TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur für Datenschutz und Datensicherheit

AUFGABENSTELLUNG FÜR DIE BACHELORARBEIT

Name, Vorname des Studenten: *Jan Sönke Huster*

Immatrikulationsnummer: *4084528*

Studiengang: *Bachelor Informatik (2012)*

Thema (deutsch): **Verbesserungen bezüglich transparenter Layer-2 Verschlüsselung mit MACsec**

Thema (englisch): **Enhancements for MACsec providing transparent Layer-2 encryption**

Zielstellung:

Mit MACsec (IEEE 802.1AE) steht ein Protokoll zur Verfügung, dass eine Integritätsprüfung sowie Verschlüsselung des Datenverkehrs auf Schicht 2 ermöglicht. Dabei werden die zu übertragenden Ethernet-Pakete mit einem MAC geschützt und gegebenenfalls verschlüsselt. Problematisch bei der aktuellen Spezifikation und Implementierung von MACsec ist, dass durch die MACsec-Header und dem angehangenen Message Authentication Code das zu übertragende Paket größer wird. Dabei kann es passieren, dass die MTU überschritten wird und der Ethernet-Frame nicht übertragen werden kann.

In der Bachelorarbeit soll daher eine Lösung entwickelt und evaluiert werden, die eine transparente MACsec-Verschlüsselung erlaubt, d.h., es ist davon auszugehen, dass weder die auf der Leitung übertragbare Ethernet-Frame-Größe vergrößert werden kann, noch dass die Größe der gesichert zu übertragenen Ethernet-Frames verkleinert werden kann. Folglich ist eine Fragmentierung umzusetzen. Neben dem naiven Ansatz, aus jedem zu großen Ethernet-Frame zwei verschlüsselte MACsec Pakete zu erzeugen, sind auch effizientere Fragmentierungsverfahren zu untersuchen.

In einer Evaluation ist zu zeigen, dass die entwickelte Lösung das Erwartete aus funktionaler Sicht leistet, wobei gleichzeitig zu argumentieren ist, dass die Sicherheit des erweiterten MACsec-Protokolls nicht schlechter ist als die Sicherheit des originalen MACsec-Protokolls. Ferner ist zu untersuchen, welchen Einfluss die Fragmentierung auf Performanceparameter wie Verzögerungszeit und Bandbreite (übertragene Datenmenge) hat. Als Baseline ist eine nicht fragmentierte Übertragung mit Hilfe von Jumbo-Frames anzusetzen.

Für eine erfolgreiche Bearbeitung des Themas sind folgende Teilaufgaben zu erfüllen:

- Erweiterung des MACsec-Protokolls um transparente Fragmentierung von zu übertragenden Ethernet-Frames
- Implementierung dieses Protokolls im Linux-Kernel
- Evaluierung der entwickelten Lösung bezüglich Funktionalität, Sicherheit und Performance

Betreuer: Dr.-Ing. Stefan Köpsell

Verantwortlicher Hochschullehrer: Prof. Thorsten Strufe

Institut: Systemarchitektur

Beginn am: 08.01.2018 Einzureichen am: 26.03.2018

8.01.18 .....

Datum, Unterschrift der/des Studierenden

.....

Unterschrift des betreuenden Hochschullehrers

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