IIOT (Integrität im Internet der Dinge)
Basierend auf dem Artikel Vertrauen und Integrität im Internet der Dinge sollen in dieser I-Seminararbeit der heutige Aufbau von IIOT Devices beleuchtet werden.
https://www.swisscom.ch/content/dam/swisscom/de/about/verantwortung/digitale-schweiz/sicherheit/documents/vertrauen-und-integritaet-im-internet-der-dinge.pdf.res/vertrauen-und-integritaet-im-internet-der-dinge.pdf

Der Fokus liegt auf der Integrität der Dinge.
- Was sind die Herausforderungen für die Anbieter von IIOT Devices?
- Welche Fortschritte wurden seither erzielt?
- Welche Möglichkeiten stehen heute zur Verfügung um IIOT Devices sicher aufzubauen?

Data in Motion (Memory Encryption)
Die grosse Herausforderung bei Cloud- Services besteht darin, dass die Hardware Komponenten teilweise nicht mehr unter der Kontrolle der Service Anbieter sind. (bspw. AWS). In den letzten Jahren haben Intel und AMD die Sicherheitsfunktionen in ihren Prozessoren erweitert, so dass der Speicher verschlüsselt werden kann. Folgende Technologien kommen zum Einsatz:
- TME (Total Memory Encryption)
- SME (Secure Memory Encryption)
- TSME (Transparent SME)
- SEV (Secure Encrypted Virtualization).

Ziele der I-Seminararbeit sind:
- Beurteilung der verschiedenen in Memory Encryption Technologien (Intel, AMD, ARM)
- Aufzeigen von Einsatzmöglichkeiten inkl. Schlüsselkonzept für die Verwaltung der Schlüssel
- Kombinierter Einsatz mit TPM 2.0 (Trusted Plattform Module)
- Herausforderungen der Technologie im täglichen Einsatz

Supply Chain Security
In der vierten industriellen Revolution setzen Unternehmen eine Reihe verschiedener und sich schnell ändernder Technologien ein, um ihren Privat- und Geschäftskunden innovative Lösungen anzubieten. Dabei setzen sie bei Hard- und Software auf eine komplexe Lieferantenkette.
Durch jüngste Enthüllungen wurde die Öffentlichkeit auf die Unversehrtheit solcher Geräte aufmerksam gemacht, denn es wurde gezeigt, dass Hardware- und Softwarekomponenten mit oder ohne Zustimmung oder Wissen des Lieferanten oder Anbieters beeinträchtigt werden können.

Schwerpunkte der I-Seminararbeit:
- Welche verschiedenen Risikofaktoren in der Industrie 4.0 sind zu berücksichtigen?
- Was bedeutet dies für die Sicherheit und Integrität der Lieferkette?
- In welcher Weise betrifft dies die kritische Infrastruktur unseres Landes?
- Welche Optionen stehen Dienstleister wie Banken, Telekommunikationsunternehmen, Energieerzeuger zur Verfügung, um den aufkommenden Risiken einer vollständig vernetzten Welt zu begegnen?

Multifaktor Authentifizierung für Computer
Benutzername und Passwort sind immernoch die meistverwendete Methode um Computer zu entsperren (login). Auf Laptops stehen Fingerprint- oder Smartcard- Reader zur Verfügung um den Login Prozess zu unterstützen oder zu vereinfachen. Der Nachteil dieser Methoden ist die spezifische Hardware, welche nicht auf allen Geräten zur Verfügung steht.
Schwerpunkte der I-Seminararbeit:
- Abklärung der Möglichkeiten einer Ein- oder Zwei-Faktor-Authentifizierung (2FA) mit einem Smartphone
- Automatisches Login durch die Proximität des Mobiltelefons (NFC oder Bluetooth)
- Benutzung eines Softwarezertifikats mit Pin auf dem Mobiltelefon (2FA)
- Ablösung etablierter Mechanismen wie etwa Smartcard, SMS, MobileID, Google Authenticator, RSA Token für die 2FA
- Einsatzmöglichkeiten dieser Kombination aufzeigen (Weblogin, Remote Terminal Session, etc.)