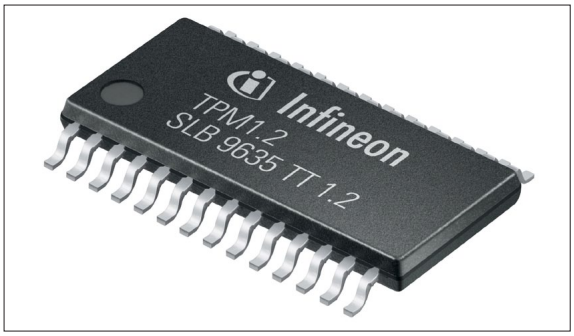
Wolfgang Altenhofer

Lukas Studer

Diplomanden	Wolfgang Altenhofer, Lukas Studer
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich
Themengebiet	Sicherheit

TPM-basierter Integrity Measurement Collector unter Windows 7

Logo unserer Trusted-NAP-Anwendung

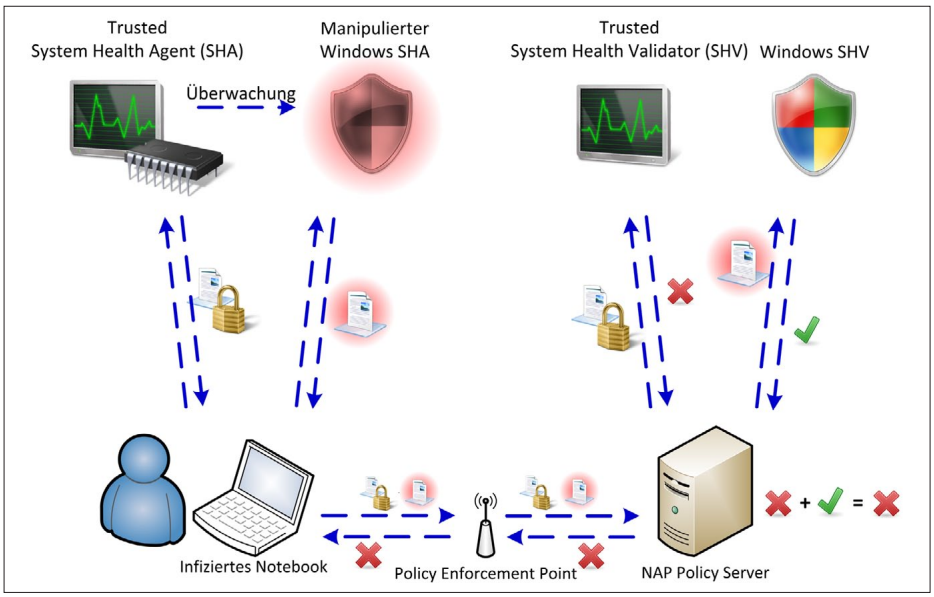


Trusted Platform Module (TPM), das auf dem Motherboard eines Computers festverbaut vorhanden ist

Ausgangslage: Das Microsoft Network Access Protection (NAP) Framework bietet einen zusätzlichen Schutz für Unternehmensnetzwerke. Die Clients werden, bevor sie Zugriff auf die Netzwerkinfrastruktur erhalten, nach definierten Regeln geprüft und erst bei Bestehen dieser Kontrolle in das Netzwerk eingelassen. Im Rahmen dieser Arbeit sollte die Sicherheit dieses Zugriffsschutzes mittels kryptografischer Hardwareunterstützung weiter erhöht werden.

Vorgehen/Technologien: Das Trusted Platform Module (TPM) ist ein auf vielen PC Motherboards festverbauter Chip, welcher dem Rechner zusätzliche Sicherheitsfunktionalitäten auf Hardwareebene zur Verfügung stellt. Dieser wird aufseiten des Clients eingesetzt, um dem NAP-Server zu beweisen, dass keine systemrelevanten Dateien manipuliert wurden.

Ergebnis: Mit Trusted NAP konnte die bestehende NAP-Lösung mit einem Trusted-Computing-Ansatz erfolgreich erweitert werden. Die Funktionalität des TPMs wird dazu eingesetzt, dass Systeme mit manipulierten NAP-Dateien nicht in ein gesichertes Unternehmensnetzwerk gelangen können. Für Systemadministratoren wird es dadurch besser möglich, die Sicherheitspolicies des Unternehmens durchzusetzen. Ein Client ist nicht mehr in der Lage, zu behaupten, dass er einen policy-konformen Sicherheitsstatus besitzt, obwohl effektiv eine Verseuchung vorliegt. Trusted NAP lässt sich überall in bestehende NAP-Infrastrukturen integrieren, wo clientseitig ein TPM sowie Windows 7 und serverseitig ein Windows-Server-2008-R2-Betriebssystem vorhanden sind.



Infizierter Client, der sich in das Unternehmensnetzwerk einwählen möchte. Aufgrund der Malware Detection wird er aber erfolgreich daran gehindert.