Institut für Netzwerke und Sicherheit

https://www.jku.at/institut-fuer-netzwerke-und-sicherheit/
(oder kurz: https://jku.at/ins)

Univ.- Prof. René Mayrhofer

vor Ort: Maximilan Kokalj

Über uns

- Wir streben danach, die **Sicherheit und Netzwerk-konnektivität 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 Computer-systemen 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 & Supply Chain Security**
  - **Network Privacy**
  - **(Long Range) Communication**
  - **Android Security & Privacy**

Pflichtlehrveranstaltungen im Bachelor

- Betriebssysteme (VO+UE) - SS
- Computernetzwerke (VO+UE) - WS
- Rechtsgrundlagen der Informatik (VO) - WS
- Projektpraktikum (PR) - WS

Themen für Bachelorarbeiten

- **Übersicht der Themen auf unserer Webseite:**
  - Themen für Bachelorarbeiten | Institut für Netzwerke und Sicherheit (jku.at)

- **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

- **Implement an example website (as a normal and as a hidden service) with a database, which is always running on a Tor hidden service (somewhere else!)**:
  - SQL and NoSQL. Test whether this works or what is needed, how efficient and resilient it is (e.g. reconnections), and do performance tests. Do this for a “classic” webpage as well as a SPA (Single Page Application): the page must load the data via JavaScript (from a Tor service!). Classic page on normal server with hidden DB, Classic page on hidden server with hidden DB, SPA on normal server with hidden API/DB, SPA on hidden server with hidden API/DB.

- **Mobile driving license reference implementation**
  - The goal of this project is to implement the current standard for mobile driving licenses (ISO/IEC 18013-5) on Android.

Themen für Bachelorarbeiten

- **Ingest probable location data using a Large Language Model**
  - In the CDL Digidow (digidow.eu) ecosystem, users have complete control over their Personal Identity Agent (PIA), which can perform tasks, such as unlocking doors based on data gathered from sensors in the surrounding environment. One aspect of securing this system is that the PIA should be aware of their user's current activities, so it can judge if the person in front of the door might actually be an impostor.
  - Two potential digital sources of such information, to take into account are the user's email account and calendar.
  - The goal of this project is live-scanning this data, extracting relevant information like booked trains, flights, hotels, or other appointments, and outputting any identified events to the PIA's location model.
  - You should use techniques like prompt engineering and agent-based approaches (no training or long-running fine-tuning) with existing local LLMs.
    You should expect to write some regular code in a reasonable language of your choice to continuously ingest input and forward the LLMs outputs.
  - Your solution should maintain a list of detected future events, in an agreed-upon format, which the LLM can update and the location model can consume.

Themen für Bachelorarbeiten

- **Bei Tor können aus dem Schlüssel für Hidden Services weitere Schlüssel abgeleitet werden.**
  - Entwurf eines Systems, dass in (abhängig von einem geheimen Startwert) in "zufälligen" Abständen neue Schlüssel generiert. Wenn man diesen 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, teste, überlegen wofür das verwendet werden kann, Vor- &Nachteile

- **Implement a VoIP tap for Softphones (i.e. VoIP phones implemented as software running on a PS)**
  - This should copy the network traffic and/or the sound output. This should then be run through libraries and speaker detection. This should then show feedback about who is talking how much (e.g. percent) and the mood of the speakers.

Themen für Bachelorarbeiten

- **Sensor node communication via ephemeral Tor Onion services**
  - The goal of this project is to create a library for simple machine-to-machine communication via short-lived hidden Onion services.

- **Security analysis of the Linux kernel in Mikrotik RouterOS**
  - Mikrotik RouterOS is a Linux kernel based embedded operating system for network routers, switches, access points, etc. While the userspace components are closed source, patches and configuration options for the used Linux kernel are available. The goal of this project is to analyze which security vulnerabilities - especially remotely exploitable ones - are publicly known for the user kernel version and if/how they have been patched. Necessary skills for this project include reading/writing C, reading and applying patches to source code, and compiling and testing native C code.

Themen für Bachelorarbeiten

- **Comparison of DNS results for TOR exit node DNS queries against different providers**
  - As seen by a recent incident at our TOR exit node, where the ISP DNS servers manipulated the outcome of certain DNS queries through a DNS filtering system, interception at the level of DNS results is a popular (though questionable) means to block unwanted web traffic.
  - In this bachelor's thesis, the outcome of presenting DNS queries performed by our TOR exit node to multiple different providers should be analyzed. Moreover, cases where deviating responses are observed should be further investigated. Interesting deviations would be primarily those caused by filtering/censorship.

- **Anything to do with energy savings in networks and/or security ;)**

- **Android device security & privacy – come talk to us!**