Cyber Threat Intelligence

- **Beschreibung:**
  - Cyber Threat Intelligence (CTI) wird mit verschiedenen Datenformaten strukturiert. MISP stellt ein solches Datenformat sowie eine CTI Sharing Plattform dar.
- **Ziele:**
  - MISP als Datenquelle (Datenformat, Datenabruf, etc.)
  - Identifizierung geeigneter Methoden der Datenanalyse
  - Analyse der MISP-CTI mittels Implementierung (z.B. in Python)
  - Bewertung der Ergebnisse der Datenanalyse
- **Voraussetzungen:**
  - Grundlegende Programmierkenntnisse
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Daniel Schlette (daniel.schlette@ur.de)

Implementierung von IAM KPI Bausteinen

NEXIS

- **Beschreibung**
  - Key Performance Indicators (KPIs) werden in Unternehmen verwendet, um bspw. Prozesse, Projekte oder Abteilungen zu kontrollieren oder zu bewerten.
  - Da jedes Unternehmen variiert, benötigt ein Unternehmen ein individuelles Set an KPIs, um Entscheidungen auf Basis von hochwertigen Indikatoren zu treffen.
  - Ein sicherheitsrelevanter Unternehmensbereich, der über KPIs überwacht werden kann, ist das Identity and Access Management (IAM).
  - Individuell auf Unternehmen zugeschnittene und qualitativ hochwertige KPIs sind daher ein Beitrag zur Erfassung und Verbesserung deren IT-Sicherheit.
- **Ziel**
  - Rudimentäre Erfassung von relevanten Kennzahlen für das IAM.
  - Implementierung eines Software Moduls, um KPIs zu verwalten und zu berechnen.
  - Programmiersprachen: Java, SQL
- **Betreuung und Organisatorisches**
  - Thomas Baumer (thomas.baumer@nexis-secure.com)
  - Verfügbare Plätze: 2 Personen
  - Voraussetzungen: OOP, Datenbanken im Unternehmen

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Visualisierung einer simulierten Anlage für eine Cyber Range

- **Beschreibung:**
  - Cyber Ranges sind virtuelle Umgebungen, die reale Systeme nachbilden, um Menschen damit auszubilden
  - Diese sollen möglichst realitätsnah abgebildet sein, um einen optimalen Lernerfolg zu erzielen
- **Ziele:**
  - Erweiterung einer bestehenden Cyber Range um eine geeignete Visualisierung:
    - » Ist Zustand: Zustände einer Abfüllanlage werden aktuell durch Logs dargestellt
    - » Soll Zustand: Visualisierung der Zustände (z.B. Füllstand der Flasche)
- **Voraussetzungen:** Programmierkenntnisse, Kreativität
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Manfred Vielberth (manfred.vielberth@ur.de)

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Integration eines SIEM Systems in eine Cyber Range

- **Beschreibung:**
  - Cyber Ranges sind virtuelle Umgebungen, die reale Systeme nachbilden, um Menschen damit auszubilden
  - SIEM Systeme sind Sicherheitssysteme, mit deren Hilfe Ereignisse analysiert werden können, um mögliche Sicherheitsvorfälle zu erkennen
- **Ziele:**
  - Austausch des SIEM Systems einer bestehenden Cyber Range
  - Dsiem soll durch Wazuh ausgetauscht werden
  - Deployment mittels Docker
- **Voraussetzungen:** Programmierkenntnisse
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Manfred Vielberth (manfred.vielberth@ur.de)

Dsiem

docker

Bachelorarbeiten

WS 2021/22

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Universität Regensburg

Analyse und Bewertung von Methoden zur IT-forensischen Analyse im Personal Internet of Things (PIoT)

- **Beschreibung:**
  - Durch den steigenden Einsatz des Internet of Things (IoT) und von IoT-Geräten in Haushalten und in der unmittelbaren Umgebung einer Person werden persönliche IoT (PIoT)-Netzwerke geschaffen (z. B. Smart Home, Smart Devices).
  - Welche Konzepte zur IT-forensischen Analysen im Bereich des PIoT bestehen, soll die Durchführung einer systematischen und strukturierten Literaturrecherche mit einer Klassifizierung der Ergebnisse hinsichtlich der Forschungsfrage erläutern.
- **Ziele:**
  - Darstellung des aktuellen State-of-the-Art und mögliche Ableitung von Forschungslücken im Bereich der PIoT-Forensik.
  - Kategorisierung und Bewertung der extrahierten Methoden und Konzepte im Bereich des PIoT.
- **Voraussetzungen:** *keine*
- **Betreuer:**
  - Sabrina Friedl (sabrina.friedl@ur.de)

Analyse der Verwendung von Cyber Ranges zur Schaffung von Security Awareness

- **Beschreibung:**
  - Um IT-Security Awareness in Unternehmen zu schaffen werden regelmäßig Kampagnen durchgeführt, mit denen Mitarbeiter geschult werden
  - Cyber Ranges sind virtuelle Umgebungen, die reale Systeme nachbilden, um Menschen damit auszubilden
- **Ziele:**
  - Analyse der Literatur mit der Fragestellung ob und wie Cyber Ranges in Awareness Kampagnen genutzt werden
  - Ableitung eines Konzepts für eine Cyber Range zur Schaffung von IT-Security Awareness
- **Voraussetzungen:** *Interesse für IT-Security*
- **Betreuer:**
  - Manfred Vielberth (manfred.vielberth@ur.de)

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Developing of interactive data acquisition agents for a compliance-driven continuous maturity assessment

- **Beschreibung:**
  - Ein *Capability Maturity Model (CMM)* im Bereich der Informationstechnologie konzentriert sich in der Regel auf die Entwicklungsprozesse und -phasen innerhalb einer Organisation.
  - Sie bilden eine solide Basis für eine unternehmensweite Bewertung.
  - Eine Bewertung mittels einem CMM ist sehr umfangreich und zeitaufwändig daher erfolgt ein Self-Assessment nur alle paar Jahre.
  - Dadurch erkennt man zu spät, dass bestimmte Fähigkeiten im Unternehmen ggf. nicht mehr vorgehalten werden.
- **Ziele:**
  - Prototypische Entwicklung von Datenerfassungs-Agenten
  - Strukturierte Identifizierung der Voraussetzungen anhand von Compliance-Vorgaben
  - Schaffung einer Möglichkeit für eine zeitnahe unternehmensweite Bewertung
  - Die Bachelorarbeit kann auf Deutsch oder Englisch angefertigt werden
- **Voraussetzungen:**
  - Gute Programmierkenntnisse in mindestens einer objektorientierten Programmiersprache (z.B.: Java)
  - Gute Kenntnisse in der Webentwicklung
- **Betreuer:**
  - Ludwig Englbrecht (Ludwig.Englbrecht@wiwi.uni-regensburg.de)

Universität Regensburg

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Datenqualität für Cyber Threat Intelligence

- **Beschreibung:**
  Eine zentrale Säule von Cyber Threat Intelligence (CTI) ist der Austausch von Bedrohungsinformationen. Aus diesem Grund ist die Datenqualität (DQ) für CTI von großer Bedeutung. Die verschiedenen Dimensionen von Datenqualität können mit Metriken eingehender bewertet werden.
- **Ziele:**
  - Aktueller Stand: Metriken und DQ von CTI
  - Technisches Konzept (Daten, Format, Technologie, Algorithmen)
  - Implementierung der DQ-Metriken
- **Voraussetzungen:**
  - Programmierkenntnisse, Motivation
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:** Daniel Schlette (daniel.schlette@ur.de)

Permissioned Blockchain Tokens

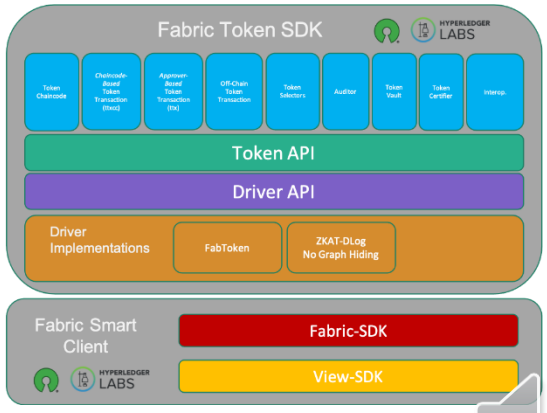
- **Beschreibung:**
  Permissioned Blockchains können auch von Tokens profitieren, die die bekannten Kryptowährungen einsetzen (z.B. zur Anreizsetzung und zum Austausch von Werten)

- **Ziele:**
  - Überblick über den aktuellen Stand der Nutzung von Token in permissioned blockchains
  - Technische Verfügbarkeit und aktuelle praktische Umsetzung. Beispiel: Fabric Token SDK (Hyperledger Labs)
  - Framework für den Einsatz von Währungs-Tokens in Unternehmensnetzwerken

- **Voraussetzungen:**
  - Grundlegendes Blockchain Verständnis

- **Mögliche Bearbeiter:** 1 Person

- **Betreuer:** Benedikt Putz (benedikt.putz@ur.de)



Praxisseminare

WS 2021/22

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

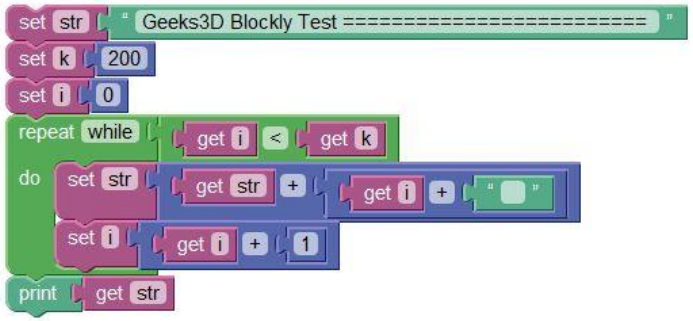
Universität Regensburg

Universität Regensburg

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Implementierung eines Ansatzes zur visuellen Erstellung von SIEM Regeln in einer Cyber Range

- **Beschreibung:**
  - Visual Programming ermöglicht es, mit Hilfe von grafischen Elementen zu programmieren
  - Cyber Ranges sind virtuelle Umgebungen, die reale Systeme nachbilden, um Menschen damit auszubilden



- **Ziele:**
  - Erweiterung einer bestehenden Cyber Range für SIEM Regeln:
    - » Ist Zustand: Regeln werden mittels JSON erstellt
    - » Soll Zustand: Regeln werden mittels Visual Programming Ansätzen erstellt
- **Voraussetzungen:** Programmierkenntnisse
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Manfred Vielberth (manfred.vielberth@ur.de)

Restrukturierung eines bestehenden Live Forensics Frameworks

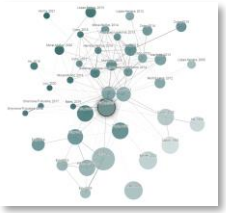
- **Beschreibung:**
  - Es wurde ein Prototyp für die passive Überwachung eines (infizierten) Smartphones entwickelt
  - Die gegebene Überwachungsumgebung ist ein Linux System mit einem WLAN-Accesspoint, wireshark, adb Bridge und einer Anbindung zu einer MongoDB
- **Ziele:**
  - Strukturierte Erfassung der gegebenen Umgebung
  - Bestimmung notwendiger Erweiterungen und eine prototypische Erweiterung umsetzen
- **Voraussetzungen:**
  - Grundlegende Linux Kenntnisse oder der Besuch der Veranstaltung „Praxis der IT-Sicherheit“ sind zwingend notwendig
  - Grundkenntnisse in bash oder Python
- **Mögliche Bearbeiter:** 2 Personen (max.) – als Team!
- **Betreuer:** Ludwig Englbrecht (ludwig.englbrecht@ur.de)

Erweiterung einer Web-Anwendungen zur STIX-basierten CTI-Erfassung

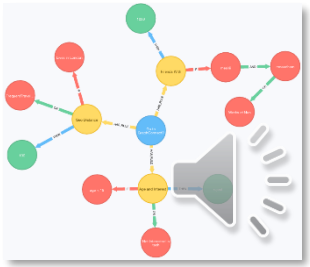
- **Beschreibung:**
  - Cyber Threat Intelligence (CTI) basiert auf strukturierten Bedrohungsinformationen über Angreifer, Malware, etc.
  - Web-Anwendung auf Basis des MEAN-Stacks bildet die Erfassung ab
- **Ziele:**
  - Erweiterung einer bestehenden Web-Anwendung
  - Erweiterungskomponenten: Usability-Aspekte, Vollständige Abbildung des STIX2.1 Standards, Hilfestellungen (Recommendations), …
  - Kreative Aufgabenstellung mit Freiheitsgraden für Umsetzung eigener Ideen
- **Voraussetzungen:**
  - Programmierkenntnisse (Webtechnologien)
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Daniel Schlette (daniel.schlette@ur.de),
  - Fabian Böhm (fabian.boehm@ur.de)

Aufbau einer Graph-Datenbank zur Sammlung wissenschaftlicher Veröffentlichungen zu Visual Security Analytics

- **Beschreibung:**
  - Bestehende, wissenschaftliche Arbeiten zu einer Thematik über unterschiedliche Datenbanken verteilt
  - Überblick über die Arbeiten und Zusammenhänge oft schwer ersichtlich
- **Ziele:**
  - Automatisierte Erfassung wissenschaftlicher Arbeiten zu Visual Security Analytics
  - Persistierung in einer graph-basierten Datenbank
  - Umsetzung unterschiedlichster, vor-definierter Abfrage

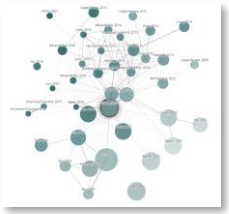


- **Voraussetzungen:**
  - Programmierkenntnisse (Internettechnologien)
  - Grundkenntnisse von NoSQL-Datenbanken (Informationssysteme – Entwicklungen und Trends)
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Fabian Böhm (fabian.boehm@ur.de)



Bibliometrische Analyse von wissenschaftlichen Veröffentlichungen im Bereich der Visual Security Analytics

- **Beschreibung:**
  - Wissenschaftliche Veröffentlichungen bieten neben den intellektuellen Erkenntnissen bspw. auch Einblicke in die Zusammenarbeit von Autoren
  - Beispiel hierfür sind Kooperationen, Zitationsnetzwerke, zentrale Autoren(gruppen)
- **Ziele:**
  - Automatisierte Durchführung bibliometrischer Analyse für den Bereich der Visual Security Analytics
  - Modulare, einfach erweiterbare Lösung im Hinblick auf Funktionalität und Datenbasis
- **Voraussetzungen:**
  - Gute Programmierkenntnisse (optimalerweise Erfahrung mit Web-Technologien und Python)
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Fabian Böhm (fabian.boehm@ur.de)



Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Untersuchung von Interoperabilitäts-Frameworks für private DLT Netzwerke

- **Beschreibung:**
  In der quelloffenen Hyperledger Community werden Technologien rund um Blockchain/Distributed Ledger entwickelt (z.B. Hyperledger Fabric und Hyperledger Besu
- **Ziele:**
  - Test der Interoperabilitäts-Projekte Weaver, YUI und Cactus
  - Visuelle Darstellung des Transaktionsablauf
  - Vergleich der Frameworks und Beurteilung der Eignung
- **Voraussetzungen:**
  - Verständnis von DLT
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:** Benedikt Putz (benedikt.putz@ur.de)

Praktische Umsetzung eines Security Orchestration Anwendungsfalles für IoT

- **Beschreibung:**
  - Klassische IT-Systeme können (im Falle eines Sicherheitsvorfalls) automatisiert/orchestriert werden
  - Internet of Things kann über klassische Mechanismen nicht orchestriert werden
- **Ziele:**
  - Umsetzung eines Use-Cases zur Sicherheitsorchestrierung
  - Erfassung der Meta-Daten des Geräts
  - OTA-Update
- **Voraussetzungen:** IT-Security I
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Daniel Schlette (daniel.schlette@ur.de)
  - Philip Empl (philip.empl@ur.de)

Ein Pattern für Digitale Zwillinge

- **Beschreibung:**
  - Digitale Zwillinge stellen virtuelle Abbilder physischer Geräte und deren Interaktion dar
  - Vielzahl an Software
- **Ziele:**
  - Identifikation relevanter Software für digitale Zwillinge
  - Extraktion der Funktionsweise und Zusammenhänge (Pattern)
- **Voraussetzungen:** IT-Security I
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Philip Empl (philip.empl@ur.de)

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Integration digitaler Zwillinge in das IoT

- **Beschreibung:**
  - Internet of Things ist eine komplexe Umgebung (Hersteller, Daten, Protokolle,…)
  - Reduktion der Komplexität durch Digital Twins
- **Ziele:**
  - Integration einer digitalen Zwilling Applikation in ein vorhandenes IoT-System
  - Definition der Konnektoren
  - Erstellung von Digital Twins
- **Voraussetzungen:** IT-Security I, Informationssysteme
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Philip Empl (philip.empl@ur.de)

Theoretische Seminare

WS 2021/22

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Universität Regensburg

Role Mining und Role Engineering: Erfolgsfaktor Datenqualität

NEXIS

- **Beschreibung**
  - Role-Based Access Control (RBAC) feiert Erfolge in Literatur und Praxis, da es die Komplexität bei der Verwaltung von Zugriffsberechtigungen reduziert.
  - Die für RBAC benötigten Rollen werden dabei über bottom-up Ansätze basierend auf bestehenden Nutzer-Berechtigung-Zuweisungen berechnet (Role Mining) oder über top-down Ansätze mittels Struktur- und Prozessanalysen abgeleitet (Role Engineering).
  - Somit hängt die gewonnene IT-Sicherheit durch RBAC von der Datenqualität ab, mit welcher die Rollen berechnet oder Strukturen und Prozesse analysiert werden.
- **Ziel**
  - Erstellung einer strukturierten Literaturrecherche zu Role Mining und Role Engineering um herauszufinden, mit welchen Dateneigenschaften gute Ergebnisse erzielt werden.
  - Aus diesen Erkenntnissen soll eine Checkliste / ein Framework erstellt werden, mit welchem die Güte eines Datensatzes bewertet werden kann.
- **Betreuung**
  - Thomas Baumer (thomas.baumer@nexis-secure.com)

Universität Regensburg

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

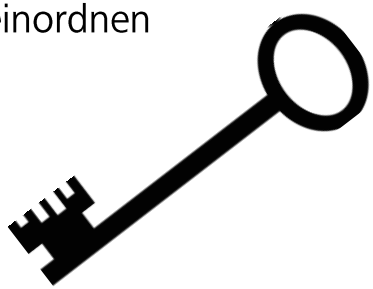
Recherche und Aufbereitung von Metriken zur Messung der Datenqualität von XACML-Policies

- **Beschreibung:**
  - Die Qualität von Zugriffskontrollregeln ist ein kritischer Faktor für die IT-Sicherheit einer Organisation und deren Administration. XACML bildet hierbei den De-Facto-Standard ab.
  - Die Datenqualität der Zugriffskontrollregeln ist daher von zentraler Bedeutung.
- **Ziele:**
  - Erarbeitung und Aufbereitung des XACML-Standards
  - Erarbeitung von Datenqualitätsdimensionen und -Metriken für attributbasierte Zugriffskontrollregeln
  - Vorstellung der Datenqualitätsmetriken und Erklärung anhand beispielhafter XACML-Policies
- **Voraussetzungen:** *keine*
- **Mögliche Bearbeiter:** 2 Personen
- **Betreuer:**
  - Sascha Kern (sascha.kern@wiwi.uni-regensburg.de)
  - Alexander Puchta (alexander.puchta@wiwi.uni-regensburg.de)

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Klassifizierungsmöglichkeiten und Einordnung von Zugriffsmodellen im Identitätsmanagement

- **Beschreibung:**
  - Zugriffsmodelle definieren den Zugriff auf Ressourcen und Berechtigungen
    - » Bekannte Vertreter sind RBAC und ABAC
  - In der Literatur gibt es eine beachtliche Menge an weiteren Zugriffsmodellen
- **Ziele:**
  - Relevante Zugriffsmodelle in der Literatur identifizieren
  - Ein Schema zur Klassifizierung von Zugriffsmodellen entwickeln
  - Identifizierte Zugriffsmodelle in entwickeltes Schema einordnen
- **Voraussetzungen:** *keine*
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:**
  - Sebastian Groll(sebastian.groll@nexis-secure.com)



Analyse von Methoden und Konzepten der IT-Sicherheit im Personal Internet of Things (PIoT)

- **Beschreibung:**
  - Durch den steigenden Einsatz des Internet of Things (IoT) und von IoT-Geräten in Haushalten und in der unmittelbaren Umgebung einer Person werden persönliche IoT (PIoT)-Netzwerke geschaffen (z. B. Smart Home, Smart Devices).
  - Welche Sicherheitskonzepte im Bereich des PIoT bestehen, soll die Durchführung einer systematischen und strukturierten Literaturrecherche mit einer Klassifizierung der Ergebnisse hinsichtlich der Forschungsfrage erläutern.
- **Ziele:**
  - Identifizierung und Kategorisierung von Möglichkeiten (Methoden und Konzepte) die IT-Sicherheit im PIoT zu gewährleisten.
  - Darstellung des aktuellen State-of-the-Art und mögliche Ableitung von Forschungslücken im Bereich der PIoT-Sicherheit.
- **Voraussetzungen:** *keine*
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:**
  - Sabrina Friedl (sabrina.friedl@ur.de)

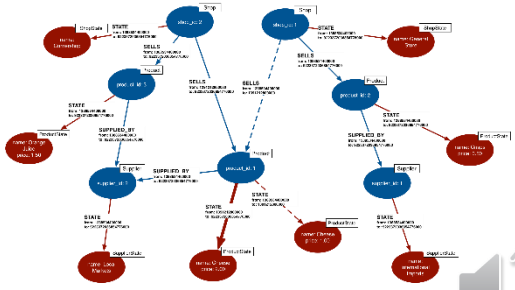
Strukturierte Analyse zur Anwendung von Digital Forensics (DF) im Consumer Internet of Things (CIoT)

- **Beschreibung:**
  - Das IoT findet eine immer breitere Anwendung, was sich bei Verbrauchern widerspiegelt. Grundsätzlich bezieht sich das CIoT auf Anwendungen und Geräte für Verbraucher (z. B. Smart Home, Smart Devices).
  - Durch die Entwicklung des IoT über die letzten Jahre häufen sich Sicherheitsvorfälle. In DF sollen mithilfe von Ermittlungs- und Analysetechniken Beweise auf IT-Systemen so erfasst und gesichert werden, dass sie vor Gericht verwendbar sind.
- **Ziele:**
  - Identifizierung und Kategorisierung von Methoden und Konzepte die im Bereich des PIoT im Zusammenhang mit Digital Forensics (DF) angewandt werden.
  - Durchführung einer systematischen und strukturierten Literaturrecherche mit einer Klassifizierung der Ergebnisse hinsichtlich der Forschungsfrage.
- **Voraussetzungen:** *keine*
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:**
  - Sabrina Friedl (sabrina.friedl@ur.de)

Zeitbasierte Graphen: Aktueller Stand der Forschung und Technik

- **Beschreibung:**
  - Netzwerk-Daten sind ein wesentlicher Bestandteil jeder Sicherheitsanalyse
  - Diese Daten bilden einen Graphen, allerdings lassen sich Zeitpunkt oder die Dauer einer Kommunikation nur schwer in einem Graph abbilden
  - Zeit-basierte Graphen bieten einen Lösungsansatz
- **Ziele:**
  - Strukturierte und umfassende Literaturanalyse zur Darstellung des Forschungsstandes hinsichtlich zeit-basierter Graphen
  - Ableitung aktueller Herausforderungen und verfügbarer Technologien

- **Voraussetzungen:** *keine*
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:**
  - Philip Empl (philip.empl@ur.de)
  - Fabian Böhm (fabian.boehm@ur.de)



Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Cyber Threat Intelligence (CTI) und Incident Response

- **Beschreibung:**
  Bedrohungsinformationen (CTI) sollen in Unternehmen der IT-Sicherheit dienen. Dies hat Relevanz insbesondere für das Bewältigen von Sicherheitsvorfällen (Incident Response).
- **Ziele:**
  - Umfassende und strukturierte Literaturrecherche zu CTI und Incident Response
  - Erfassung und Systematisierung der relevanten Forschungsergebnisse
- **Voraussetzungen:**
  - Interesse an IT-Sicherheit
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:** Daniel Schlette (daniel.schlette@ur.de)

Experteninterviews zu Erfolgsfaktoren von DLT Konsortien

- **Beschreibung:**
  Ein DLT Konsortium ist ein Verbund von Unternehmen, der über Distributed Ledger Technologie (z.B. Blockchain) Daten teilt.
- **Ziele:**
  - Ermittlung der Erfolgsfaktoren von DLT Konsortien über einen Fragebogen
  - Entwurf eines Experteninterview-Fragebogens
  - Test des Fragebogens mit verschiedenen Experten
- **Voraussetzungen:**
  - Verständnis von DLT
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:** Benedikt Putz (benedikt.putz@ur.de)

Wie können digitale Zwillinge im Sicherheitskontext erstellt werden?

- **Beschreibung:**
  - Digitale Zwillinge sind virtuelle Abbilder von physischen Objekten und deren Interaktion, z.B. Synchronisation
  - Im Sicherheitskontext können diese dazu verwendet werden, um bspw. Sicherheitsanalysen zu einem bestimmten Asset durchzuführen
- **Ziele:**
  - Durchführung einer systematischen Literaturrecherche
  - Identifikation und Klassifikation der Möglichkeiten, wie digitale Zwillinge erzeugt werden können
- **Voraussetzungen:** IT-Security I
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:**
  - Philip Empl (philip.empl@ur.de)

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

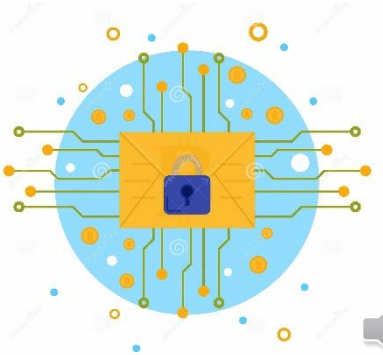
Security Orchestration für das Internet of Things: Architekturvergleich

- **Beschreibung:**
  - Starke Orientierung von vorhanden Mechanismen und Technologien an klassischer IT-Architektur
  - Klassische Orchestrierung unter Umständen nicht umsetzbar im Internet of Things (IoT)
- **Ziele:**
  - Definition relevanter Anforderungen an IoT-Architektur
  - Vergleich von zwei Architekturen für die Orchestrierung im IoT
    - » Ohne Middleware
    - » Digitaler Zwilling als Middleware
- **Voraussetzungen:** IT-Security I
- **Mögliche Bearbeiter:** 2 Person
- **Betreuer:**
  - Daniel Schlette (daniel.schlette@ur.de)
  - Philip Empl (philip.empl@ur.de)

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

IoT Security Metrics

- **Beschreibung:**
  - Internet of Things (IoT) stellt eine komplexe Umgebung dar (Hersteller, Protokolle, Daten, usw.)
  - IoT oftmals als Einfallstor in Unternehmen, daher Bestimmung der Sicherheit einzelner Geräte
- **Ziele:**
  - Durchführung einer systematischen Literaturrecherche
  - Identifikation von relevanten Metriken und einbezogenen Daten
- **Voraussetzungen:** IT-Security I
- **Mögliche Bearbeiter:** 2 Person
- **Betreuer:**
  - Daniel Schlette (daniel.schlette@ur.de)
  - Philip Empl (philip.empl@ur.de)



Masterarbeiten

WS 2021/22

Prof. Dr. Günther Pernul
Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
FAKULTÄT FÜR WIRTSCHAFTSWISSENSCHAFTEN

Universität Regensburg

Blockchain Governance Patterns

- **Beschreibung:**
  Selbstverwaltung (Governance) von Blockchain Netzwerken erfolgt sowohl on-chain als auch off-chain über vertragliche Regelungen.
- **Ziele:**
  - Empirische Analyse bestehender Ansätze von Blockchain Konsortien
  - Empirische Analyse von Ansätzen in DeFi/DAO Projekten
  - Ableitung einer Liste von Patterns der Blockchain Governance
- **Voraussetzungen:**
  - Verständnis der Funktionsweise von DLT/Blockchain
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:**
  - Benedikt Putz (benedikt.putz@ur.de)

Blockchain Governance Anforderungsanalyse und Abgleich mit dem Status Quo

- **Beschreibung:**
  Selbstverwaltung (Governance) von Blockchain Netzwerken erfolgt sowohl on-chain als auch off-chain über vertragliche Regelungen.
- **Ziele:**
  - Erhebung der Anforderungen an die Governance eines Blockchain Netzwerks mit mehreren Unternehmen
  - Analyse der aktuellen Umsetzung der Anforderung
  - Abgleich mit den technischen Möglichkeiten verschiedener Frameworks/Tools (Fabric, Ethereum, Corda)
- **Voraussetzungen:**
  - Technisches Verständnis der Funktionsweise von DLT/Blockchain
- **Mögliche Bearbeiter:** 1 Person
- **Betreuer:**
  - Benedikt Putz (benedikt.putz@ur.de)