TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur für Datenschutz und Datensicherheit

AUFGABENSTELLUNG FÜR DIE BACHELORARBEIT

Name, Vorname des Studenten: Garten, Gregor

Immatrikulationsnummer: 4055357

Studiengang: Informatik (2009)

Thema (deutsch): **Low-Latency-Kryptographie für transparente Layer-2 Verschlüsselung mit MACsec**

Thema (englisch): **Low-Latency Cryptographic Algorithms for MACsec providing transparent Layer-2 encryption**

Zielstellung:

MACsec (IEEE 802.1AE) ist ein Protokoll, daß eine Integritätsprüfung sowie Verschlüsselung des Datenverkehrs auf Schicht 2 ermöglicht. Dabei werden die zu übertragenden Ethernet-Pakete mittels MAC geschützt und gegebenenfalls verschlüsselt. Aktuell ist in MACsec jedoch nur ein Kryptoverfahren (AES-GCM) spezifiziert, welches dazu nur mit einer Schlüssellänge (128 bit) implementiert ist. Das Kryptoverfahren stellt die wesentliche und rechenaufwändigste (Gruppe von) Operation(en) dar und charakterisiert damit das gesamte Verfahren bezüglich seiner Effizienz und Anwendbarkeit auf verschiedene Anwendungsgebiete. Ziel ist es daher, die vorhandene Implementation von MACsec (Linux-Kernelmodul plus entsprechende Systemwerkzeuge) so zu erweitern, daß es möglich wird, weitere Kryptoverfahren in MACsec verwenden zu können. Dazu soll zuerst eine Auswahl verschiedener in Frage kommender Verfahren getroffen werden. Dies soll in Abhängigkeit des Anwendungsfalles (Kommunikation im industriellen Umfeld) und bereits vorhandener Implementationen geschehen. Zwei Abschlussarbeiten am Lehrstuhl beschäftigten sich bereits mit unterschiedlichen Low-Latency-Kryptoverfahren und deren Effizienz. Die Ergebnisse dieser Arbeiten sollen herangezogen werden. Nachdem MACsec mit den identifizierten Verfahren erweitert wurde, muss gezeigt werden, daß es immer noch aus funktionaler Sicht genau das leistet, was es soll. Ferner ist zu belegen, daß die Sicherheit nur gemäß des veränderten Kryptoverfahrens verändert wird. Darüber hinaus sollen die neuen Verfahren mit AES-GCM und gegeneinander bezüglich bestimmter Performanceparameter wie Latenz und Bandbreite verglichen werden. Dazu ist eine entsprechende Messinfrastruktur aufzusetzen. Für eine erfolgreiche Bearbeitung sind folgende Teilaufgaben zu erfüllen:

- Festlegung der zu verwendenden Kryptoverfahren
- Erweiterung der MACsec-Implementation sowie benötigter Systemwerkzeuge um die ausgewählten Kryptoverfahren
- Aufbau einer Messinfrastruktur für die Evaluation
- Bewertung der verwendeten Verfahren nach Funktionalität, Sicherheit und bestimmter Performanceparameter, wie Latenz und Bandbreite

Betreuer: Dr.-Ing. Stefan Köpsell

Verantwortlicher Hochschullehrer: Prof. Thorsten Strufe

Institut: Systemarchitektur

Beginn am: 4. Juni 2018 Einzureichen am: 20. August 2018

4.06.2018 .....

Datum, Unterschrift der/des Studierenden

.....

Unterschrift des betreuenden Hochschullehrers

Verteiler: Prüfungsamt (Original); Student (Original – Deckblatt der Bachelorarbeit); HSL + Sekr. (Kopie); elektr. Datei → Sekretariat