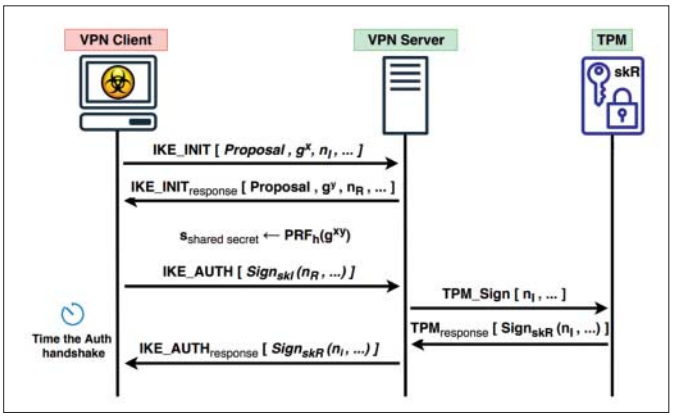
Angriff auf Trusted Platform Modules (TPM 2.0)

Häufig genutzte Sicherheitsmodule für PCs, Notebooks, Tablets und Embedded Systems sind anfällig für einen Angriff, der den vermeintlich gut geschützte **Geheimwert für ECDSA-Signaturen ausliest**. Die Attacke „TPM-Fail“ betrifft Trusted Platform Modules (TPM 2.0) von STMicroelectronics (ST33TPHF2E) sowie das in fast allen PCs mit Intel-Technik vorhandene Firmware-TPM (fTPM 2.0). Glücklicherweise sind nur Anwendungen gefährdet, die tatsächlich den Elliptic Curve Digital Signature Algorithm (ECDSA) des TPM nutzen. Microsoft hat klargestellt, dass das etwa bei Windows nicht der Fall ist – BitLocker verwendet RSA statt ECDSA. Doch OpenSSL für VPN-Server lässt sich für ECDSA per TPM konfigurieren.

TPM-Fail ist eine Timing-Attacke, die winzige Zeitunterschiede auswertet, die bei der Verarbeitung von ECDSA-Signaturen durch das TPM auftreten. Um einen Schlüssel auslesen zu können, sind sehr viele Anfragen nötig, was über eine Stunde lang dauert. Bei Zugriff über ein schnelles Netzwerk auf einen VPN-Server dauert der Angriff rund fünf Stunden. Die TPM-Fail-Entdecker betonen, dass die lückenhaften TPMs von Testlabors nach FIPS 140-2 zertifiziert wurden, das ST33TPHF2E sogar nach Common Criteria Evaluation Assurance Level 4+ (CC EAL 4+). Im Rahmen der koordinierten Veröffentlichung haben STMicro und Intel weitere Informationen und erste Firmware-Updates bereitgestellt (CVE-2019-16863, CVE-2019-11090, Intel Security Advisory SA-00241, siehe ct.de/ygvx). Ein Intel-Tool ermittelt die Version der ME-Firmware. *(ciw@ct.de)*

CSME-Tool: ct.de/ygvx



TPM-Fail extrahiert den ECDSA-Schlüssel aus einem TPM per Timing-Attacke auch via Netzwerk.

Bild: Worcester Polytechnic Institute, Uni Lübeck, UC San Diego

Anzeige

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover