



Research on IF-MAP

Ingo Bente (Trust@FHH)

15.04.2011, University of Frankfurt

ESUKOM

Introduction



Trust@FHH Research Group

- Team
 - Chair: Prof Dr. Josef von Helden
 - 3 research associates
 - 4 student assistants
- Research Fields
 - Trusted Computing
 - Network & Mobile Security
- Selected Projects
 - TNC@FHH
 - IRON
 - ESUKOM
- More Information
 - trust.inform.fh-hannover.de



The ESUKOM Project in a Nutshell

- Motivation
 - Smartphones are used in business environments
 - Impact of Smartphones in terms of IT-Security is unclear
 - Idea: Address **Smartphone Challenge** by leveraging IF-MAP
- Project Goals
 - Investigation of Smartphone platforms in terms of security
 - Development of IF-MAP prototype infrastructure
- Duration
 - 10/2010 – 09/2012 (2 years)
- Funding
 - Funded by german BMBF
- Website
 - www.esukom.de

SPONSORED BY THE

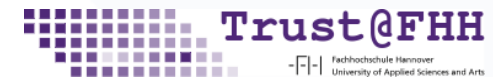


Federal Ministry
of Education
and Research

Project Consortium

- 3 SMEs & 2 Academic Institutions

- DECOIT GmbH
- mikado soft GmbH
- NCP Secure Communications
- Fraunhofer SIT
- Trust@FHH, FH Hannover



- Further Cooperations

- Infoblox, Juniper, Enterasys, Infineon
- PhD Programme with Universität der Bundeswehr München



Why using IF-MAP anyway?



ESUKOM Problem Statement

- How to secure smartphones in business environments?
- What we knew in advance
 - (Some) characteristics of smartphones
 - Smartphones are not properly addressed today ...
 - ... but existing security tools are deployed
 - Our technological background (TC, TNC, IF-MAP)
- What we did **not** know
 - How do smartphones change attack surface?
 - What aspects of smartphones are important in terms of security?
 - What (existing/new) means are appropriate to secure smartphones?

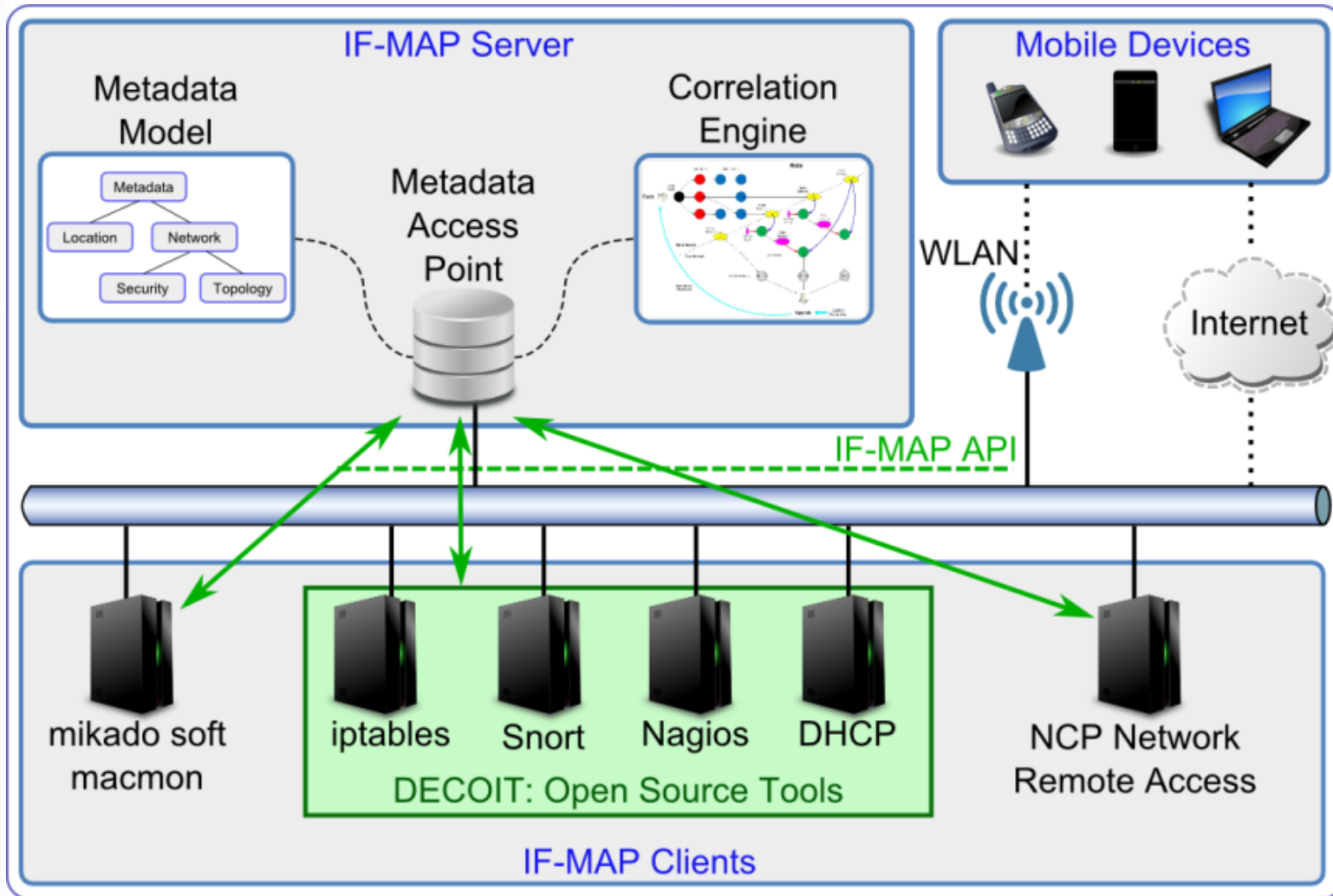


ESUKOM Idea

- Idea
 - Leverage existing tools to secure smartphone usage
 - Follow network oriented approach
 - Correlate (smartphone) metadata from arbitrary sources
 - No system security
- Why IF-MAP?
 - General purpose, content based pub/sub protocol
 - Integration of existing security solutions
 - Good experiences from adoption (IRON project)
 - Exciting new technology



ESUKOM High Level Architecture



The Field of Mobile Phone Security



Mobile Phone Security Research

- Research questions
 - Threats introduced by smartphones?
 - Limitations and flaws of current platforms?
- Research field is gaining momentum
 - Focus on Android and iOS
 - Mostly exploits & system security approaches
 - For example Taintdroid, Kirin & Saint (Enck et al. 2009 & 2010, PSU)



Smartphone Threat Analysis for ESUKOM

- Goal
 - Threat model for smartphones used in corporate environments
 - Smartphones == mobile consumer electronic devices
- Smartphone Characteristics
 - Built-in Sensors
 - Connectivity
 - Internet-support
 - Resource Paradox
 - App-based Architectures
 - Platform Diversity



Smartphone Threat Analysis for ESUKOM

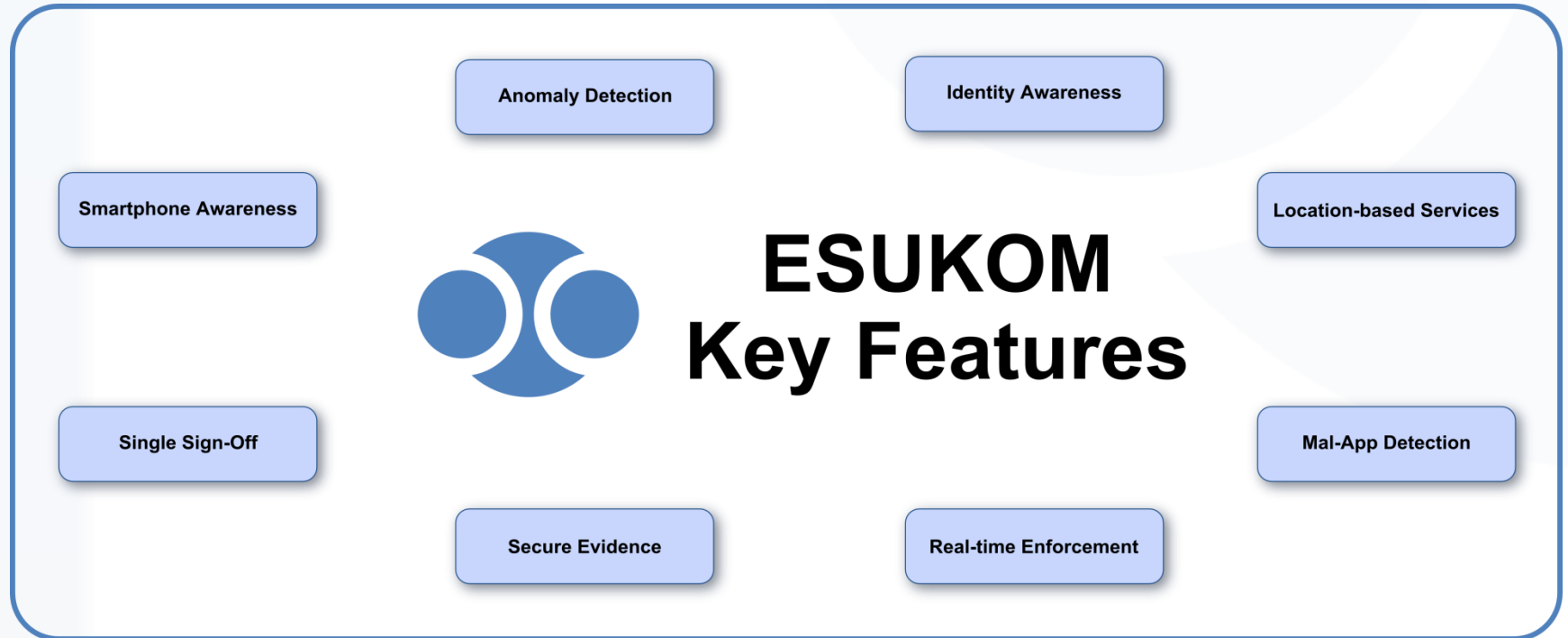
Target of Attack	Physical Environment	Smartphone	IT-Infrastructure
Exemplary Attacks	<ul style="list-style-type: none">Sensory Mal-AppsInsider Sensor Sniffing	<ul style="list-style-type: none">Resource Exhaustion Mal-AppsTrojan SMS/MMS SpammingLocal Data Sniffing Mal-AppsBotnet Mal-AppsPhysical Loss / Theft	<ul style="list-style-type: none">Smartphone Mounted Data TheftSmartphone Mounted Profiling



ESUKOM Key Features



ESUKOM Key Features



Open (Research) Questions

- Effective correlation of large metadata graphs
 - What are suitable correlation approaches?
 - What part of metadata graph is relevant for what purpose?
- Smartphone specific metadata vocabularies
 - Status of sensors
 - Location
 - Platform Details (installed apps, used permissions)
- Interdomain MAP
 - MAP-Server to MAP-Server Communication
- Threats introduced by IF-MAP?
 - Impact of rouge MAPCs
 - Trustworthiness of metadata graph





Thank You
Questions ?

ESUKOM

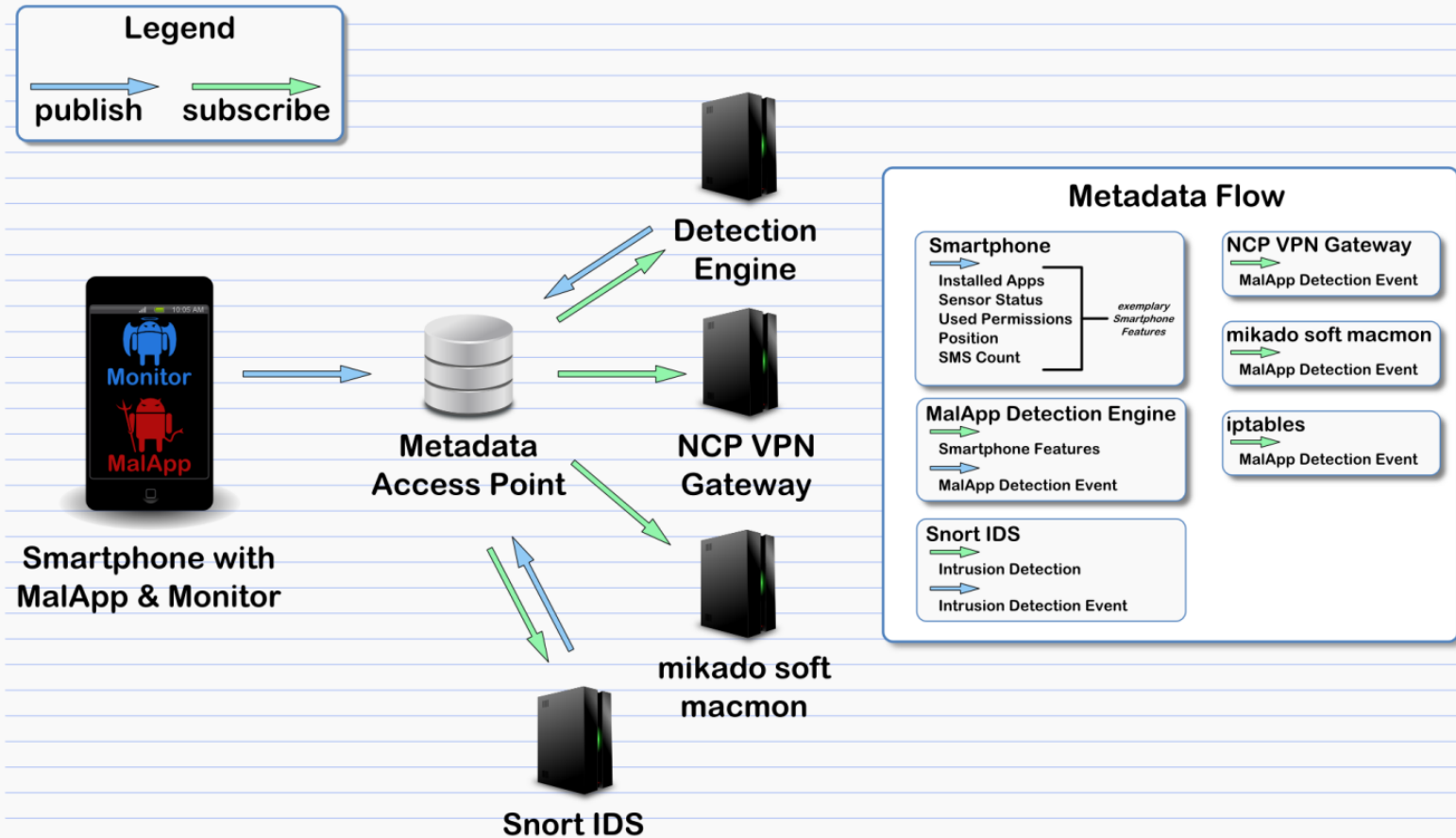
Backup Slides



ESUKOM Key Feature MalApp Detection

ESUKOM Key Feature

MalApp Detection



www.esukom.de

info@esukom.de

Live Demo



IF-MAP Demo

- MAP Server
 - ironD 0.2.1
- MAP Clients
 - soapUI (triggers IF-MAP operations)
 - ironGUI 0.1.0 (visualization)
- Software available at
 - <http://trust.inform.fh-hannover.de>
 - www.soapui.org
 - Licenses: Apache License 2 & LGPL 2.1



Copyright 2011

Das dem Projekt zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen „01BY1050“ gefördert. Die Verantwortung für den Inhalt liegt bei den Autoren.

*Die in dieser Publikation enthaltenen Informationen stehen im Eigentum der folgenden Projektpartner des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projektes „**ESUKOM**“: DECOIT GmbH, Fachhochschule Hannover (FHH), Fraunhofer-Institut für Sichere Informationstechnologie (SIT), NCP engineering GmbH und der mikado soft GmbH. Für in diesem Dokument enthaltenen Information wird keine Garantie oder Gewährleistung dafür übernommen, dass die Informationen für einen bestimmten Zweck geeignet sind. Die genannten Projektpartner übernehmen keinerlei Haftung für Schäden jedweder Art, dies beinhaltet, ist jedoch nicht begrenzt auf direkte, indirekte, konkrete oder Folgeschäden, die aus dem Gebrauch dieser Materialien entstehen können und soweit dies nach anwendbarem Recht möglich ist.*

