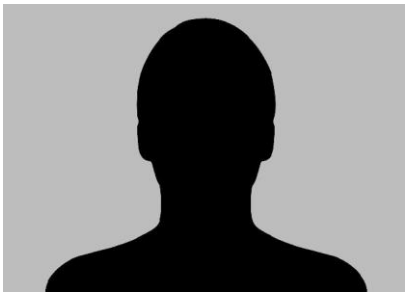
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

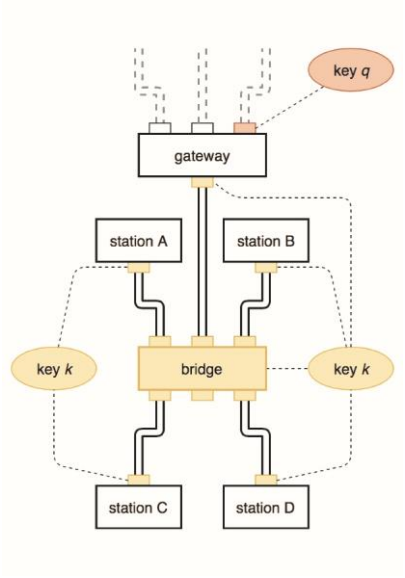
Preventing Supply Chain Insecurity by Authentication on Layer 2



Diplomierende
Dennis Camera
Raphael Ungricht

Dozent
Stephan Neuhaus

In Anbetracht der aktuellen Tendenzen der Datenspeicherung wird die Menge der in Rechenzentren gespeicherten Daten kontinuierlich zunehmen. Demzufolge werden datenverarbeitende Server in Zukunft ein immer interessanteres Angriffsziel werden.
Ein am 4. Oktober 2018 von Bloomberg veröffentlichter Artikel mit dem Titel 'The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Com-panies' zeigt ein neues Angriffsszenario auf Server auf.
Es sind kleine Chips, die auf die Leiterplatten der Geräte gelötet werden. Diese elektronischen Komponenten sind mittlerweile so stark geschrumpft, dass sie mit blossem Auge kaum noch erkennbar sind. Den-noch sind sie so weit fortgeschritten, dass sie komplexe Berechnungen durchführen können, ihren eigenen Speicher haben und mit anderen Komponenten oder Computern über das Netzwerk kommunizieren können.
In dieser Arbeit haben wir verschiedene Ansätze verfolgt, um die Auswirkungen solcher Angriffe, die durch Schwachstellen in der Lieferkette ermöglicht werden, zu minimieren.
Als Resultat unserer Forschung haben wir ein IEEE~802.3-kompatibles Authentifizierungsprotokoll auf dem MAC-Layer mit dem Namen 'L2Auth' entwickelt und als Machbarkeitsnachweis eine Implementierung für den Linux Kernel umgesetzt.
Sowohl das Design als auch die Implementierung garantieren, dass nicht autorisierter Netzwerkverkehr blockiert wird, bevor er das interne Netz-werk verlassen kann. Dadurch ist eine effektive Verhinderung von Daten-Exfiltration durch solche mikroskopischen Chips möglich.
Wir konnten mit unserer L2auth-Implementierung einen maximalen Durchsatz von 693 Mbit/s auf einem Apple MacBook Pro aus dem Jahre 2010 ohne Hardware-Beschleunigung messen. Dies ist eine Reduktion von 26 % im Vergleich zum maximal möglichen Durchsatz auf reinem Ethernet.



Die obige Abbildung zeigt ein L2auth-geschütztes Netzwerksegment mit vier Stationen, die an einer Bridge angeschlossen sind, sowie einem Gateway. Alle Geräte innerhalb einer Broadcast-Domäne benutzen denselben Schlüssel zur Authentifizierung der Datagramme.