Proaktive Strategien als Fundament der IT-Sicherheit

Sicherheitsstandards in der Seitenlage?

Vor allem im Laufe der vergangenen zehn Jahre haben sich die Angriffe auf IT-Strukturen drastisch vermehrt und der Druck auf die IT-Branche steigert die Nachfrage nach geeigneten Gegenmaßnahmen im Bereich der IT-Sicherheit. Die stetige Anpassung der IT-Sicherheitsstrategien begegnet zwar immer mehr Gefahren und weicht Angriffen aus, ein großes IT-Sicherheitsproblem wird dabei jedoch außer Acht gelassen: Es werden stets nur die wirklich akuten Risiken beseitigt. Somit stagniert die IT-Sicherheit mit den bereits bewährten Problemlösungsstrategien: Erkennen, Analysieren, Anpassen. Das dabei entstehende Flickwerk an Softwarekomponenten leidet dann wiederum an unentdeckten IT-Sicherheitslücken, wie wir jeden Tag den Medien entnehmen können. Diese Lücken werden weltweit immer wieder von Kriminellen für einen erfolgreichen Angriff missbraucht. Eine langfristigere IT-Sicherheitslösung muss daher vor allem neue IT-Sicherheitsmethoden schaffen, die IT-Systeme sicher und robust machen und neue Angriffe abwehren. Proaktive IT-Sicherheitssysteme sind eine hilfreiche Idee, diese Herausforderung zu überwinden.

Bekannte IT-Sicherheitsprobleme

Ein Computersystem umfasst eine Vielzahl an Hard- und Softwarekomponenten. Oft wird diese Vielzahl an Anwendungen gar nicht benötigt. Die Anzahl vorinstallierter Softwarekomponenten steigt schon bei Auslieferung eines neuen Betriebssystems. Um diese Vielzahl an Komponenten zu verwalten, werden von den Herstellern bereits IT-Sicherheitslösungen integriert, über die wir jedoch im seltensten Fall die volle Kontrolle haben.

Eingriffe in solche Strukturen bleiben nur IT-Sicherheitsexperten überlassen. Die Komponenten sind nicht isoliert und haben im eigenen System meist Zugriff aufeinander, solange der Administrator die Konfiguration seiner Benutzeraccounts vernachlässigt. Während sich mobile Betriebssysteme wie Android bereits durch ihre Sandboxing-Lösungen, bei denen jede Applikation (App) in einer eigenen Umgebung ausgeführt wird, auszeichnen, setzen gängige Desktop-Betriebssysteme noch primär auf eine Kontrolle durch Benutzerrechte, die gerade in privaten Haushalten und bei den meisten mittelständischen Unternehmen durch fehlende Erfahrung keine Beachtung finden. Die Komponenten haben dann in der Regel Zugriff auf alles, was dem Benutzer zugeordnet ist. Am Arbeitsplatz ist ein ordentliches Rechtemanagement im Unternehmen also obligatorisch.

Software-Kartenhaus

Isolierung und Rechtemanagement allein zeigen wenig Nutzen, wenn die Schwachstellen in der Qualität der Softwarelösungen stecken. Selbst wenn nur eine Komponente des Computersystems kompromittiert ist, kann das einen erheblichen Einfluss auf die Gesamtsicherheit haben. IT-Sicherheitslücken sind in der Regel keine Absicht, sondern ein Resultat des Entwicklungsprozesses. Software wird noch immer von Menschen entwickelt und so bleiben Fehler, trotz vieler Gegenmaßnahmen durch spezielle Programmiermethodiken und Softwaregutachten, leider nicht aus. Die Fehlerdichte einer Software wird anhand der Fehler pro 1.000 Programmzeilen (lines of code, kurz: loc) gemessen. Der daraus resultierende Quotient sagt dann in etwa aus, wie anfällig ein Programm potenziell ist, wobei erst bei einer Fehlerdichte $< 0{,}5$ ein Programm als wirklich stabil gilt. Eine so geringe Fehlerdichte ist vor allem dort Pflicht, wo Menschenleben von einer Anwendung abhängen, wie beispielsweise bei Steuerungssystemen von Flugzeugen.

Akzeptanz finden Programme jedoch schon ab einem Fehlerquotienten von 10, obwohl in der Regel stets ein Quotient < 2 angestrebt wird. Fehlerhafte Programme können gerichtlich sogar zur Kompensationszahlung [1] verpflichten. Kommerzielle Software weist eine durchschnittliche Fehlerdichte von 0,76 auf, bei Open-Source-Software sogar nur 0,61 [2]. Selbst wenn Fehler behoben werden, sind die Update-Zyklen oftmals sehr lang und damit problematisch.

Andere Kernel, andere Sitten

Es gilt vor allem zu entscheiden, welche Betriebssysteme für welchen Einsatz aus Sicht-

weise der IT-Sicherheit geeignet sind. Zum besseren Verständnis soll ein kleiner Exkurs in die Kernel-Architekturen folgen:

Ein Kernel ist der zentrale Bestandteil eines Betriebssystems und bildet dessen unterste Softwareschicht ab. Kernel unterscheiden mindestens zwei verschiedene Ausführungsmodi, den User-Modus und den privilegierteren Kernel-Modus. Letzterer genießt eine besondere Priorität beim Ausführen von Kommandos und ist daher für unverzichtbare Funktionen geeignet. Zwischen den bestehenden Kernel-Architekturen selbst bestehen gravierende Unterschiede in der Aufteilung der Modi.

Unix und unixoide Systeme wie Android, GNU Linux, BSD und andere basieren auf einem monolithischen Kernel. In dieser Kernel-Architektur sind neben der Prozesskommunikation und Speicherverwaltung bereits viele wichtige Funktionen, wie Zugriff auf die Hardware durch Treiber, im Kernel-Modus implementiert und benötigen keine zusätzlichen Programme. Gegenüber anderen Kernel-Architekturen bietet die monolithische Architektur daher einen Vorteil in Sachen Performance. Architekturen auf monolithischem Kernel sind jedoch anfälliger für Systemausfälle, da fest integrierte, wichtige Teile des Kernels nicht ohne weiteres neu gestartet werden können, falls diese abstürzen. In einem Mikrokernel hingegen laufen nur grundlegende Funktionen im Kernel-Modus, wie Prozess- und Speichermanagement. Alle weiteren Funktionen sind durch eigene Prozesse oder Programmbibliotheken im User-Modus implementiert. Einzelne Komponenten des Betriebssystems können im Betrieb ausgetauscht oder neu gestartet werden, ohne dass deren Absturz das gesamte System gefährdet.

Eine weitere Kernel-Architektur stellt der Exokernel dar, der so weit wie möglich auf Abstraktionen verzichtet, das heißt, er erlaubt Software den direkten Zugriff auf den Speicher. Er löst lediglich Ressourcenkonflikte aus Performancegründen eigenständig und ist in seiner Funktionalität noch weiter eingeschränkt als der Mikrokernel.

Als Alternative zu den bestehenden Architekturen wurde ein hybrider Kernel, eine Mischung aus Mikro- und monolithischem Kernel entwickelt, der versucht, die Vorteile beider zu vereinen. Es sind einige Komponenten des monolithischen Kernels in den Mikrokernel integriert worden, um mehr Performance zu generieren. Nicht alle Funktionen laufen jedoch im privilegierten Kernel-Modus und das Gesamtsystem ist daher weniger anfällig für Ausfälle. Ein Vergleich der Kernel-Architekturen zeigt Abbildung 1.

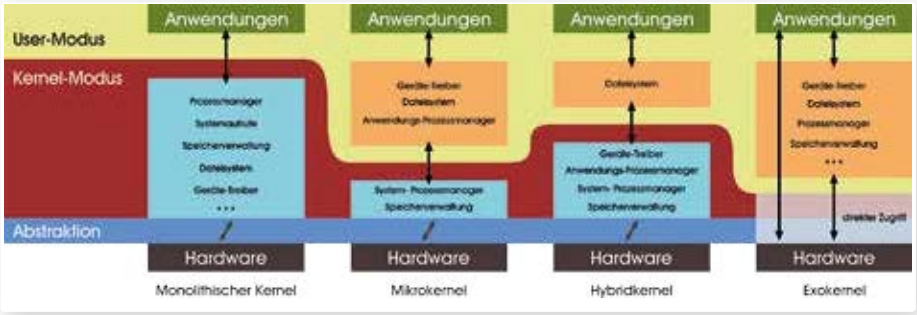

Abb. 1: Kernel-Architekturen im Vergleich

Systeme nach Maß

Die klassische, monolithische Kernel-Architektur eignet sich durch ihre Performance für den Betrieb von Desktop- oder Notebooksystemen. Dasselbe gilt für mobile Betriebssysteme wie Android, da die Anforderungen durch die hohe Bandbreite an Apps mindestens so hoch sind wie bei einem Desktop-PC. Solche Systeme lassen sich zusätzlich abhärten, indem bewusst auf Funktionen verzichtet wird, die für den vorgesehenen Einsatz nicht benötigt werden. So lassen sich beispielsweise einige Linux-Distributionen noch vor der Installation anpassen, wie beispielsweise Hardened Gentoo [3], wo Kernel und Module mit zusätzlichen Sicherheitspatches versehen sind und eigenhändig kompiliert werden. SELinux, eine Open-Source-Erweiterung für den Linux-Kernel, erweitert das System um weitere Zugriffskontrollen (Mandatory Access Control, MAC) und ist als Kernel-Erweiterung im System verwendbar. Durch die Erstellung von Regeln (SELinux Policies) kann ein Rechnersystem problemlos in seinen Aufgaben eingeschränkt werden.

Betriebssysteme sind sehr groß und selbst gehärtet bestehen sie noch aus mehreren Millionen Zeilen Programmcode. Mikrokernel sind vergleichsweise winzig, da viele Funktionen erst durch Programme im User-Modus verfügbar werden. Mikrokernel wie Minix3 [4] bestehen beispielsweise aus etwa 5.000 Zeilen Code. Eine so geringe Menge an Codezeilen ist weitaus effektiver zu prüfen und daher qualitativ hochwertiger zu entwickeln, als es bei einem monolithischen Kernel möglich ist, wie dem Linux-Kernel 4.4, der mit etwa 21 Millionen Zeilen Code zu Buche schlägt.

Alle weiteren Funktionen neben dem absoluten Minimum an Prozess- und Speichermanagement müssen beim Mikrokernel für die entsprechende Hardware selbst implementiert werden. Sie eignen sich daher bestens für Steueranlagen und Anwendungsfälle, in denen nur ein sehr begrenzter, aber stabiler Funktionsumfang vorausgesetzt wird. Je mehr IT-Systeme miteinander vernetzt werden, desto schwieriger wird es, die Fehlerrate einzelner Komponenten zu reduzieren und durch das Gesamtsystem zu kompensieren. In Zeiten der Industrie 4.0 sollte der vermehrte Einsatz von Mikrokernel daher dringend in Betracht gezogen werden, auch wenn die Anpassung und Spezialisierung solcher IT-Systeme sehr zeit- und kostenintensiv ist. In kritischen Infrastrukturen sind Ausfälle nur schwer hinnehmbar.

Sicherheitskritische Softwarekomponenten sollten daher in einer minimalen Systemschicht zwischen Kernel und Anwendung untergebracht werden. Zusammen mit Hardware und Kernel bildet sie die Trusted Computing Base (TCB), deren Integrität vor Ausführung verifiziert werden muss [6]. So wird der unerlaubte Zugriff auf diese Komponenten noch einmal erheblich erschwert. Wenn in der TCB eine Schwachstelle vorhanden ist, dann ist das ganze IT-System betroffen. Schäden durch Schwachstellen oberhalb können anhand von Sicherheits-

Policies eingeschränkt werden, daher sind TCB sehr sorgfältig designt und implementiert. Basiert eine TCB auf einem Mikrokernel, besteht sie zusammen mit den Virtualisierungs-, Isolierungs- und Sicherheitsmechanismen aus etwa 100.000 Codezeilen und lässt sich auch schon semiformal verifizieren, was es möglich macht, einen sehr hohen Level an Softwarequalität zu erreichen.

Abb. 2: Trusted Computing Base

Sicherheit beginnt bei der Hardware

Software alleine hat aber auch ihre Grenzen. Eingebaute Software-Schutzmechanismen können manipuliert werden und dürfen keine Aussage über die Integrität eines IT-Systems tätigen. Die Wahl einer geeigneten Hardware zum Schutz der Software gehört zu den vielversprechenderen Ansätzen im Bereich der IT-Sicherheit. Viele Sicherheitsprobleme können durch spezielle Sicherheitsanker im Vorfeld abgeschwächt oder teilweise sogar verhindert werden. Sicherheitsanker repräsentieren einen stark vertrauensvollen Punkt im Computersystem und lassen sich durch autonome Hardwarekomponenten realisieren.

Das Trusted Platform Module (TPM) verfügt über einen kleinen Krypto-Prozessor, der einen Zufallszahlen-, Schlüssel-, Hashgenerator usw. bereitstellt. Als Sicherheitschip ist das TPM fest mit dem Mainboard eines Rechnersystems verbunden. Es wird im Rahmen vertrauenswürdiger IT-Systeme dazu benutzt, Manipulationen an der Hard- und Software aufzudecken, bei denen mit geeigneten Maßnahmen bis hin zur Sperre des IT-Systems reagiert wird. Jedes TPM enthält einen speziellen, ihm zugeordneten Basis-Schlüssel (Endorsement Key – EK). Der EK verlässt das Modul nach Erzeugen nicht mehr, sondern kann nur durch Erzeugen eines neuen Schlüssels überschrieben werden. So bleibt sichergestellt, dass der EK des TPM nicht extern missbraucht wird. Das TPM kann auch genutzt werden, um die im Betriebssystem verwendeten Schlüssel zu verwalten. Dazu wird ein weiterer Schlüssel des TPM – der Storage Root Key (SRK) – bereitgestellt, um alle im TPM gespeicherten Schlüssel des Benutzers abermals zu verschlüsseln. Private Schlüssel zur E-Mail-Kommunikation lassen sich auch auf die Art sicher über das TPM verwalten.

Seit 2014 ist der neue Standard TPM 2.0 [7] verabschiedet und löst den bisherigen TPM 1.2 ab. Ein maßgeblicher Unterschied zum Vorgänger ist die Implementierung noch stärkerer Krypto-Algorithmen wie SHA-256 und elliptischer Kurven. Unterstützt wird er bereits von den Betriebssystemen ab Windows 8 beziehungsweise dem Linux-Kernel 4.0. In einer Variante für mobile Endgeräte zeigt sich das von der Trusted Computing Group als Spezifikation entwickelte Mobile Trusted Module (MTM) [5]. Das MTM wurde bislang nur selten im Unternehmensumfeld oder im Labor für wissenschaftliche Arbeiten verwendet. Eine flächendeckende Verwendung gibt es hier bislang also nicht. So wären bei entsprechender Implementierung auf Endgeräten sowohl sichere Transaktionen, die geschützte Lagerung von Schlüsseln und Zertifikaten als auch die Integritätssicherung des Endgeräts möglich.

Sicherheit im Hosentaschenformat

Smartphones sind kleine Rechnersysteme und sowohl im privaten als auch im Unternehmensumfeld stark verbreitet. Hochwertige Hardware-Sicherheitschips wie das TPM weisen zwar einen umfassenden Kern an kryptografischen Funktionen auf, die Verfügbarkeit für gängige Smartphones ist in der Praxis jedoch schlecht, da sie ursprünglich für den Einsatz in Notebooks und Desktop-Rechnersystemen entwickelt wurden. Im Bereich der Smart Mobile Devices haben diese jedoch nie Einzug gefunden und sind nur selten im Unternehmensbereich oder in der Forschung anzutreffen.

Die Notwendigkeit eines Sicherheitsankers in dieser Endgeräteklasse macht die Suche nach Alternativen erforderlich; eine Smartcard könnte hier in einigen Punkten Abhilfe schaffen. Smartcards sind auch hochwertige Hardware-Sicherheitschips, die in verschiedenen Formfaktoren am Markt erhältlich sind. Die am meisten gebräuchlichen Varianten sind die klassische Chipkarte im Scheckkartenformat und USB-Sticks mit NFC-Schnittstellen.

Smartcards bieten eine Reihe an kryptografischen Funktionen und sind als Sicherheitstoken einer Public-Key-Infrastruktur (PKI) gebräuchlich. So lassen sich Angestellte innerhalb eines Unternehmens identifizieren und authentifizieren, um entsprechende Zugriffe durch Zertifikate zu schützen. Smartcards werden auch im Format einer MicroSD-Karte gebaut, stießen im Smartphone-Bereich jedoch durch die Limitierung ihrer Kartenslots auf Ablehnung, da die Möglichkeit der Speichererweiterung damit entfällt. Seit einiger Zeit sind daher MicroSD-Smartcards auf dem Markt, die auch über einen eingebauten Flash-Speicher verfügen. Die eigentliche Smartcard ist dabei vom Speicher getrennt. Mit den neuen, vielfältigen Möglichkeiten einer Smartcard muss das Ziel gesetzt werden, die proaktiven Sicherheitsmechanismen auch auf Smartphones zu übertragen. Smartcards sind durch die physikalische Trennung vom Mainboard des Rechnersystems im Gegensatz zum TPM nicht fest mit der restlichen Hardware verbaut und sollten daher, anders als das TPM oder MTM, nicht für eine Integritätsmessung herangezogen werden. Sie sind dagegen aber austausch- und nachrüstbar für alle Endgeräte mit einem regulären MicroSD-Kartenslot. Ihre kryptographischen Funktionen unterstützen dann das Endgerät. Die Sicherheit muss also nicht nur aus dem Smartphone und von dessen Hersteller kommen.

Im Rahmen eines Forschungsprojekts im Institut für Internet-Sicherheit – if(is) wird unter dem Namen „SmaSA – Smartcard Based Security Anchor for Android" in Zusammenarbeit mit Rohde & Schwarz Cybersecurity (Sirrix AG) bereits in diesem wichtigen Umfeld geforscht. Ziel ist die herstellerunabhängige Endgerätesicherheit durch Sicherheitsanker für das Betriebssystem Android. Um den Mangel an TPMs in mobilen Endgeräten auszugleichen, soll eine Smartcard die Nach-

frage an Funktionen bedienen, die unter anderem zum sicheren Speichern der Schlüssel als auch zur sicheren Authentifizierung des Benutzers vor dem eigentlichen Startvorgang (Pre-Boot Authentication) des Geräts genutzt werden. Erst eine erfolgreiche Anmeldung gibt dann das Gerät zur Nutzung frei. Alle Anwendungen, Daten und auch das Betriebssystem selbst sollen ansonsten verschlüsselt bleiben. Technologien wie ARM® TrustZone® oder andere Trusted Execution Environments (TEE) sollen für diese Absicht ebenfalls erforscht und dann, wie Abbildung 3 demonstriert, eingesetzt werden.

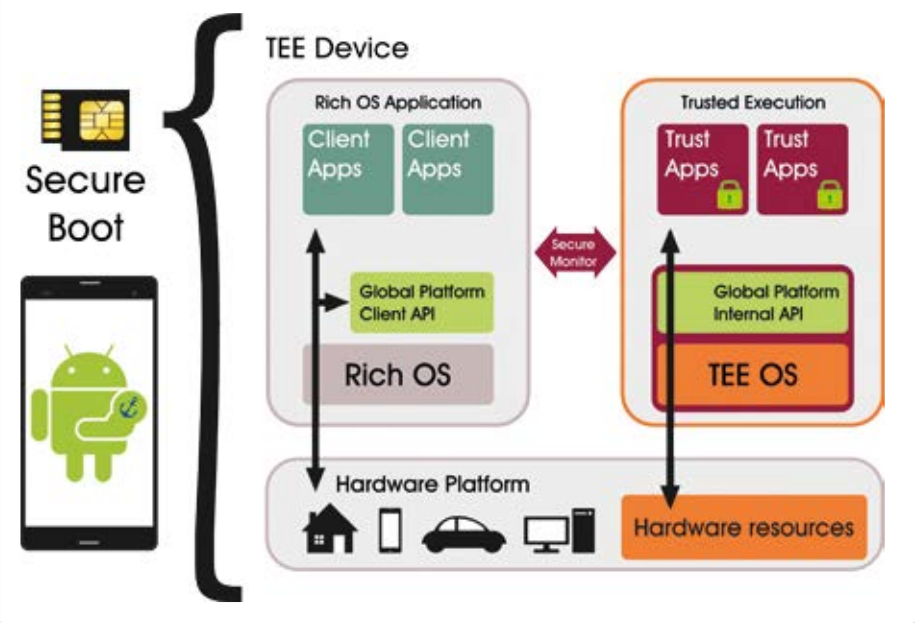

Abb. 3: SmaSA-Trusted-Execution-Konzept

Diese Konzepte sind im Bereich der Desktop-Umgebungen bereits vorhanden, doch ist es unabdingbar, die neuen Technologien auch für Smartphones zu erschließen, da sie bei bleibender Entwicklung nicht mehr aus den gängigen Geschäftsprozessen eines Unternehmens herauszudenken sind. Durch die Möglichkeit, solche Sicherheitsanwendungen auch auf Android zu benutzen, ergeben sich viele neue Einsatzfelder für die Technologien. Das Projekt nutzt dabei bestehende, Hardware-gestützte Technologie, um einen vergleichbaren Schutz zu IT-Sicherheitssystemen auf PC-Basis zu schaffen.

Fazit

Es herrschen auch weiterhin die bekannten Probleme der IT-Sicherheit vor, dabei sind alle Endgeräte – völlig unabhängig von ihrer Art – betroffen. Forschung und Entwicklung müssen die Verfügbarkeit bewährter Technologien für jede Endgeräteklasse in den Fokus fassen. Sicherheitslücken in der Software werden auch in den kommenden Jahren noch eine sehr reale Bedrohung darstellen. Professionelle Hacker nutzen dies für ihre Zwecke aus. Die einzig wirksame Methode ist der Entzug der Grundlage durch das sorgfältige Zusammenstellen ihrer Softwarekomponenten. Zukünftige Computersysteme müssen daher gehärtet und entschlackt werden. Sie dürfen nie mehr Software enthalten, als unbedingt für ihren speziellen Zweck notwendig ist.
Mit dem Ziel, die Risiken für IT-Systeme zu minimieren, muss ein verantwortungsvoller Umgang mit bestehenden Möglichkeiten in der IT-Sicherheit stattfinden. Die Notwendigkeit, IT-Systeme zukünftig exakt auf ihren Aufgabenbereich abzustimmen, ist dabei die vielversprechendste Aufgabe für Unternehmen und Forschung. Innovative Ansätze helfen dabei, diese Verantwortung gemeinsam umzusetzen. ■

[1] *Linda Laird & Carol Brennan: „Software Measurement and Estimation: A Practical Approach.", Wiley & Sons, 2006*
[2] *Coverity® Scan Open Source Report 2014*
[3] *https://wiki.gentoo.org/wiki/Project:Hardened, zuletzt abgerufen am 04.03.2016*
[4] *http://www.linux-magazine.com/Issues/2009/99/Minix-3, zuletzt abgerufen am 04.03.2016*
[5] *http://www.trustedcomputinggroup.org/solutions/mobile_security, zuletzt abgerufen am 04.03.2016*
[6] *A. Speier, N. Pohlmann: „Eine Diskussion über Trusted Computing – Sicherheitsgewinn durch vertrauenswürdige IT-Systeme". IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 5/2013*
[7] *http://www.trustedcomputinggroup.org/resources/tpm_library_specification, zuletzt abgerufen am 04.03.2016*

DAVID BOTHE,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen im Forschungsbereich „Vertrauenswürdige IT-Systeme"

ANDREAS SPEIER,
wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen und Leiter des Forschungsbereiches „Vertrauenswürdige IT-Systeme"

NORBERT POHLMANN,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen