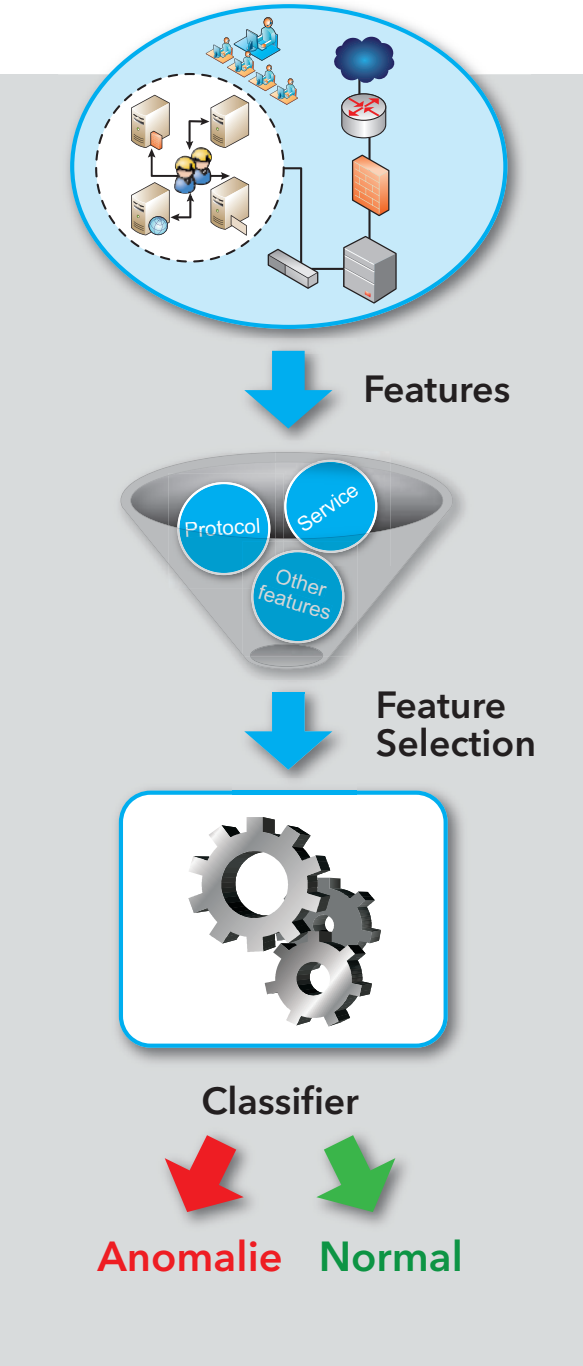
# SecMonet

## Entwicklung eines Sicherheitsanalysetools zur automatisierten Netzwerküberwachung




### Überblick

Zum Schutz vor unberechtigten Eindringversuchen in Rechnernetze werden Intrusion Detection Systeme (IDS) eingesetzt. Das Forschungsprojekt verfolgt einen neuartigen anomalie-basierten Ansatz, um auch bisher unbekannte Angriffe (sog. Zero-Day Attacks) frühzeitig erkennen zu können. Die adaptive Bestimmung des Normalprofils des Netzes und der davon ungewöhnlichen Abweichungen stehen im Fokus der Aktivitäten. Dabei werden verschiedene Ansätze und Techniken des Maschinellen Lernens in den vier Bearbeitungsphasen des IDS (Data Collection, Preprocessing, Classification, Prevention) entwickelt. Ziel des Projektes ist die Erstellung der Echtzeit-Plattform SecMONET, die den Datenverkehr in Rechnernetzen effektiv mit hoher Erkennungsrate als *normal* oder *anormal* klassifiziert.

**Hochschule Fulda**
*University of Applied Sciences*

**Prof. Dr. Ulrich Bühler**
u.buehler@informatik.hs-fulda.de
T 0661 9640-325

**M.Sc. Maher Salem**
maher.salem@informatik.hs-fulda.de
T 0661 9640-225

**B.Sc. Sven Reißmann**
sven.reissmann@informatik.hs-fulda.de
T 0661 9640-225

Hochschule Fulda
Fachbereich Angewandte Informatik
Network & Data Security
Marquardstraße 35
36039 Fulda

**www.hs-fulda.de/NDSec**

FORSCHUNG FÜR DIE PRAXIS
DIE HESSISCHEN HOCHSCHULEN FÜR ANGEWANDTE WISSENSCHAFTEN


## Hintergrund

Die Vielfalt der Cyber-Attacken reicht von dem unbemerkten Einbringen scheinbar harmloser Zusatzsoftware (Adware) über die heimliche Installation von Spyware (Wirtschaftsspionage, Geheimdienste, Terroristen) bis hin zur vollständigen Fernsteuerung des Opferrechners als Bestandteil eines Botnetzes.

Schutz vor derartigen Angriffen bieten Intrusion Detection Systeme (IDS). Solche Systeme sammeln und analysieren Informationen (Features) von Netzwerkkomponenten, um ungewöhnliches Verhalten und Sicherheitsverletzungen festzustellen. Die (klassischen) signatur-basierten Ansätze können bisher unbekannte Angriffsszenarien nicht erkennen, da die benötigten Angriffsmuster nicht zur Verfügung stehen. Dagegen identifizieren anomaliebasierte IDS alle Aktivitäten, die von einem definierten Normalverhalten des Rechners bzw. Netzwerks abweichen. Ihr Vorteil besteht also in der Erkennung bisher unbekannter Angriffe.

## Vorgehensweise

Die benötigten Verkehrsdaten können aus den einzelnen Komponenten des Netzes gesammelt werden. Die Features beschreiben das Profil des Rechnernetzes. Da die Struktur der Daten sehr unterschiedlich ist, müssen sie in ein einheitliches Datenmodell transferiert werden (Datennormalisierung).

Eine gute Performance des IDS wird erreicht, indem Features mit unwesentlichen Informationen ausgesondert werden. Vielversprechende Ergebnisse liefert eine Kombination aus Sequential Backward Search und Information Gain. Auf der Menge der so erhaltenen signifikanten Features wird ein Normalzustand des Netzes definiert. Ein Klassifizierer (Classifier) erkennt mögliche Abweichungen des aktuellen Netzprofils vom Normalzustand und identifiziert einen Eindringversuch.

Die Auswahl eines geeigneten Klassifizierers wie Self-Organizing Map (SOM), Support Vector Machine (SVM) in Verbindung mit Ensemble Methoden und paralleler Verarbeitung wird wesentlichen Einfluss auf die Performance und die Erkennungsrate haben. Auf anormales Verhalten reagiert das System mit geeigneten Schutzmaßnahmen.

## Ausblick

Als Weiterentwicklung von SecMONET soll ein adaptives anomalie-basiertes IDS entwickelt werden, das selbstlernend bisher unbekannte Angriffe effektiv klassifiziert, den Normalzustand eines Netzes kontinuierlich an die sich verändernden Bedingungen anpasst und somit Abweichungen vom Normalzustand mit minimaler False Positiv Rate identifiziert.

## Projektpartner

Das Projekt wird in enger Zusammenarbeit mit dem Partnerunternehmen Nethinks GmbH durchgeführt. Beteiligt sind weiterhin JUMO GmbH & Co. KG, IT-Security@Work GmbH und Wissenschaftler der Hochschule Fulda und der Universität Kassel.

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

## SECMONET

SecMonet is a research project in Network and Data Security group at the University of Applied Sciences Fulda. The target of this project is to develop a real time anomaly-based Network Intrusion Detection System that has the ability to early detect unknown attacks (Zero-Day Attacks). This project tends to reduce data dimensionality of the intended network, improve the performance of the network by enhancing the detection rate and suppressing the false positive rate. Our research includes Data Aggregation, Feature Selection, Classification and Prevention. This project is funded by the German Federal Ministry of Education and Research (BMBF).