Institute for Internet Technologies and Applications

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

# Bachelorarbeit 2014

# Endpoint Compliance Monitoring based on Software Identification Tags

**Studenten: Danilo Bargen, Christian Fässler, Jonas Furrer**

**Betreuer: Prof. Dr. Andreas Steffen**

**Ausgabe: Montag, 17. Februar 2014**

**Abgabe: Freitag, 13. Juni 2012**

## Einführung

Das amerikanische National Cybersecurity Center of Excellence [1] schlägt in einem Entwurfsdokument [2] vor, über eine kontinuierliche Ueberwachung der installierten Software auf Client-Systemen (Desktop PCs, Laptops, Tablets, Smartphones, etc.), die Gefahr von Cyberattacken zu minimieren. Das Software Asset Management soll über Software Identification (SWID) Tags erfolgen, die auf der 2014 Revision der ISO/IEC 19770-2 Norm basieren sollen.

Die Trusted Network Connect (TNC) Funktionalität der strongSwan Open Source VPN Software kann Windows, OS X, Android und Linux Clients nach SWID Tags durchsuchen und dieses Inventar an einen zentralen TNC Server übermitteln [3]. Neu soll ein SWID Generator Tool für Linux Clients erstellt werden, das SWID Tags für alle installierten Linux Pakete generieren kann, die durch einen Paket Manager verwaltet werden.

Die vorgeschlagene Arbeit soll weiter auf dem bestehenden strongTNC Policy Management Tool [4] aufbauen, das in der Skriptsprache Python geschrieben ist und das Django Web-Framework benutzt. Die von den Clients gelieferten SWID Tags sollen zusammen mit Metadaten, die aus den XML-codierten Tags extrahiert werden, in der TNC Datenbank abgespeichert und verwaltet werden. Über eine geeignete Benutzerführung soll visualisiert werden können, welche Version eines Software Paketes in welchem Zeitraum auf welchen Clients installiert war.

## Aufgabenstellung

- Einarbeiten in den ISO/IEC 19770-2:2014 SWID Tag Draft Standard.
- Erstellen eines SWID Generators in der Skriptsprache Python, der ISO/IEC 19770-2:2014 SWID Tags für einzelne oder alle Linux Pakete erzeugen kann, die durch den **dpkg** Paket Manager (Debian, Ubuntu, etc.) verwaltet werden.
- Es soll über eine Konfigurationsoption des SWID Generators möglich sein, die Pfadnamen aller Dateien, die durch ein Linux Paket installiert werden in das SWID Tag aufzunehmen.
- **Optional**: Unterstützung weiterer Paket Manager wie z.B. **rpm** (Fedora, RedHat, SuSE) oder **pacman** (Arch Linux).

- Erstellung eines Architektur-Konzepts für die Erfassung und Verwaltung von SWID Tags über eine Erweiterung des bestehenden strongTNC Policy Manager Tools.
- Bidirektionale Verknüpfung der SWID Tags mit den bestehenden strongTNC Objekten *Devices*, *Sessions*, *Packages* und *Files*.
- Implementation der SWID Funktionalität als strongTNC Erweiterung auf der Basis Python/Django.
- Korrektur diverser Bugs in der bestehenden strongTNC Applikation.
- Aufteilung der strongTNC Zugriffsrechte auf einen **read-only** User und einen **admin** User mit erweiterter write/update Berechtigung.

## Links

[1] National Cybersecurity Center of Excellence
**http://csrc.nist.gov/nccoe/The-Center/Mission/Strategy.html**

[2] Continuous Monitoring Building Block - Software Asset Management
**http://csrc.nist.gov/nccoe/Building-Blocks/Continuous%20Monitoring%20Building%20Block%20-%20Software%20Asset%20Management.pdf**

[3] strongSwan TNC Server Funktionalität
**http://www.strongswan.org/tcg/TCC_Orlando_2013.pdf**

[4] strongTNC Policy Manager
**https://github.com/strongswan/strongTNC**

Rapperswil, 17. Februar 2014

Prof. Dr. Andreas Steffen