2019 i-Seminar Themen -> 4 Gruppen/Studenten notwendig

- **WPA3 (Next Generation of Wireless Security)**
  - Mehr als 10 Jahre nach der Standardisierung von WPA2 wurde auf Mitte 2018 das WPA3-Protokoll von der Wi-Fi Alliance verabschiedet und soll nun 2019 laufend auf neueren Access Points und Clients eingeführt werden. Die WiFi-Alliance verspricht: “WPA3 enhances user experience while maintaining secure connections”.
  - Ist WPA3 für den Endbenutzer wirklich viel sicherer als WPA2?
  - Dazu sind in dieser I-Seminararbeit folgende Punkte zu untersuchen:
    - Was waren die Verwundbarkeiten und Schwachstellen in WP2 (SOHO, Open Networks, …)?
    - Was sind die hauptsächlichen Neuerungen und Verbesserungen in WPA3?
    - Welche Empfehlungen bezüglich Sicherheit können sie zu WPA2 und WPA3 ihren Kollegen geben?
    - Welche Verbesserungen zu IoT wurden in WPA3 adressiert?
    - Welche Zertifizierungsrichtlinien wurden bisher für WPA3-konforme Geräte von der WIFi-Alliance erlassen?
- **How can AI and ML help to improve security?**
  - First of all: ML should always help and assist human to do tasks more efficiently. ML is not intend (nor designed) to supersede, replace or even disrupt humans work!
  - What is **Artificial Intelligence for IT Operations (AIOps)**: These are ML tools which can help resolve an ongoing dilemma faced by many organizations today. On one hand we spend millions of money each year to strengthen information security and to look for better answers (e.g to experience major breaches, improve the stability of our system, etc.) and on the other hand we do not have the resources to analyse produced data in a short time frame.
  - That’s where ML is coming in. ML tools are used in order to make sense of data and keep engineers informed about both patterns and problems so they can address them promptly or even just in time. The objective of AIOps is to enhance these processes by consolidating, automating, and updating them. As such AIOps may help to minimize data breach incidents especially in case of identity authentication and authorization which are still primary points of attack.
  - The task for this topic will be to analyse, document and explain based on specific examples (if available) the role of ML, helping professionals to better do their daily work.
- **Additional Signature Schemes**
  - Beside the ‘classic’ digital signature schemes using RSA and DSA where correctness (a verifier can check the correctness of a message) and unforgeability (a forgery is not being able to create a valid signature of another message) are requested, additional schemes has been developped in the past to support diverse application scenarios (e.g. Proxy Signatures, Attribute-based Signatures, Blank Signatures, Group Signatures, Blind Signatures, Redactable Signatures, …). The task for this topic will be to examine, document and explain (with an example) the purpose and the process of some selected (most occurring) special signature schemes.
- **IIOT (Industrie 4.0 und Kryptographie)**
  - Die Digitalisierung in der Industrie (Industrie 4.0, IIoT) bringt ein Anzahl Neuerungen mit sich. Die Vernetzung der physischen Geräte und Systeme im Internet nimmt rasant zu und man geht davon aus, dass die Gesamtzahl der angeschlossenen Sensoren und Devices bis in ein paar Jahren auf mehr als 50 Milliarden ansteigen wird. Dies wirft unweigerlich Fragen auf zur Privatsphäre, zur Authentizität bzw. Integrität der Daten und zur vertraulichen Übermittlung.
  - In verschiedenen Bereichen von IIOT werden sensible Daten übermittelt und somit ist das Thema der kryptographischen Absicherung und des Datenschutzes allgegenwärtig und ernst zunehmen. Nebst der Automobilindustrie befasst sich auch der Verein öffentlicher Verkehr (VöV) in der Schweiz mit diesem Thema. Die Vernetzung von Devices und Systemen im IoT-Bereich setzt eine sichere und zuverlässige Authentifizierung und Autorisierung voraus. Je nach Anwendungsfall ist zusätzlich die Integrität, die Verschlüsselung von Daten, sowie die Nichtabstreitbarkeit zwingend erforderlich.
  - Klassische PKI Modelle (wie z.B. eine Unternehmens-PKI für User- und Client-Zertifikate) sind eher langsam und können einem grossen Mengengerüst bzw. den neu gestellten Anforderungen voraussichtlich nicht mehr gerecht werden. Bestehende Architekturen müssen folglich überdenkt werden. Künftig müssen PKI-Umgebungen je nach Anwendungsfall mehrere tausend Zertifikate pro Sekunde erstellen, verteilen und validieren können. Schafft man dies mit klassischen PKI-Infrastrukturen? Des Weiteren müssen PKIs moderne Schnittstellen anbieten, damit Prozesse rund um Zertifikate möglichst schnell und automatisch abgewickelt werden können.
  - In dieser I-Seminararbeit sollen die Probleme rund um IIOT und Sicherheit beleuchtet werden und

mögliche Alternativen zu klassischen PKI Modellen und Strategien aufgezeigt werden, welche je nach Anforderung performanter sein müssen.