Security by Isolation Prinzipien in der öffentlichen Verwaltung

Sanfte Migration zu virtualisierten Anwendungen bei bestehenden Betrieb im Rahmen des Open Security Projekts

Ross King, Mihai Bartha, Oliver Maurhart
AIT Austrian Institute of Technology

April 10, 2014

Abstract

Das Open Security Projekt integriert "Security by Isolation" Techniken in die öffentliche Verwaltung. Hauptaugenmerk liegt dabei auf den Schutz gegen Viren und Trojaner beim unbedarften und sorglosen Umgang mit dem Internet, Schutz gegen Infektionen mit Malware beim Laden von Dokumenten von Datenträgern wie USB-Sticks und ähnlichen sowie Schutz vor der unbeabsichtigten Veröffentlichung vertraulicher Informationen. Die Integration der Schutzmaßnahmen erfolgt dabei unaufdringlich in eine bestehende IT Infrastruktur ohne die vorhanden und verwendeten domainspezifischen Lösungen und Einrichtungen zu gefährden. Wir zeigen in dieser Arbeit wie eine sanfte Überführung und Migration einzelner bestehender Anwendungsfälle im großen Maßstab im öffentlichen Bereich mit Hilfe von Open Source bei gleichzeitigen Betrieb erfolgen kann. Die angestrebte Lösung richtet sich nach dem Security by Isolation Ansatz aus mittels diesem Applikations- und Systemgrenzen definiert werden um potentielle Schadsoftware einzugrenzen.

1 Motivation

Jede Organisation muss ihre IT-Infrastruktur vor internen und externen Gefahren schützen. Besonders davon betroffen sind auch öffentliche Institutionen, welche private Bürgerdaten wie Strafregister, Krankengeschichte und Meldedaten oder für die Staatssicherheit relevante Informationen verwalten.

Wie Einzelfälle und Statistiken belegen[1], kommt es aber immer wieder und zunehmend häufiger zu Vorfällen, bei denen private Daten in falsche Hände geraten. Solche Daten können in kürzester Zeit weltweit über das Internet verteilt werden, was schnell zu Worst-Case-Szenarien führen kann. So können beispielsweise private Adressen von Polizeibeamten ihren Weg zu kriminellen Organisationen finden oder private Gesundheitsdaten in die Hände potenzieller zukünftiger Arbeitgeber.

Durch die sensible Natur dieser Informationen, sind die Nutzer solcher öffentlichen Einrichtungen oft zu geschlossenen und sicheren lokalen Netzwerk gedrängt. Diese Systeme verfügen oft über keinen Zugang zum Internet (WWW) oder über Anschlüsse für tragbare Speichermedien (TSM) um den sorgfältigen Umgang mit diesen Daten zu gewährleisten.

[1] WELCHE?

Das von der FFG[2] geförderte Open Security[3] Projekt bietet eine Lösung, die Angestellten davor schützt, kritische oder sensible Daten ungewollt preiszugeben. Dieser Schutz beläuft sich auf den Verlust oder den Diebstahl von Datenträgern (z.B. USB-Sticks) und den Befall des Rechners oder Notebooks von Viren, Trojanern und dergleichen. Dabei soll jeder Computer oder Terminal einer Organisation so ausgestattet werden, dass unkontrollierter Datenaustausch verhindert wird.

Bei diesem Projekt kommt erschwerend zur Aufgabenstellung hinzu, dass die Zielumgebung ein heterogenes Anwendungs- und Systemspektrum aufweist, keines der betroffenen Systeme völlig neu aufgesetzt werden darf und ein Rollout zentral gesteuert auf mehreren Rechnern, möglicherweise entfernt in parallel, stattfindet.

Unser Lösungsansatz im Open Security Projekt ist eine Client Architektur, die sicherstellt, dass alle auf tragbare Geräten gespeicherten Daten basierend auf einem Digital Rights Management automatisch verschlüsselt werden. Persönliche Daten von BürgerInnen können ausschließlich verschlüsselt auf Festplatten, optischen oder USB-Speichern sowie externe Netzlaufwerken gespeichert werden. Durch Open Security soll jeder Computer oder Terminal einer Organisation unabhängig von seinem Betriebssystem davor geschützt werden, unkontrollierten Datenaustausch zuzulassen. Das Einbringen oder das Mitnehmen von elektronischen Daten durch die Benutzer soll, im Sinne des Institution und des Benutzers selbst so erfolgen, dass es zu keinem Schaden oder Missbrauch kommen kann. Der gestohlene Laptop, der verlorengegangene USB-Speicher oder das verlegte Mobile Device (wie Tablet-PC oder Smartphone) sollen zukünftig außer dem materiellen keinen weiteren Schaden verursachen.

Im Fall, dass Hardware (z.B. ein Notebook) oder Speichermedien (z.B. ein USB-Stick) verloren gehen oder gestohlen werden, sind keine sensiblen unverschlüsselten Daten gefährdet. Wurden dennoch sensible Daten preisgegeben, was aufgrund von Richtlinien genehmigt werden kann, dann rekonstruiert die Kontrollkette aus den aufgezeichneten Datenströmen den Ereignispfad. Anhand der Informationen aus einem zentralisierten Logging kann nachvollzogen werden, welche Daten die Organisation verlassen haben und auf welchem Weg (z.B. durch welchen Benutzer, Medium).

Die Innovation von Open Security besteht in der Verbindung des DLP[4]-Ansatzes mit einer zentralen Management-Lösung und einer “Security by Isolation” Architektur.

Das Internet, als dicht vernetztes Gefüge untereinander verbundener Geräte, bietet eine ideale Angriffsfläche für sich selbst replizierenden Schadcode. Aus diesem Grund ist Anti-Virensoftware ein zentraler Bestandteil jeder Sicherheitsstrategie. Eine solche Lösung ist stark abhängig von Signatur-Updates und schützt nur vor bekannten Malware. Nicht entdecktes Malware kann als erstes den Update-Mechanismus des Antivirus deaktivieren um später nicht entdeckt zu werden.

2 Security by Isolation

Heutige Mainstream-Betriebssysteme für den Desktop wie Apple Mac OS X, Microsoft Windows oder auch Linux, sind unzureichend, wenn es um die Datensicherheit geht. Ihr gemeinsames und unüberwindliches Problem liegt darin, dass sie nicht in der Lage sind, die verschiedenen Programme, die gleichzeitig auf einem Rechner laufen, ausreichend von einander zu isolieren. Wenn zum Beispiel der Browser einer Nutzerin oder eines Nutzers durch einen aus dem Netz geladenen Trojaner kompromittiert wird, ist das Betriebssystem normaler Weise nicht in der Lage, andere Software oder auch Daten davor zu schützen, ebenfalls kompromittiert zu werden. Besonders schwerwiegend

[2] Österreichische Forschungsförderungsgesellschaft
[3] http://www.opensecurity.at
[4] ERKLÄRUNG

wird das Problem, wenn wichtige Systemkomponenten, wie etwa die Gerätetreiber, kompromittiert wurden. In so einem Fall ist keines der genannten Betriebssysteme in der Lage, die übrige Software oder die Daten der NutzerInnen vor dem kompletten Kompromittieren zu schützen. Dieser kritische Zustand lässt sich direkt auf Designentscheidungen der Systemarchitekturen zurückführen. Diese schließen zu komplexe Programmierschnittstellen (API) ebenso ein wie unsichere graphische Nutzerschnittstellen (GUI) und monolithische Kernelarchitekturen.

Bisher wird vor allem auf reaktive Ansätze zurückgegriffen. Viele Anbieter versuchen, jede bekannte Sicherheitslücke zu patchen. Solche Ansätze skalieren aber nicht nur nicht, sie funktionieren schon deshalb nicht, weil nur bekannte und vor allem viel genutzte Angriffe abgewehrt werden können. Vor neuen oder nicht so bekannten, gezielter ausgenutzten Sicherheitslücken kann so nicht geschützt werden.

Die Alternative zu diesem als "Security by Correctness" bekannten Ansatz verfolgt eine ganz andere Herangehensweise: "Security by Isolation" (Sicherheit durch Isolation). Die Idee dabei ist, ein System in getrennte Untersysteme aufzuspalten so dass ein Fehlverhalten eines Teilsystems nicht andere Teilsysteme berührt. Die Aufteilung in sinnvolle Untersysteme und das Einrichten geeigneter Zugriffsrichtlinien ist einer der Hauptaufgaben und größten Herausforderungen. Dieser Ansatz vermittelt nun Anwenderzugriffe und -Umgang mit Ressourcen aus unsicheren oder zweifelhaften Quellen wie Internet oder Mobile Datenträger indem die dabei verwendete Teilsysteme durch Virtualisierung voneinander getrennt werden. Durch den Einsatz dieser Virtualisierungsschicht werden die darin gekapselten Systemkomponenten vom Trägersystem unabhängig und sind somit auf einer Vielzahl aktueller und moderner Desktop Betriebssysteme implementier- und ausführbar.

Es gibt zwei wichtige Projekte, die dieser Herangehensweise folgen: Ethos ist ein sicheres Betriebssystem, das auf den Xen Hypervisor aufsetzt. Seine Entwicklung wird von Jon Solworth von der University of Illinois, Chicago, geleitet und von den Kryptographen Daniel Bernstein und einem Team von Mitwirkenden unterstützt. Qubes wird von Joana Rutkowska, die durch ihre Arbeit an Rootkits bekannt ist, und von Rafal Woitcuk, beide vom Invisible Thing Lab, entwickelt.

Beide Systeme setzen allerdings auf den Xen Hypervisor und damit auf ein Linux (bzw. BSD oder Solaris) Grundsystem, auf dem in Folge weitere Systeme aufgesetzt werden. Da das Open Security Projekt sich an den Einsatz im öffentlichen Bereich orientiert ist von einer großflächige Umstellung auf ein derartiges bare-metal Virtualisierungssystem abzusehen.

Im Open Security Projekt werden die "Security by Isolation" Konzepte angewendet um mögliche durch Malware verursachten Schäden mittels einer in erster Linie hosted Virtualisierung entgegenzuwirken. Eine zentralisierte und im Fehlen einer Verbindung zum zentralen Dienst auch lokale Anti-Virus Architektur detektiert in einen eingegrenzten Bereich Malware bevor diese auf sensible Bereich des Systems übergreifen kann. Die dabei entstandenen Komponenten und Dienste lassen sich aber auch auf eine bare-metal Virtualisierung wie XEN implementieren.

3 Architektur

Aus der Perspektive von Open Security werden zwei Sicherheitszonen identifiziert: das sichere Netzwerk (SN) ist das zu schützende Unternehmensnetzwerk des Bedarfsträgers. Die Interaktion des Benutzers ist aufgrund der sensiblen Natur der Informationen und Daten zur Zeit auf dieses Netz begrenzt. Das SN gilt als vertrauenswürdige und wird durch Isolation von der Außenwelt getrennt. Es existieren sehr strenge Zugangsbeschränkungen zu externen Ressourcen um die Datensicherheit im SN nicht zu kompromittieren. Die Sicherung der Interaktion mit eben unsicheren oder zweifelhaften Ressourcen (mobile Datenträger und Internet) kann auf diese großen

Herausforderungen heruntergebrochen werden:

1. Vermittlung und Steuerung des Zusammenspiels mit unsicheren Ressourcen.
2. Schutz des SN vor Malware.
3. Schutz sensibler Informationen vor Diebstahl oder durch Verlust von tragbaren Geräten.

Prinzipiell kann eine bare-metal- als auch user-space- Virtualisierungslösungen verwendet werden. Im Open Security Projekt existiert eine generische Virtual Machine (VM) Orchestrierung Schicht, die leicht erweiterbar ist, um weitere Hypervisoren unterstützen können. Um eine fließende Migration einer bestehenden Infrastruktur zu ermöglichen basiert die aktuelle Implementierung auf einem user-space Virtualisierungslösung (VirtualBox) auf einem bereits existierenden Betriebssystem (Windows).

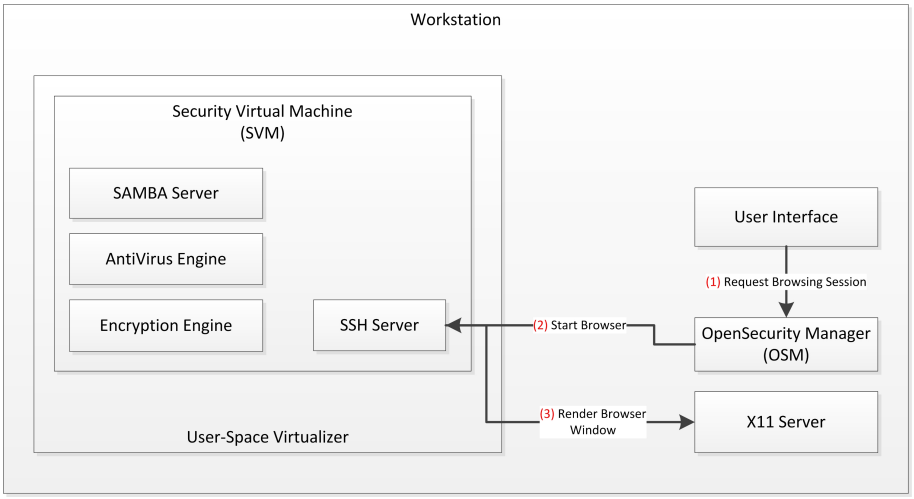

Figure 1: Architektur - Sichere Internet-Zugang

Die wichtigsten architektonischen Komponenten sind der Open Security Manager (OSM) und die Security Virtual Machine (SVM). Das Open Security System ist rund um die SVM, eine auf Linux basierende virtuellen Maschine inklusive der tatsächlichen Subsystemen, welche die Interaktion des Benutzers mit den unsicheren Ressourcen vermittelt, gebaut. Der OSM ist eine Management Schichte zur Steuerung der Virtuellen Maschinen samt Benutzeroberfläche und ist für die Verarbeitung von Benutzeranforderungen sowie Hardware-Events (bsp. USB) verantwortlich.

3.1 Sicheres Surfen

Beim Start einer Browser-Sitzung kümmert sich der OSM um die Instanziierung, Konfiguration und Start einer neuen SVM, welche speziell nur für diese Browser-Sitzung verantwortlich ist. Die neue SVM-Instanz wird als Disposable Virtual Maschine (DVM - “Wegwerf” Virtuelle Maschine) aus einer vorhandenen SVM-Vorlage erstellt .

DVMs sind eigens hergestellte virtuelle Maschinen, die leicht instanziiert und wieder entsorgt werden können, mit ebenfalls sehr kurzen Bootzeiten. Das DVM Konzept wird durch die Nutzung von

unveränderlichen virtuellen Festplatten-Snapshots und differenzierender Festplatten-Abbildungen sowie mit einer SVM-Vorlage im Ruhezustand implementiert. Diese Lösung stellt sicher, dass alle Änderungen der Browser-Sitzung (wie auch möglicherweise unerkannte Malware) in der DVM an der neuen SVM-Instanz gemacht werden und bei Beendigung der Sitzung gelöscht werden.

Außerdem hat diese Lösung den Vorteil der Minimierung an Plattenplatznutzung und ermöglicht eine einfache Aktualisierung der SVM Vorlage. Durch das Update der Vorlage wirken Änderungen in allen neu erstellten SVM Instanzen. Der Update-Mechanismus wird durch das OSM Update-Backend angestoßen, welcher auf ein Paket-Repository des Open Security Projekt zurückgreift.

Die Referenz SVM-Implementierung basiert auf einer minimalen Debian Installation. Die installierten Software-Pakete enthalten einen Web-Browser, Verschlüsselungs-Software, Antivirensoftware, einen SSH-Server und einen SAMBA-Server.

Aus Sicht des OSM umfasst das Starten einer neuen Browser-Sitzung mehrere Konfigurationsaufgaben. Der OSM startet einen X11-Server auf dem Host-Betriebssystem und nutzt einen SSH-Client mit X-Weiterleitung um den Browser innerhalb der SVM auszuführen. Dies ermöglicht eine nahtlose Integration des Browserfensters innerhalb der Host-Umgebung und lässt die Anwendung, welche in einer DVM läuft, native in der gewohnten Umgebung erscheinen. Um auf mögliche heruntergeladene Dokumente zuzugreifen, nachdem diese geprüft wurden, wird zusätzlich der Download-Ordner des Browsers von der SVM als SAMBA Netzlaufwerk im Hostsystem eingebunden.

Beim Zugriff auf heruntergeladene Inhalte wird die angesprochene Datei nicht direkt sofort auf das Hostsystem übermittelt, sondern duch den Einsatz von OsecFS automatisch mittels einer Anti-Virus Einheit auf Malware untersucht. Das OsecFS basiert dabei auf einen FUSE[5] Ansatz und bietet somit ein virtuelles Dateisystem dem SAMBA Service innerhalb der SVM an. Das Backend des OsecFS bietet dabei generische Schnittstellen um adaptiv beliebige Anti-Viren Systeme anbinden zu können. Vorrangig gilt es dabei unternehmensweite Anti-Viren Server Systeme anzusprechen, allerdings sind auch lokale AV Prüfungssysteme integrierbar.

Der SVM-Instanz wird eine Host-Only-Netzwerkschnittstelle für die Kommunikation mit dem Host zugewiesen. Auf dieser sind nur vom Host initiierte Verbindungen zugelassen. Die SSH-Kommunikation wird durch automatisch generierte Public/Private Schlüsselpaare gesichert und der Verbindungsaufbau durch Bereitstellen der authorized_keys Datei in einem spontan erzeugten ISO-Image ermöglicht. Diese Verbindung dient zum einen dem OSM die Virtuelle Maschine zu administrieren, zum anderen auch um das GUI der jeweiligen Anwendung innerhalb der SVM auf den Host darzustellen.

Damit die SVM auch eine Verbindung nach aussen über den Host hinaus besitzt, verfügt schließlich die SVM auch über eine NAT-Schnittstelle für den Zugriff auf das Internet. Die Kommunikation, welche über dieses NAT Interface läuft, wird durch die user-space Virtualisierungslösung (VirtualBox) über dessen Netzwerk Treiber durch den Host durchgeleitet.

3.2 Sichere Datenverwaltung auf externen Trägern

Der Umgang mit Daten auf externen Trägern wie USB Sticks hat neben dem Ziel den Anwender und damit das Host System von Malware zu schützen auch die Intention sensible Daten nur verschlüsselt auf diese Medien abzulegen.

Der OSM unterbindet das automatische Laden von Gerätetreiber und das Einhängen von geöffneten Dateisystemen am Hostsystem. Statt dessen wartet der OSM auf entsprechende Hardwareevents und leitet diese an neu instantiierte SVM Einheiten weiter. Diese SVMs binden

[5] Filesystem in user space

nun die jeweiligen Gerätetreiber innerhalb ihres Systems ein, können damit die neu hinzugefügte Hardware ansprechen und öffnen den Datenträger. Analog zum Download Bereich aus vorigem Kapitel über das Sichere Surfen wird auch hier der Dateninhalt nicht unmittelbar über eine SAMBA Schnittstelle an das Hostsystem weitergeleitet. Vielmehr prüft auch hier eine OsecFS Instanz sämtliche open und read Anweisungen und leitet die betroffenen Dateiströme an ein Anti Viren System. Wird die betroffene Datei als kompromittiert erkannt, schlägt eine Öffnen dieser Datei somit mit einer entsprechenden Fehlermeldung fehl.

Das Ablegen und Speichern von Dateien auf dem Medium erzwingt das Verschlüsseln dieser Dateien. Ein write auf den SAMBA Share im Hostsystem wird im OsecFS erkannt und stößt damit einen Verschlüsselungprozess an. Die aktuell verwendete Technologie dazu ist Truecrypt[6], es können aber auch andere Anbieter oder Technologien eingesetzt werden.

Je nach eingesetzter Verschlüsselungstechnik kann in Folge der Datenträger auch von einem nicht Open Security System erkannt und geöffnet werden.

4 Sanfte Migration

Das Open Security Projekt zielt auf die Verwendung in der öffentlichen Verwaltung ab. Dabei sind diese Eckpunkte für einen Erfolg gegeben:

- Großflächiger Einsatz. Die Anzahl der Zielsysteme für eine Installation ist hoch (> 1000). Ein Rollout in einer derartigen IT Landschaft kann nicht autonom vom einzelnen Anwender selbst angestoßen werden, sondern muss über zentrale Dienste und organisatorische Einheiten erfolgen.

- Heterogene Systeme. Durch die gegebene Einkaufspolitik in einem Unternehmen oder einer Organisation dieser Größenordnungen sind selbst innerhalb eines Teilbaumes der Gesamtorganisation unterschiedlichste Systeme und Konfigurationen anzutreffen. Es ist nicht zweckmäßig weitreichende und detaillierte Anforderungen an die Zielsysteme durchzusetzen um ein optimales Funktionieren der eingesetzten Lösung garantieren zu können. Vielmehr ist es Aufgabe von Open Security sich an die Gegebenheiten anzupassen und die eigenen Anforderungen zu minimieren.

- Parallelbetrieb. Der Einsatz und die Integration dieser Security Lösung erfolgt am "offenen Herzen". Bereits eingesetzte Systeme, welche durch Open Security nicht ersetzt oder abgelöst werden, dürfen durch den Einsatz von Open Security nicht berührt werden. Die Sicherheitsmaßnahmen, welche durch Open Security eingeführt werden, gelten zusätzlich und lösen nur Teilaspekte im operativen Tagesgeschäft. Officeanwendungen, ERP/CRM oder beispielsweise domänenspezifische Applikationen laufen ohne Änderungen neben Open Security am gleichen System weiter.

- Know-How Anforderung. Open Security richtet sich an alle Anwender und nicht an eigens geschulte IT-affine Mitarbeiter. Die entwickelte Lösung bettet sich daher in das gewohnte Erscheinungsbild des Systems ein schafft durch die Verwendung bereits bekannter Elemente eine hohe Akzeptanz (bsp. Anstoßen von Open Security Funktionalitäten über eine System-Tray Applikation). Daneben erfüllt die Integration ihre Aufgaben unaufdringlich im Hintergrund und modifiziert damit das Wahrnehmungsbild des Anwenders über das System kaum.

[6] http://www.truecrypt.org/

Diese Technologie kann neben dem sichern Surfen im Internet und die sichere Verwaltung von Daten auf externen Datenträgern auch auf weitere Anwendungsfälle ausgedehnt werden. Die zentrale Frage ist dabei lediglich, ob die Zielapplikation in eine SVM migriert werden kann oder nicht.

Da das Open Security Projekt auf rein quelloffener Software besteht, fußen die verwendeten Technologien zum großen Teil aus Konzepten und Möglichkeiten aus dem Linux Umfeld (bsp. SAMBA, FUSE). SVMs sind in Folge daher Linux Snapshots, welche mit entsprechender Software und Rechtekonfigurationen versehen wurden.

Werden nun andere Anwendungsfälle auf Open Security migriert, so ist daher ein entsprechender Ersatz auf Linux Basis oder zumindest auf einer Windows ähnlichen Schicht (bsp. Wine) vorausgesetzt. Existent dabei sind jedenfalls PDF Reader, Officesuite, Instant Messaging, Skype und Bildverarbeitung. All diese Anwendungen können Schritt für Schritt automatisch durch entsprechende Updates der SVMs aus einem Repository eingepflegt werden und in ihren jeweilig sicheren SVM Instanzen zur Ausführung gebracht werden.

Durch den Parallelbetrieb von eingeschlossenen Linux Systemen sowie von proprietären Windowslösungen am gleichen System können die Vorteile beider Welten genutzt werden, ohne dass der Anwender sein gewohntes Umfeld verlassen muss.

Ein Seiteneffekt dieses Migrationspfades ist daher auch die Lösung von unmittelbaren Abhängigkeiten proprietärer Software. Läßt sich eine Virtualsierungstechnik wie VirtualBox oder VMWare installieren dann kann prinzipiell jedes Hostsystem gewählt werden und dennoch stehen die gewohnten Applikationen in einer sicheren Umgebung zur Verfügung. Mehr noch: da die einzelnen SVMs voneinander unabhängig sind und über Repositories Updates erfahren, können diese umfassende System- und Anwendungsupdates erhalten ohne die restlichen Komponenten des Gesamtsystems zu berühren. Portable SVMs lassen sich auch von einer Maschine zur nächsten transferieren und erfüllen dann in einem physisch völlig anderen Umfeld dennoch die gleiche Funktionalität.