Anwenderforum für Fernmeldetechnik, AFCEA Computer, Elektronik und Automatisierung

AFCEA Bonn e.V. Studienpreis 2017

Kernthesen der Arbeit

Titel der Arbeit:	Security Analysis of Autonomic Network on Cisco gear
Tag der Einreichung:	16.01.2017
Hochschule:	RWTH Aachen (BIT Kooperation; Uni Bonn)
Name des Verfassers:	Omar Eissa
Betreuender Professor:	Prof. Dr. Michael Meier

*Kurze Beschreibung (1 Seite !) der **Kernthesen**.*

Was ist die Quintessenz der Arbeit?

Die vorliegende Arbeit untersucht die Sicherheit von Funktionen des „Autonomic Networking“ (AN), welches von Cisco-Geräten implementiert wird. Die Idee von AN sind selbständige Netzwerk-Geräte, die eigenständig folgende Aufgabenbereiche übernehmen: Self-Configuration, Self-Optimization, Self-Healing, Self-Protection. Menschliche Betreuung zum Betrieb der Geräte und anderer Netzwerkkomponenten ist so mit weniger Aufwand verbunden, als bei aktuell üblicherweise eingesetzten Netzwerk-Geräten.

Im Vordergrund der Arbeit stehen dabei insbesondere die durch einen Angreifer über das Netzwerk ausnutzbaren Verwundbarkeiten der AN-Implementierung auf Cisco-Hardware. Da es sich nicht um offene Standards handelt ist für die Sicherheitsanalyse zunächst ein Reverse-Engineering der Kommunikation notwendig. Auf Basis dieser extrahierten Kommunikationsprotokolle sollen dann mögliche Verwundbarkeiten des Systems ermittelt werden.

Mögliche Angriff-Szenarien sind der unautorisierte Zugriff auf das mit AN konfigurierte Netzwerk oder die Beeinflussung der Komponenten bis hin zu einem Denial-of-Service.

Die Darstellung der Arbeit umfasst zunächst die notwendigen Schritte zur Analyse der komplett verschlüsselt ablaufenden Kommunikation der Geräte untereinander. Sie demonstriert die kreative Herangehensweise die notwendig ist, um diese Verschlüsselung so zu manipulieren, dass ein Zugriff auf die Klartextkommunikation möglich ist.

Darauf aufbauend werden verschiedene Teile des Protokolls auf Inkonsistenzen und mögliche Verwundbarkeiten überprüft. Das betrifft insbesondere die Interpretation von Datenfeldern in der Kommunikation, aber auch die Konsistenz und Resilienz der Zustandsautomaten bei verschiedenen Funktionsabläufen.

Die durchgeführten Angriffe zeigen die Möglichkeiten sowohl die Interpretation der Whitelist auf den Geräten zu beeinflussen als auch durch speziell eingebrachte Out-of-Order-Nachrichten verschiedener Protokollschritte einen Router zum Absturz zu bringen. Das ist selbst dann möglich, wenn das AN-Feature auf dem Gerät gar nicht aktiviert ist.

Die erkannten Sicherheitslücken wurden dem Hersteller gemeldet. Dies führte abschließend zu zwei CISCO Security Advisories mit dem Severity-Level „High“ unter den CISCO SA-IDs „cisco-sa-20170320-ani“ und „cisco-sa-20170320-aniipv6“.