En Vogue

Eine neue Plattform für die Absicherung mobiler Endgeräte

Kai-Oliver Detken

Durch die Einführung von mobilen Endgeräten wächst der IT-Schutzbedarf stark. Während sich früher Angriffe vor allem gegen die Server richteten, verlagern sie sich heute nicht nur auf die Firewall und das VPN-Gateway, sondern wenden sich besonders gegen Endgeräte, die sich zeitweilig außerhalb des sicheren Netzes befinden. Denn wer sie kompromittiert, erlangt in vielen Fällen zugleich einen bequemen Zugang ins Unternehmensnetz. Natürlich haben sich bereits Lösungen etabliert, die helfen sollen, mobile Geräte abzusichern. Allerdings sind diese meist plattformspezifisch. Neben mehr Interoperabilität wäre daher eine Distributionsplattform wünschenswert, die Software an mobile Endgeräte sicher verteilt und dabei die Installation von Schadsoftware verhindert. Hierzu erhofft man sich von dem BMBF-Projekt VOGUE verwertbare Ergebnisse.

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

Der Einsatz mobiler Endgeräte in Unternehmen steigt derzeit durch zusätzliche Anforderungen an Produktivität und Flexibilität rasant an. Dabei stellen insbesondere die vorhandenen Sicherheitsmechanismen eine Schwachstelle dar, was zum einen an den kurzen Entwicklungszyklen liegt, die Schwächen in der Implementierung beinhalten, und zum anderen an fehlenden PC-ähnlichen Schutzapplikationen. Hinzu kommt, dass die Komplexität mobiler Endgeräte weiter zunimmt. Der Trend geht zum Smartphone, das viele Applikationen sowie mannigfaltige Netzzugangsmöglichkeiten bietet.

Des Weiteren sind mobile Endgeräte heute in Unternehmensnetzen oftmals nicht Teil der IT-Sicherheitsrichtlinien. Die Synchronisation der Daten erfolgt willkürlich durch spezielle Software der jeweiligen Hersteller/Anbieter. Die integrierten Sicherheitsmechanismen reichen auch nicht für einen Schutz unternehmenskritischer Daten aus. Bei Verlust des Gerätes sind die Daten dann unwiderruflich verloren.

Jedes mobile Endgerät stellt heute einen leistungsfähigen Computer dar, der ähnlich aufgebaut ist, wie ein Arbeitsplatzrechner. Zusätzlich enthält es spezielle, für den mobilen Betrieb ausgelegte Hardwarekomponenten (z.B. niedriger Stromverbrauch). Allerdings kann die Hardware mobiler Endgeräte kaum erweitert oder gar verändert werden. *Bild 1* zeigt die wichtigsten Komponenten eines mobilen Endgeräts in Bezug auf die Hardware, wie sie auch für eine Sicherheitsanalyse relevant sind.

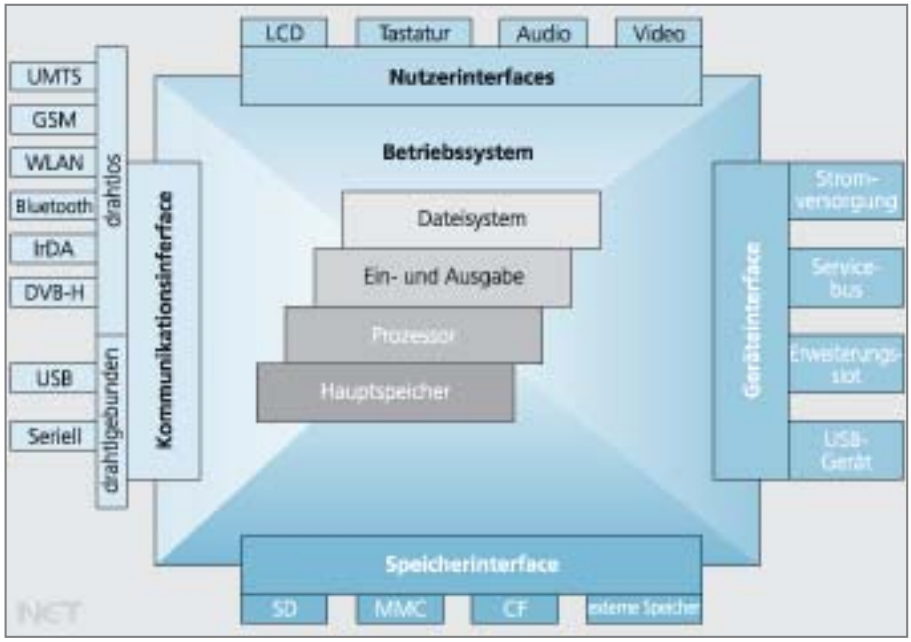

Bild 1: Basismodell eines mobilen Endgerätes

Bei der neuesten Gerätegeneration besteht zwischen Soft- und Hardwareimplementierungen ein fließender Übergang, insbesondere bei der Kommunikationshardware, deren Funktionen maßgeblich durch Software umgesetzt werden. Mannigfaltige Interfaces ermöglichen zwar eine flexible Kommunikation, schaffen aber auch Angriffspotenziale. Weil aber jedes Gerät unterschiedliche Schnittstellen anbietet und diese auch verschieden absichert, hängt die IT-Sicherheit immer stark vom jeweiligen Gerätetyp ab.

Das Vogue-Projekt

Aufgrund der neuen und künftigen Herausforderungen, die an die Vertrauenswürdigkeit von Mobiltelefonen gestellt werden, wird daher im BMBF-Projekt Vogue (Vertrauenswürdiger mObiler ZuGriff auf UnternehmensnetzE, www.vogue-project.de) eine Plattform zur Absicherung mobiler Endgeräte entwickelt. Insbesondere stellt sie Mechanismen für eine vertrauenswürdige Geräteauthentifizierung zur Verfügung. Anhand des Szenarios „Mobiler Zugriff eines Gastes auf ein Firmennetz" wird der Sicherheitsgewinn nachgewiesen. Die in Vogue entwickelte Sicherheitslösung für Mobiltelefone wird aber nicht nur auf das genannte Anwendungsszenario beschränkt bleiben, sondern kann grundsätzlich zur Absicherung mobiler Applikationen eingesetzt werden.

Als Basis der Sicherheitsplattform sind die Mechanismen bzw. die Spezifikationen der Trusted Computing Group (TCG) vorgesehen. Hier kann vor allem auf den Ansatz Trusted Network Connect (TNC) zurückgegriffen werden, der einen vertrauenswürdigen Zugang mobiler Endgeräte zu Infrastrukturen von Organisationen bietet. Der Zeitpunkt für eine erfolgreiche Umsetzung eines solchen Projektes ist günstig, weil mit Android jetzt eine offene Plattform für die Entwicklung auf mobilen Geräten zur Verfügung steht, die eine Realisierung von endgeräteseitigen Sicherheitsmechanismen für TNC und die Integration von Trusted Computing ermöglicht.

Die Integration von Trusted-Computing-Aspekten ist ein Schwerpunkt von Vogue. Daher wurde ein entsprechender TPM-Emulator entwickelt, der es ermöglicht, für die aufkommende Sicherheitstechnik Produkte im Vorfeld anzugehen. Derzeit ist ein solcher TPM-Chip für mobile Systeme zwar spezifiziert, aber seine Markteinführung steht noch bevor.

Die TCG entwickelte mit der TNC-Spezifikation einen Ansatz, um die „Reinheit" von Endpunkten sicherstellen zu können. Das heißt, es kann durch Authentifizierungs- und Autorisierungsinformationen eine Zustandsprüfung erfolgen, die sicherstellt, dass das Endgerät den IT-Sicherheitsregeln des Unternehmens entspricht. Die TNC-Architektur (*Bild 2*) ist somit die Entwicklung einer offenen und herstellerunabhängigen Spezifikation zur Überprüfung der Integrität von Endpunkten, die einen Verbindungsaufbau starten. Die Architektur bezieht dabei schon bestehende Sicherheitsaspekte wie Virtual Private Network (VPN), IEEE 802.1x, Extensible Authentication Protocol (EAP), Transport Layer Security (TLS), Hyper-Text Transfer Protocol Security (HTTPS) und Radius mit ein.

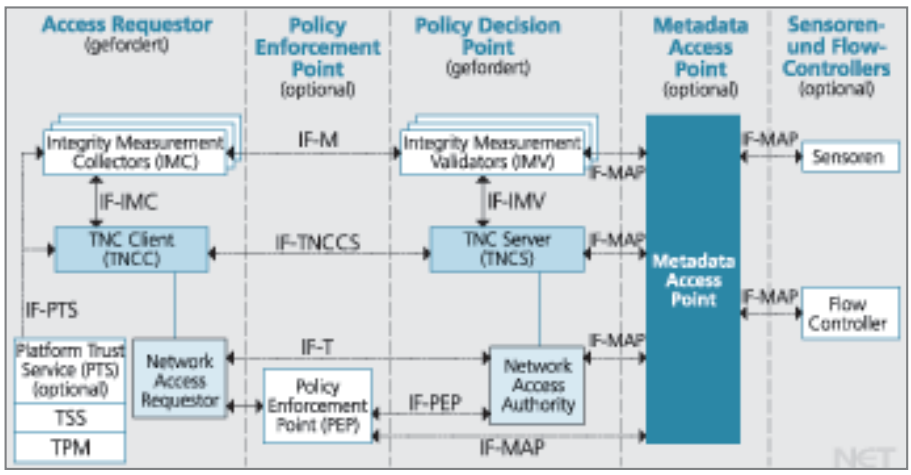

Bild 2: TNC-Architektur

Als Besonderheit bietet TNC optionale Hardwareunterstützung mit dem Trusted Platform Module (TPM) oder dem Mobile Trusted Module (MTM) an. So macht das TPM es u.a. möglich, nur signierte Software auf einem System auszuführen. Während das TPM bereits serienmäßig in Hardware (z.B. von IBM) eingebaut wird, existiert das MTM bisher nur als Entwurf. Darüber hinaus ermöglicht die Einführung des MAP-Servers das Weglassen einer dedizierten Hardwareunterstützung bei ähnlichem Sicherheitsgrad.

Mobile Sicherheitsmechanismen

Heutige mobile Endgeräte besitzen einige implementierte Sicherheitsmechanismen, die sich aus dem Vorhandensein der verschiedenen Betriebssysteme ergeben. Die wichtigsten Mechanismen sind:

- Authentifizierung: Kennwortabfrage und ggf. biometrische Verfahren wie Fingerabdruckscanner;
- Autorisierung: Bei Neustart des Gerätes oder der Nutzung bestimmter Anwendungen kann eine Benutzerauthentifizierung erzwungen werden, um den Teilnehmer zur Nutzung des Gerätes oder für bestimmte Funktionen zu autorisieren;
- Vertraulichkeit: Die SIM-Karte wird bei mobilen Endgeräten als Standardabsicherung zur vertraulichen Speicherung persönlicher Daten verwendet. Auch verschlüsselte Daten werden so abgesichert.

Die Realisierung mobiler Dienste untergräbt allerdings oft die Sicherheitsmechanismen, da die Benutzerdienste meist als Applikation direkt auf dem Endgerät zur Ausführung gebracht werden und dann direkt auf das Application Programming Interface (API) des Betriebssystems zugreifen. Dadurch erlangt man den vollen Zugriff auf die Ressourcen und Funktionen des mobilen Endgerätes. Aus diesem Grund sind Angriffe, die durch Applikationen ausgeführt werden (Viren, Trojaner usw.), besonders gefährlich.

Durch das Signieren der Applikation werden in den meisten Fällen die Echtheit des Herstellers angezeigt und die Gefahr des Kompromittierens verringert. Häufig werden auch Anwendungen durch sog. Frameworks realisiert, die eine Abstraktionsebene der API des Betriebssystems anbieten, beispielsweise bei .NET und Java. Mit einem Sandbox-Framework wie J2ME können dann Zugriffe auf das mobile Endgerät, in Abhängigkeit den Java-Funktionen, kontrolliert und ggf. unterbunden werden.

Die Verschlüsselung mobiler Endgeräte wird sehr unterschiedlich realisiert. Dies bezieht sich insbesondere auf die Schnittstellen zwischen den Verschlüsselungsmechanismen und den Anwendungen der Betriebssysteme. Dadurch werden meist nur wenige mobile Dienste unterstützt oder der Aufwand der Realisierung ist für den Anwender zu hoch. Zusätzlich besitzen viele mobile Dienste eigene Verschlüsselungsvarianten, die aber die Ressourcen der Endgeräte zusätzlich belasten oder sich kontraproduktiv zu den vorhandenen Verschlüsselungsarten der Betriebssysteme verhalten.
Fehlerhafte Implementierungen tun ein Übriges, um die Bedrohungslage für mobile Endgeräte wachsen zu lassen. So hat z.B. Apple bis zum Verkauf des neuen iOS4 für das iPhone allein 65 Sicherheitslücken schließen müssen.
Zudem ist abzusehen, dass ähnliche Angriffe, wie sie heute bei Arbeitsplatzrechnern die Regel sind, künftig auch bei mobilen Endgeräten auftauchen. Hinzu kommt, dass ein mobiles Endgerät sowohl privat als auch geschäftlich genutzt wird. Dadurch verändern sich die Benutzerparadigmen, und neue Anwendungsszenarien ermöglichen neue Sicherheitslücken.

Erhöhung des Sicherheitsniveaus durch Vogue

Gegenüber stationären Betriebssystemen besitzen mobile Systeme zusätzliche Funktionen, z.B. ein aufwendiges Energiemanagement, verschiedene Benutzerschnittstellen oder diverse Kommunikationsvarianten. Auch die verwendeten Dateisysteme sind unterschiedlich und unterstützen z.B. Flash-Speicher sowie das Starten von Anwendungen ohne Ladevorgang. Da der Speicher in mobilen Endgeräten knapp bemessen ist, kommen auch andere Speicherkonzepte zum Tragen. Ein weiterer Punkt ist die heutige Unabhängigkeit zwischen Hardware und Betriebssystem. Dadurch können Neuerungen wie der TPM-Chip nicht mehr so einfach verbreitet werden bzw. lassen sich Sicherheitslücken nicht einheitlich verhindern, da mehr als ein Hersteller für diese Prozesse zuständig ist.

Bei der Komplexität des TNC-Ansatzes stellt sich natürlich die Frage nach der Umsetzbarkeit. Bereits die erste Phase des Verbindungsaufbaus zeigt die Problematik, dass die zuverlässige Erkennung der Verbindungsart und des Endgerätes garantiert werden muss. Anschließend muss das Endgerät an-

Bild 3: TPM-Chip von Infineon, Kooperationspartner von Vogue (Foto: Infineon)

hand der MAC- oder IP-Adresse dem Netz zugeordnet werden. Eine zusätzliche Schwierigkeit kommt hinzu, wenn man nicht voraussetzt, dass der Teilnehmer mit seinem Endgerät ausschließlich gute Absichten verfolgt. Ist das Endgerät mit Malware infiziert oder versucht ein Angreifer direkt in das Unternehmensnetz zu gelangen, wird der offizielle Verbindungsversuch unterdrückt werden. Der TNC-Ansatz muss dann beurteilen, ob das Endgerät den Zugang erhält oder nicht. Zusätzlich muss dem Endgerät das Netz ein Stück weit geöffnet werden. Sobald dann aber der Angreifer eine Verbindung erhält, besitzt er auch weitere Möglichkeiten, um Sicherheitslücken auszukundschaften. Es gibt mannigfaltige Angriffsmöglichkeiten. Problematisch ist zudem, dass der Quarantänebereich für unsichere Endgeräte die Möglichkeit bietet, andere Teilnehmer anzugreifen, die eben-falls nicht eingelassen werden. Denn, da auch diese Endgeräte Sicherheitsschwächen haben, ist die Chance auf Erfolg hier höher als in sicheren Umgebungen.
An diesem einfachen Beispiel sieht man bereits, dass mobile Sicherheit nicht per Installationsroutine realisiert werden kann. Man sollte konzeptionell die Anforderungen an ein solches System im Vorfeld erarbeiten und dann die technischen Systeme dementsprechend umsetzen. Im Vogue-Projekt wird nun eine Plattform zur Absicherung mobiler Endgeräte entwickelt. Aufgrund der Quelloffenheit und definierter Schnittstellen wurde dafür exemplarisch das Betriebssystem Android ausgewählt. Vogue wird eine Sicherheitsplattform zur Verfügung stellen, die Mechanismen für eine vertrauenswürdige Geräteauthentifizierung enthält. Dabei soll ein Sicherheitsgewinn am Beispiel von Android nachgewiesen werden.

Ausblick

Das Vogue-Projekt steht aktuell noch am Anfang. Während in der ersten Phase die Anforderungen anhand eines Business-Intelligence-Szenarios definiert wurden, arbeitet man zurzeit an der Spezifikation der Sicherheitsplattform auf Basis des Trusted-Computing-Standards. Dabei werden auch Sicherheitsanalysen des mobilen Betriebssystems Android durchgeführt. Allerdings haben die verschiedenen Ansätze und nicht fertige Standards dazu beigetragen, dass sich Trusted Computing bisher noch nicht durchsetzen konnte. Auch verlangt der Einsatz von TNC ein globales Netzkonzept im Unternehmen, was die Integration komplexer gestaltet. Zusätzlich haben sich andere Zugriffstechniken im direkten Umfeld weiterentwickelt. Aktuelle Betriebssysteme bieten inzwischen viele Reglementierungsmöglichkeiten, die Benutzermechanismen und Updates des Kernels betreffend. Auch gibt es Lösungen zur Zugriffskontrolle auf Schnittstellen wie USB oder Speicherkarten. Aus diesem Grund geht der Trend eher zur Realisierung von Teilbereichen des Trusted Computing, wie dies beispielsweise durch Authentifizierungslösungen mit Hilfe von Radius-Servern und dem IEEE-Standard 802.1x ermöglicht wird. Um mobile Betriebssysteme sicherer machen zu können, wäre allerdings der Einsatz eines TPM-Chips in Smartphones zu empfehlen (*Bild 3*). Dieser könnte über den Trusted-Computing-Ansatz nicht manipulierbare Messwerte über den Sicherheitszustand der Hardware liefern und so vorhandene Sicherheitslücken der Betriebssysteme kompensieren. *(bk)*