OpenSecurity
@ OPEN COMMONS_KONGRESS 2014

OpenSecurity
open source solution for public institutions

OpenSecurity

Open Source Sicherheitslösungen schützen Angestellte und Daten in öffentlichen Institutionen

Das Projekt – Das Produkt

Nikolaus Dürk, MAS
X-Net Services GmbH

OpenSecurity – Das Projekt

OpenSecurity
open source solution for public institutions

- KIRAS PL2 4. Call
- November 2012 – Oktober 2014
- Sechs Partner:

Firma / Organisation	Partnerrolle
AIT Austrian Institute of Technology GbmH	Koordinator und Forschungspartner
IKARUS Security Software GmbH	Unternehmenspartner
X-Net Services GmbH	Unternehmenspartner
Linzer Institut für qualitative Analysen	GSK Partner
IKT Linz Infrastruktur GmbH	Bedarfsträger
Bundesministerium für Landesverteidigung und Sport	Bedarfsträger

OpenSecurity – Das Projekt

OpenSecurity
open source solution for public institutions

- Internet (Mail, Web)
- Datenträger (USB Devices)

- Internet (Mail, Web)
- Datenträger (USB Devices)

OpenSecurity – Das Projekt

OpenSecurity
open source solution for public institutions

- OpenSecurity soll den Verlust und (un-)gewollten Missbrauch von sensiblen, bürgerbezogenen Daten bei öffentlichen Einrichtungen verhindern.
- OpenSecurity setzt „Security by Isolation“ Prinzipien ein: durch eine Sicherheitsschicht in einer unabhängigen virtuellen Maschine (die Security Virtual Machine, oder SVM), die über MS Windows läuft.
- Diese Schicht kontrolliert, verifiziert und verschlüsselt jegliche Kommunikation, die auf USB-Geräten stattfindet. Sie ermöglicht auch sicheres, isoliertes Web-Browsing.
- OpenSecurity wird unter eine Open Source Lizenz gestellt. (Ausnahme: optionale IKARUS Komponenten)

OpenSecurity – Das Produkt

OpenSecurity
open source solution for public institutions

Wichtige Use Cases:

- Secure USB
- Secure Web Browsing
- Zentralisiertes Viren-Scanning

OpenSecurity – Das Produkt

OpenSecurity
open source solution for public institutions

Secure USB:

- 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.

OpenSecurity – Das Produkt

OpenSecurity
open source solution for public institutions

Secure USB:

- Windows hat standardgemäß ein hohes Trust-Level für USB Geräte. Das macht diese zu gefährlichen Malware-Überträgern.
  - Z.B. wurde die StuxNet Malware über USB transportiert
- OpenSecurity entschärft dieses Risiko, indem es USB Geräten nur über eine isolierte Virtual Machine Zugang gewährt. Dadurch kann keine schädliche USB Aktivität (z.B. Rootkit Installierung) den echten Host angreifen.
- Zusätzlich werden alle eingehenden Files auf Viren oder Malware überprüft (lokal oder zentral).

OpenSecurity – Das Produkt

OpenSecurity
open source solution for public institutions

Secure USB:

- Neben der Gefahr Malware Überträger zu sein, können USB Geräte (da klein und transportierbar) leicht verloren gehen.
- OpenSecurity entschärft das Problem, indem es die Verschlüsselung von Files, die auf USB Geräte kopiert werden erzwingt.
- Dadurch bleibt die Information gesichert, selbst wenn ein Gerät verloren geht (oder gestohlen wird).

OpenSecurity – Das Produkt

OpenSecurity
open source solution for public institutions

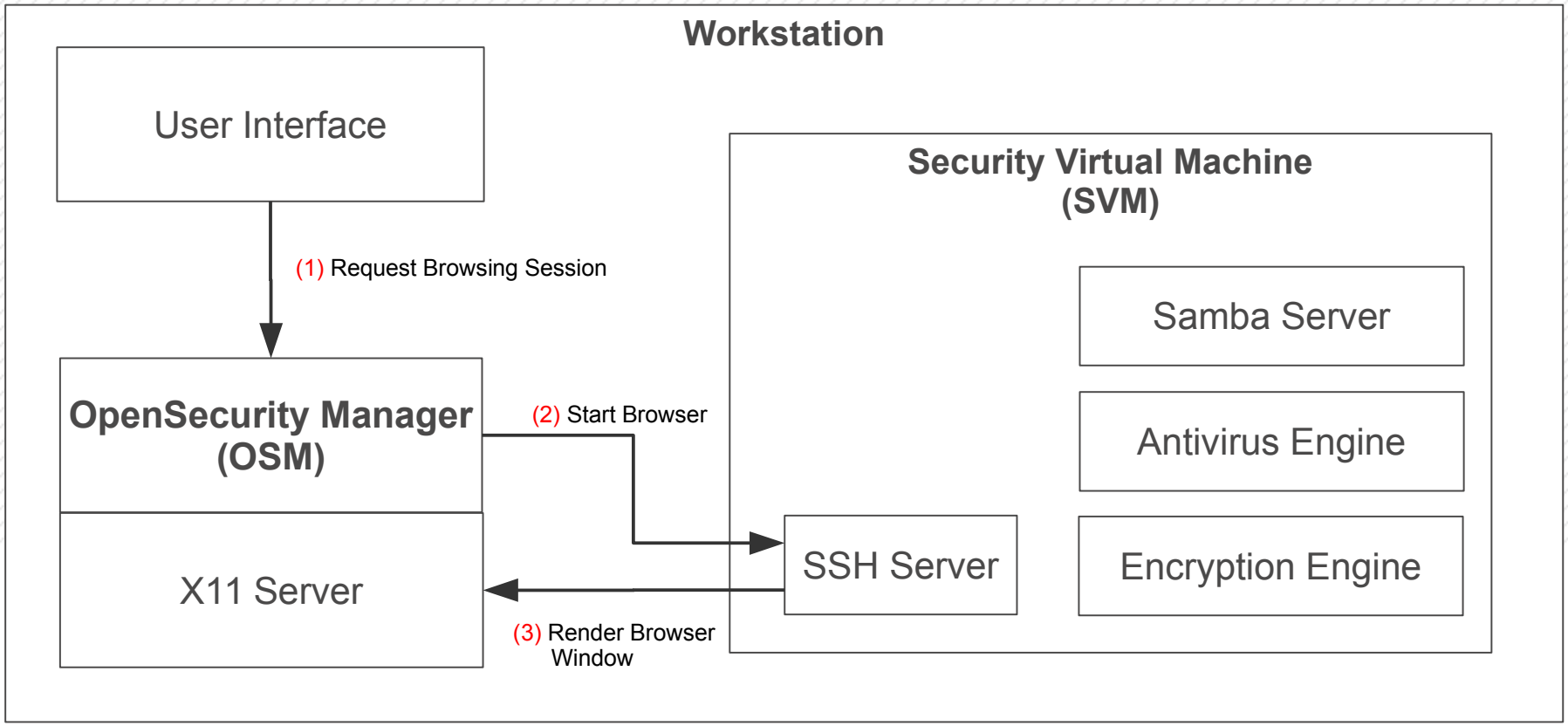
Secure Web Browsers:

- Web-Browser sind aufgrund von Phishing Attacken oder Exploits in Browser Code oder Plugins wie Java oder Flash eine zweite ernstzunehmende Malware Quelle.
- OpenSecurity entschärft diese Risiken, indem es Browser-Zugang nur über eine isolierte Virtual Machine zulässt.
- Wenn eine Browser-Sitzung geschlossen wird, wird die Virtual Machine komplett gelöscht.
- Dateien können über dasselbe sichere Protokoll übertragen werden, wie es vom OpenSecurity USB Mechanismus genutzt wird.

OpenSecurity – Das Produkt

OpenSecurity
open source solution for public institutions

Secure Web Browsing - Architektur



OpenSecurity – Das Produkt

OpenSecurity
open source solution for public institutions

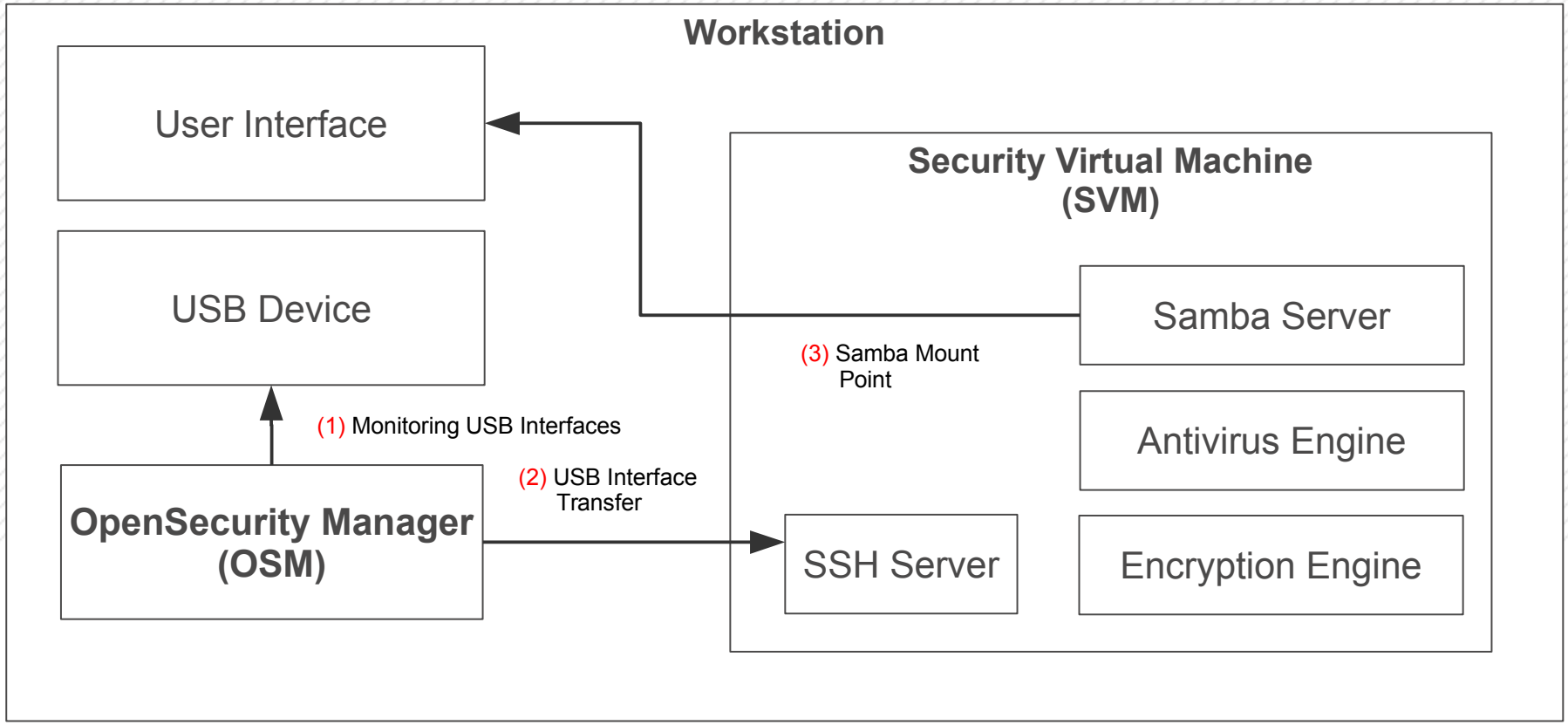
Zentralisiertes Viren-Scanning:

- In OpenSecurity werden neben reinen Klassifikationstechnologien auch IKARUS Serverapplikationen genutzt, die für den skalierbaren und hochperformanten Serverbereich entwickelt wurden.
- Für Institutionen ergeben sich mit dem Einsatz von zentralisierten OpenSecurity folgende Vorteile:
  1. Weniger Arbeitsaufwand durch die zentrale Verwaltung der Überprüfung von Geräten;
  2. Wenig Ressourcenaufwand am Endgerät selbst.

OpenSecurity – Das Produkt

OpenSecurity
open source solution for public institutions

Zentralisiertes Viren-Scanning - Architektur



OpenSecurity – Das Produkt

Deployment:

- OpenSecurity wurde für Windows 7 Clients entworfen und getestet.
- Das Installationspaket wurde für den zentral administrierten Masseneinsatz in Unternehmen zusammengestellt.

OpenSecurity – Mehr Information

Projekt Homepage:

http://www.opensecurity.at/

Support:

support@opensecurity.at