Masterarbeiten mit SOPHOS

Das FIM bietet in Kooperation mit der IT-Sicherheitsfirma SOPHOS (UK und Linz) mehrere Themen für Masterarbeiten an. Eine entsprechende finanzielle Dotierung für die Masterarbeiten ist vorgesehen. Weitere Themen sind in Vorbereitung.
Bei Interesse wenden Sie sich an Univ.-Doz. Gerhard Eschelbeck (ge *[at]* sophos.com) bzw. an Hr. Hörmanseder (rh *[at]* jku.at).

(File-Based) Encryption for Linux and Android

Goal:
Investigate the possibilities of transparent, file-based and full-disk encryption for Linux and Android.

Description:
Sophos is already working on a solution for file-based encryption for the MAC based on FUSE. FUSE and solutions as ENCFs based on FUSE are available also on Linux. These solutions typically provide an encrypted file system in user-space. This research shall investigate all the possibilities (user-space but if realizable also kernel-space) of file-based encryption for Linux. Furthermore, the possibilities of full-disk encryption shall be evaluated. The research shall also include Linux derivates as Android.

Possible Research Tasks:
- Investigate all the possibilities and solutions available for file-based encryption on Linux in user-space
- Investigate the technologies for full-disk encryption on Linux
- Investigate the solutions for encryption on Linux derivates as Android
- Work out an evaluation of all the found technical solutions based on typical customer use cases
- Develop first prototypical implementations using the most promising approaches

Example Links:
- EncFS Encrypted Filesystem - http://www.arg0.net/encfs
- Notes on the implementation of encryption in Android 3.0 - http://source.android.com/tech/encryption/android_crypto_implementation.html

Built-In Security on Android Devices (Trust Zone Architecture)

Goal:
Investigate the TrustZone Technology (Part of the state-of-the-art Android / ARM architecture) and how it can be in future used for security applications (e.g. encryption applications).

Description:
TrustZone enables a specialized, hardware-based form of system virtualization. TrustZone provides two zones: a “normal” zone and a “trust” or “secure” zone. TrustZone is a capability inherent in modern ARM applications processor cores, but at this time only a few SoCs using these cores fully enable TrustZone. This research shall investigate the possibilities of TrutsZone for security applications.

Possible Research Tasks:
- Work-in in the TrustZone architecture and its features
- Try-out TrustTone and the development for TrustZone with real devices (We are already in contact to Qualcomm and should be able to organize devices)

- Investigate the extended possibilities for security applications (e.g. encryption) using the TustZone architecture or better the TrustZone environment
- Prepare first prototypes for demonstration purpose

Example Links:

- http://www.arm.com/products/processors/technologies/trustzone.php
- http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf

Application Sandboxing on Android

Goal:

Investigate possibilities of providing secure, enterprise sandboxes on Android

Description:

Enterprise smartphones are more and more used for private purposes but also bring-your-own-device is gaining more and more acceptance. This raises the need to specially protect enterprise data on a smartphone. One approach to achieve this requirement is to provide special sandboxes for enterprise applications that are secured and isolated from the private, common environment. This research shall investigate the possibilities on Android for realizing such solutions.

Possible Research Tasks:

- Research possibilities on Android for providing such a secure environment and sandboxes
- Asses these possibilities in regards of their future readiness and usability (e.g. if solution uses some system low level functionality that is at this time accessible, but may be no more available in the future, this might be no feasible solution to implement)
- Prepare first prototypes for the identified possibilities

Agent-Based Data Discovery and Analysis

Goal:

Develop a concept for a solution (agent-based) that perform a constant analysis of all the data in an organization based on certain criteria and that can initiate specific actions (as encrypting files, educating the user,….)

Description:

Data Discovery is one of the main use cases for DLP applications to discover and monitor the location and flow of sensitive data and to educate end users and enforce controls to prevent loss of sensitive data. Data Discovery is also an important use case for Data Protection when it comes to initially encrypting large amount of data or when wanting to assure that data is encrypted according to the defined rules, as for example for compliance reasons. This research should work out a concept for a light-weight solution that assures that all the data is constantly analyzed in an organization and based on this analysis actions can be taken.

Possible Research Tasks:

- Investigate the main use cases for data discovery from a DLP point of view and Data Protection view
- Work out a general light-weight concept for a solution that constantly analysis the data in an organization (Idea is to have agents all over the organizations that analyze the data autonomously)
- Prepare first prototypes for the different platforms especially for server platforms (Linux, Windows, …)