

INSTITUT FÜR NETZWERKE UND SICHERHEIT



Univ.-Prof. DI Dr. René Mayrhofer
Informatik Bachelorinfoabend

ÜBER UNS

- Wir streben danach, die Sicherheit und Netzwerkkonnektivität von Computersystemen sowohl in weltweiten als auch in lokalen Netzwerken durch Forschung, Bildung und spezifische Projektarbeit zu verbessern.
- Neben der akademischen Forschung und Lehre glauben wir fest daran, dass es unsere gemeinsame Verantwortung ist, die praktische Sicherheit von alltäglichen Computersystemen und Infrastrukturen zu verbessern, von denen unsere gegenwärtige Gesellschaft zunehmend abhängig ist.

LEITBILD

- Computernetzwerke und Sicherheit sind schnell bewegende Ziele. **Forschung und Lehre am Institut für Netzwerke und Sicherheit umfasst daher das gesamte Spektrum von theoretischen bis zu sehr praktischen Fragestellungen.**
- Aktuelle Forschungsschwerpunkte zur Verbesserung des aktuellen Standes der Technik sind:
 - Digital Identities
 - Secure Code
 - Long Range Communication

PFLICHTLEHRVERANSTALTUNGEN IM BACHELOR

- Operating Systems (VO) - SS
- Operating Systems (PR) - SS
- Computer Networks (VO) - WS
- Computer Networks (UE) - WS
- Rechtsgrundlagen der Informatik (VO) - WS
- Projektpraktikum (PR) - WS

THEMEN FÜR BACHELORARBEITEN

■ Post-Quantum-Cryptography – Signierung auf Cloud-Server

- Implementierung einer Post-Quantum Signatur auf einem Cloud-System mit Remote Attestation. Zuerst wird verifiziert (Attestation) dass der erwartete Code in einem „akzeptablen“ System läuft. Anschließend werden der private Schlüssel und die zu signierenden Dateien („Streaming“ – uU sehr viele Daten) übermittelt. Am Ende wird eine Quanten-sichere Signatur erstellt und zurückgeliefert. Die Daten werden lokal (= in der Cloud) gelöscht. Implementierung des Systems als Demonstrator.

THEMEN FÜR BACHELORARBEITEN

■ Integration und Erweiterung eines Demo-Systems für (unsichere) Web-Applikationen

- Ein existierendes virtuelles System mit mehreren Web-Applikationen, die unsicher sind, soll in eine einzige größere Applikation zusammengefasst werden. Auch zusätzliche Beispiele von Angriffen sind einzubauen. Das System basiert auf JavaScript+Node.js (beizubehalten). Auswahl der zu implementierenden Angriffe (sowie der abgesicherten korrekten Version) nach Interessen der Person bzw nach Absprache.

THEMEN FÜR BACHELORARBEITEN

■ Ableiten weiterer Schlüssel aus existierendem Tor Hidden Service Schlüssel

- Das wird schon beim Directory benützt. Entwurf eines Systems, dass in (abhängig von einem geheimen Startwert) in "zufälligen" Abständen neue Schlüssel generiert. Wenn man dieser Geheimen Wert kennt, kann man auch aus (nur!) dem öffentlichen Schlüssel die zugehörigen abgeleiteten öffentlichen Schlüssel berechnen. Dies würde ein "Hopping" bei Hidden Services erlauben. Implementieren, testen, überlegen wofür das verwendet werden kann, Vor- & Nachteile.

THEMEN FÜR BACHELORARBEITEN

■ Sicherheitsprüfung der Remote-Control Software “Rustdesk”

- Diese Software dient dem Remote-Zugriff auf andere Computersysteme, ähnlich zu Teamviewer oder AnyDesk. Der Client und ein einfacher Server sind jedoch als Open Source verfügbar. Es soll eine systematische Sicherheitsuntersuchung erfolgen, insbesondere unter der Annahme, dass der Server nicht vertrauenswürdig ist. Es kann entweder ein Server des Herstellers oder ein eigener verwendet werden: Wie sieht es hier mit der Sicherheit der Verbindungen/Systeme aus, wenn dieser Server nicht vertrauenswürdig ist? Beinhaltet Protokoll- und Quellcodeanalyse.

THEMEN FÜR BACHELORARBEITEN

■ Comparison of the Benchmarking Libraries of Rust

- Various benchmarking libraries exist in Rust for measuring implementation performance. However, many of them suffer from drawbacks, such as requiring copy-pasted code, having poor usability, or being limited to benchmarking public elements. This project investigates several benchmarking libraries, comparing their limitations and differences, with a particular focus on ease of use. It also explores how these libraries can be applied in a sequential workflow and how private items can be benchmarked using workarounds when necessary. The outcome of this project is a document presenting the findings along with code examples.

THEMEN FÜR BACHELORARBEITEN

- **Scanning der Onion Adressen, die wir aktuell sammeln + Extrahieren unterschiedlicher Marker.**
 - (Teilweise) Reproduktion und Auswertung der Arbeit von <https://onionscan.org/> für V3 onion services, wie/ob sich das Darknet seit damals verändert hat.

THEMEN FÜR BACHELORARBEITEN

■ Win11 Memory forensics with Volatility

- Create an example for Windows memory forensics: Some chat application should be running and the computer is available (with Admin permissions), resp locked (without password). Test various methods to obtain a memory dump¹. The resulting dump should then be analyzed with the SW Volatility (and manually/with tools to develop) to obtain as much information about the chat application as possible, especially any currently displayed messages, the user ID etc.

¹ see <https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/how-to-force-a-diagnostic-memory-dump-when-a-computer-hangs/257809>

THEMEN FÜR BACHELORARBEITEN

■ Reconstructing internet video from a network trace

- This should work for IP video telephony, but potentially also for other communications. The main task here is to handle missing parts, e.g. keeping the old picture or replacing it with "white/black screen". The sniffed traffic should then be playable and be accompanied by exact specifications what was found, and what/when there were "holes" filled.

THEMEN FÜR BACHELORARBEITEN

■ Multiplattform-App-Entwicklung mit nativem Rust-Kern: Ein Framework-Vergleich

- In diesem Projekt wird eine Multiplattform-App mit verschiedenen Frameworks – darunter Kotlin Multiplatform, React Native und Flutter – umgesetzt. Im Zentrum steht ein nativ kompilierter Kern in Rust, der von den jeweiligen Plattform-Implementierungen genutzt wird. Ziel ist es, die Integration eines gemeinsamen nativen Kerns in unterschiedliche App-Frameworks zu erproben und die jeweiligen Möglichkeiten, Stärken und Herausforderungen systematisch zu evaluieren.

THEMEN FÜR BACHELORARBEITEN

- Weitere Themen auf unserer Website:





**JOHANNES KEPLER
UNIVERSITY LINZ**