

# VOGUE

Handys und andere mobile Endgeräte haben sich in den vergangenen Jahren zu unersetzlichen Begleitern und Arbeitsgeräten einer breiten Bevölkerungsschicht entwickelt. Es gilt in vielen Bereichen der Arbeits- und Privatumgebung, dass verschiedene Abläufe ohne mobile Geräte nicht mehr denkbar sind. Mit dieser Entwicklung geht eine immer stärkere Systemkomplexität einher, die sich auch auf die Sicherheit und damit Vertrauenswürdigkeit der Gesamtlösung auswirkt. Der Anwender erwartet, dass Daten- und Kommunikationskanäle sicher gegen den Zugriff Dritter sind. Dies kann aber nur dann wirkungsvoll gewährleistet werden, wenn auch das Endgerät die erforderlichen Voraussetzungen erfüllt einen solchen Kanal zu sichern.



Es gilt indes aber, dass mobile Endgeräte in einer aus Sicht der Serviceanbieter, Netzbetreiber und Gerätehersteller durchaus „feindlichen“ Umgebung betrieben werden. Die Besitzer der Endgeräte haben abhängig von ihren Absichten unter Umständen ein erhöhtes Interesse die angedachte Funktionalität des Endgerätes zu Manipulieren und auf dieser Weise sich einen Vorteil zu verschaffen. Dies gilt beispielsweise besonders für gestohlene Geräte, die sich per SSL oder andere VPN Techniken Daten vertrauenswürdig und abhörsicher kopieren, aber aufgrund z.B. manipulierter Software diese Daten an nicht autorisierte Benutzer weiter geben. Dies eröffnet einen für die Wirtschaftsspionage interessanten Angriff.

Der Markt verlangt immer stärker integrierte Lösungen, die aufgrund der adressierten Herausforderungen mit einer steigenden Komplexität verbunden sind, aber auch einem starken Kostendruck unterliegen. Flexibilisieren und Wiederverwenden von Anwendungen oder Modulen stellt hierbei eine wichtige Methodik dar. Dies gilt insbesondere auch für den IT-Sicherheitsbereich.

Sicherheit als Service ist eine wichtige Technik, die der Wiederverwendung und der Qualität dient.

VOGUE konzentrierte sich auf die Entwicklung einer integrierten Sicherheitsplattform, so dass mobile Endgeräte vertrauenswürdig auf verschiedenste IT-Systeme (z.B. Lieferketten-übergreifende Applikationen, Unternehmensnetze) zugreifen können. Eine solche Plattform setzt sich hierbei aus Hard- wie auch Software zusammen. Die umzusetzende Lösung wurde auf den Standards des Trusted Computing aufsetzen, die im Kern einen Hardwarevertrauensanker beschreiben. VOGUE baut auf diesen Hardwareeigenschaften von Trusted Computing und mobiler Endgeräte auf und beschreibt eine Softwarearchitektur, mit deren Hilfe ein erweitertes Vertrauen in die Endgeräte durch die Serviceanbieter erreicht wird. Die Sicherheitsmechanismen sind aktuell auf Basis von Android auf mobilen Endgeräten einsetzbar. Durch die Ergebnisse des Projektes VOGUE bekommen insbesondere KMU Methoden und Werkzeuge an die Hand, die das Vertrauen der potentiellen Kunden in neuartige sensible bzw. missbrauchsgefährdete Applikationen nachhaltig und demonstrierbar erhöhen. Der Nachweis des Gewinns an Sicherheit wird am Beispiel des Szenarios „Mobiler Zugriff eines Gastes auf ein Firmennetz“ erbracht.

VOGUE besitzt folgende Hauptmerkmale:

1. Sichere Authentifizierung des Benutzers und der vorhandenen mobilen Hardware
2. Etablieren und Erprobung von TPM-basierten Lösungen
3. Bei fehlender Hardware-Unterstützung, Nutzung eines TPM-Emulators
4. Etablierung einer vertrauenswürdig Plattform für mobile Endgeräte
5. Administrationstool zum Plattform-Management
6. Modulare Plattform, inkl. VPN-Gateway, Firewall, TNC-Server, RADIUS-Server, TNC-/VPN-Client

Komponenten:

- Linux-Betriebssystem ab Linux Kernel 2.4
- Module: OpenVPN, iptables Firewall, RADIUS, TNC, LDAP
- Mobiles Betriebssystem: Android 2.2, 2.3

Systemanforderungen:

- Linux-Betriebssystem
- 2 GHz CPU mit 512 MByte RAM
- 120 GByte SATA Festplatte
- Virtualisierung ist möglich