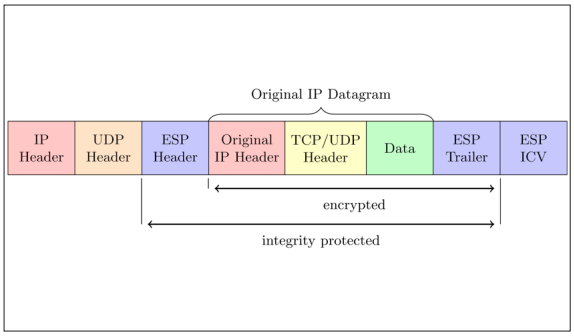
Giuliano Grassi

Ralf Sager

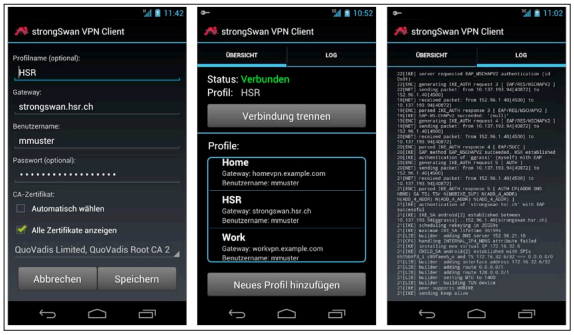
Diplomanden	Giuliano Grassi, Ralf Sager
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich
Themengebiet	Sicherheit

Userland IPsec für Android 4.0

Entwicklung einer Userland-Implementation der IPsec Encapsulating Security Payload (ESP) für Linux und Android



Header eines IPsec-Tunnel-Mode-ESP-Paketes (in UDP gekapselt)



Verschiedene Views des strongSwan VPN Clients

Ausgangslage: IPsec ist normalerweise direkt im Kernel implementiert, während ein Daemon im Userspace für den Schlüsselaustausch über das Internet-Key-Exchange-Protokoll (IKE) zuständig ist. Eine Konsequenz dieser Architektur ist, dass zumindest ein Teil des IKE-Daemons mit Root-Privilegien ausgeführt werden muss, um mit dem IPsec Stack kommunizieren zu können. Dies erschwert den Einsatz von IPsec auf dem Linux-basierten Betriebssystem Android, da Benutzeranwendungen auf vielen Android-Geräten per Default nur eingeschränkte Privilegien haben.

Vorgehen/Technologien: Um dieses Problem zu lösen, wurde im Rahmen dieser Arbeit eine minimale Userspace-IPsec-Implementation für Linux und Android als Teil des strongSwan-Projektes entwickelt. Diese unterstützt die IP Encapsulating Security Payload (ESP) im Tunnel-Modus, zusammen mit den gängigsten kryptographischen Algorithmen. Die für NAT-Umgebungen unabdingbare ESP-in-UDP Encapsulation wird ebenfalls unterstützt. Im Gegensatz zum Linux IPsec Stack verwendet die Userland-Library virtuelle Netzwerk-Interfaces (TUN-Devices) sowie das normale Kernel-Routing zur Steuerung des durch einen Tunnel geschützten Traffics. Des Weiteren wurde ein strongSwan VPN Client für Android entwickelt. Dieser verwendet IKEv2 und erlaubt das Verwalten von mehreren VPN-Profilen. Durch den Einsatz der eigenen IPsec-Implementation sowie einer neuen API in Android 4.0, welche gewisse VPN-bezogene Funktionen zugänglich macht, benötigt dieser IPsec-Client keine erhöhten Privilegien mehr.

Ergebnis: Durch die Entwicklung einer Userspace IPsec-Implementation ist es gelungen, die Hürden zum Einsatz von IPsec-basierten VPNs auf Android zu überwinden. Die entstandene Applikation kann ohne Root-Privilegien benutzt werden und funktioniert daher auf allen Android-Geräten.