Jan Hutter
Martin Willi

strongSwan II

Eine IKEv2-Implementierung für Linux

Diplomanden	Jan Hutter, Martin Willi
Examinator	Prof. Dr. Andreas Steffen
Themengebiet	Internetsicherheit

Aufgabenstellung: Immer mehr Unternehmen nutzen das Internet, um ihre Standorte kostengünstig zu vernetzen. Das Schlagwort in diesem Bereich heisst VPN und steht für Virtual Private Network. Ein solches VPN wird meistens mit IPsec realisiert, welches das Internet-Protokoll (IP) um Sicherheitsfunktionen wie Vertraulichkeit und Integrität erweitert.
Um eine Verbindung über IPsec herzustellen, müssen sich die Kommunikationspartner vorgängig über diverse Details wie verwendete Schlüssel und Algorithmen einigen. Dazu wird das Internet Key Exchange-Protokoll (IKE) eingesetzt. In der Praxis hat sich gezeigt, dass die Grundfunktionalität von IKE zu unflexibel ist, woraufhin diverse proprietäre Erweiterungen entstanden sind. Leider sind diese teilweise als unsicher zu betrachten. Auch wird IKE als zu komplex und somit fehleranfällig beurteilt.
Die Version 2 von IKE behebt die Fehler der Vorgängerversion. Unsichere Eigenschaften wurden entfernt und nützliche Funktionen hinzugefügt. Es ist zu erwarten, dass das neue IKE-Protokoll das alte in den nächsten Jahren ablösen wird.

strongSwan II –IKEv2 unter Linux

Charon: Fährmann aus den griech. Mythen

Ziel der Arbeit: Die etablierte OpenSource-Software strongSwan bietet unter Linux eine IKE-Implementierung der Version 1. Damit strongSwan auch in Zukunft eine starke Alternative zu anderen Produkten bleibt, ist eine Unterstützung des IKE-Protokolls in der Version 2 erstrebenswert.
Die Architektur von strongSwan ist in vielen Jahren evolutionär gewachsen und deshalb unübersichtlich geworden. Darum soll mit dieser Diplomarbeit eine neue Architektur für strongSwan definiert und in der Programmiersprache C implementiert werden. Die neu aufgebaute Architektur soll einfach zu erweitern sein und die zukünftige Basis von strongSwan II bilden. Des Weiteren soll die Unterstützung für das neue IKE-Protokoll in der minimalsten Form implementiert werden.

Lösung: Der neue Dämon „charon“ ist modular und übersichtlich aufgebaut. Er unterstützt das IKE Protokoll der Version 2 in einer minimalen Form. Im Gegensatz zur Single-Thread Event-Queue des alten IKE-Dämons von strongSwan basiert die neue Architektur auf einem Multi-Threading-Modell.
Wiederverwendbare Algorithmen, beispielsweise zur Verschlüsselung, sind aus dem bestehenden strongSwan-Code übernommen und an die neue Architektur angepasst worden. Die dabei eingesetzten objektorientierten Prinzipien machen den Code verständlicher und einfach erweiterbar.
Mit strongSwan II ist eine Software im Aufbau, welche hoffentlich breite Verwendung findet und von der OpenSource-Community weitergepflegt wird.