IFIP World Computer Congress (WCC2010)

Leveraging Trusted Network Connect for Secure Connection of Mobile Devices to Corporate Networks

VOGUE

Prof. Dr.-Ing. Kai-Oliver Detken

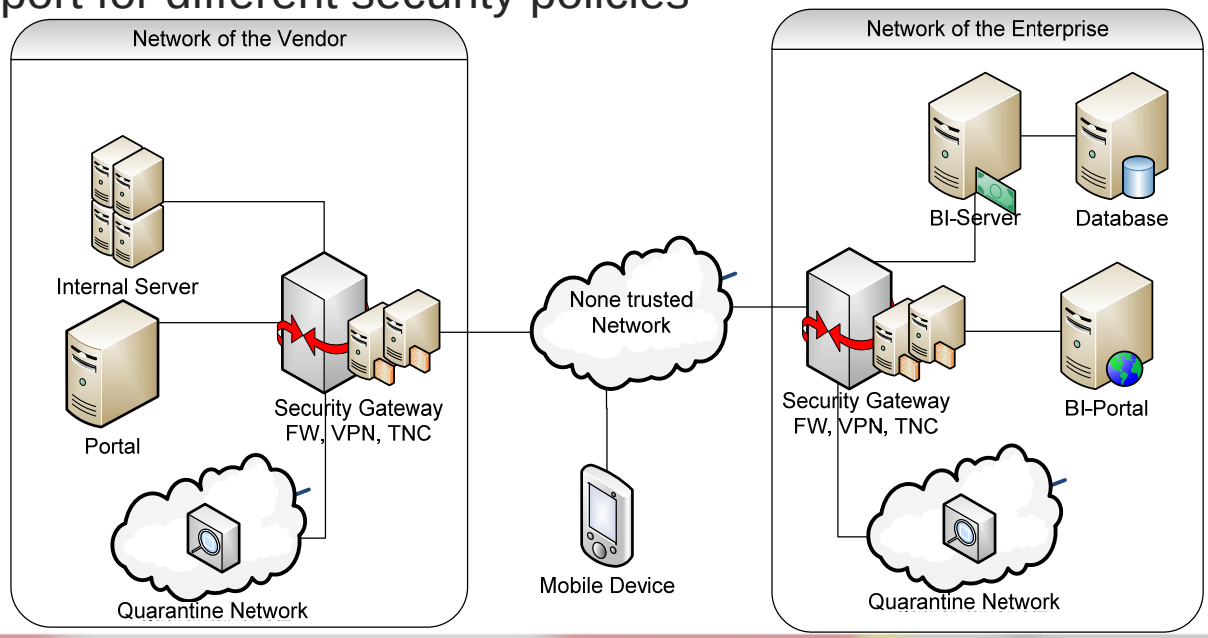
DECOIT GmbH, http://www.decoit.de, detken@decoit.de

Table of Contents

VOGUE

Motivation and Background

- Using of mobile devices in two different networks with separate policies (generic scenario of VOGUE)
  - No security check currently
  - No hardware control available
  - No support for different security policies



Security risks and challenges

- Endpoint misconfiguration
  - Configuration failures in security systems like firewalls, VPN Gateways etc.
  - Vulnerable mobile devices
- Open and overall nature of mobile endpoints
  - Access and manage of critical business data
  - No integrity check of the hardware is possible
  - Growing malware market for smartphones
  - Using of mobile devices in unsecure networks

VOGUE

Security requirements

- Backward compatibility and scalability
- Enterprise`s network security policy should be reliably enforced
- Isolation and automatic remediation
- Endpoints platform authentication
- Support of federation of trust
- Usability

VOGUE

Trusted Network Connect (TNC)

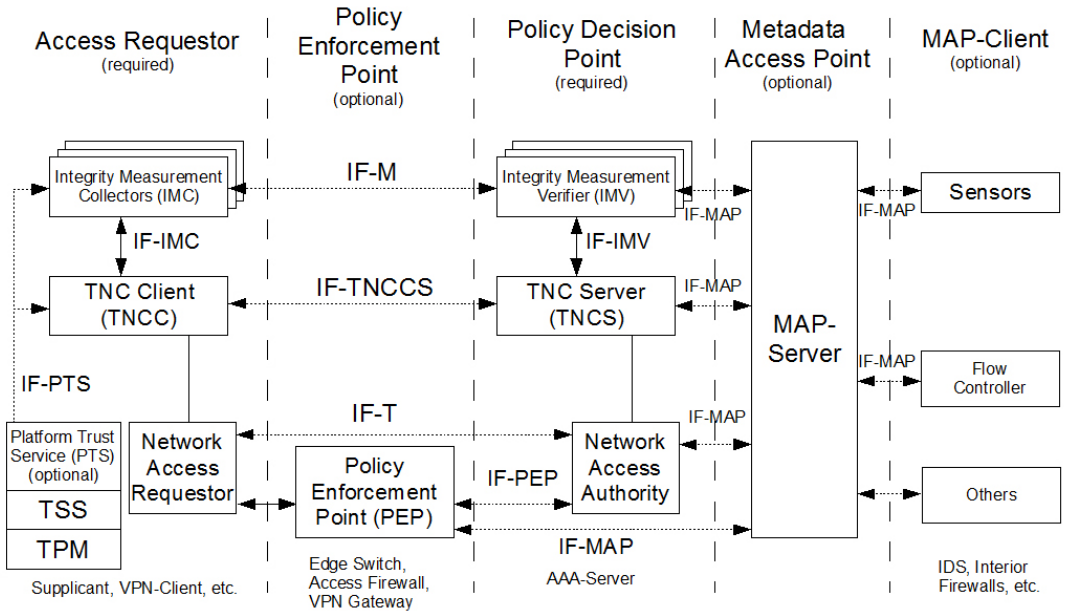
- TNC is an open architecture for Network Access Control (NAC), promulgated by the Trusted Network Connect Working Group (TNC-WG) of the Trusted Computing Group (TCG)
- It aims to enable network operators to provide endpoint integrity at every network connection, thus enable interoperability among multi-vendor network endpoints
- Trusted Computing encompasses six key technology concepts
  - Endorsement key
  - Secure input and output
  - Memory curtaining / protected execution
  - Sealed storage
  - Remote attestation
  - Trusted Third Party (TTP)
- The objective is to get an open and vendor-independent specification for checking the endpoint integrity of third party equipment
- TNC uses available technologies like
  - Network access: 802.1x, VPN, PPP
  - Data transport: EAP, TLS & HTTPS
  - Authentication: Radius Server, Diameter

TRUSTED COMPUTING GROUP™

VOGUE

Architecture of TNC

- Integrity Check: Measurement of the system status (assessment phase)
- Isolation: Check of the security policy (isolation phase)
- Remediation: Reintegration after recover of integrity (remidiation phase)
- Extension of the integrity check is possible (e.g. binding of access data to mobile device)



TNC Architecture for Interoperability Version 1.4, Revision 4

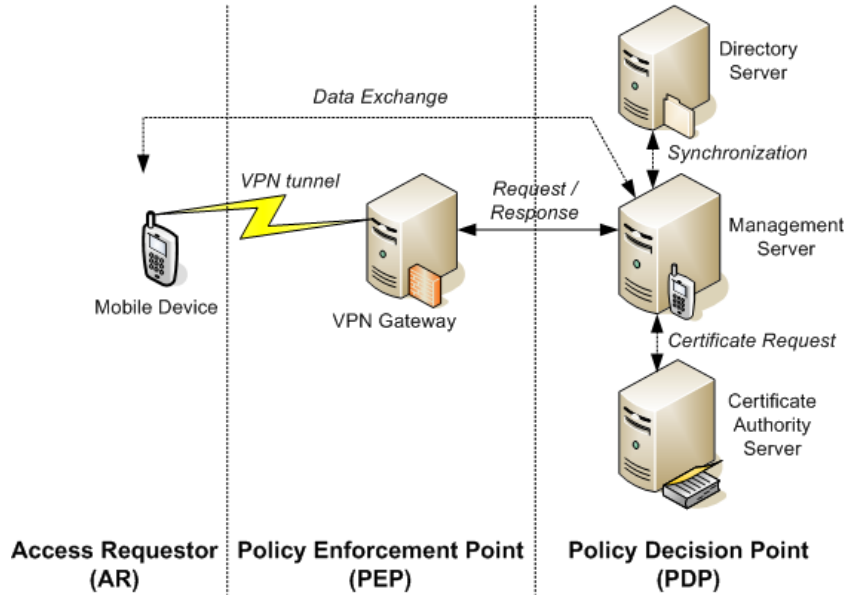
The VOGUE project

- Founded by the Federal Ministry of Education and Research (BMBF) of Germany (URL: http://www.vogue-project.de)
- VOGUE started in October 2009 and will end at September 2011
- Partners of the project are:
  - DECOIT GmbH (leader of the project)
  - Fraunhofer SIT
  - Mobile Research Center (MRC)
  - NCP engineering GmbH
  - OTARIS
- The targets of the VOGUE project are:
  - Tapped/tapping into the emerging market of TPM based solutions within the mobile area for the industry in Germany
  - Developing a basis for trials of TPM-based solutions while using an emulator that enables small and medium sized businesses to enter into this new business field
  - Facilitate security relevant and mobile business processes by establishing a trustworthy platform for mobile end-devices. This will, for example, prevent possible attacks and/or reduce the damage that may occur through attacks
  - Demonstration on the basis of a distributed platform for mobile end-devices

VOGUE

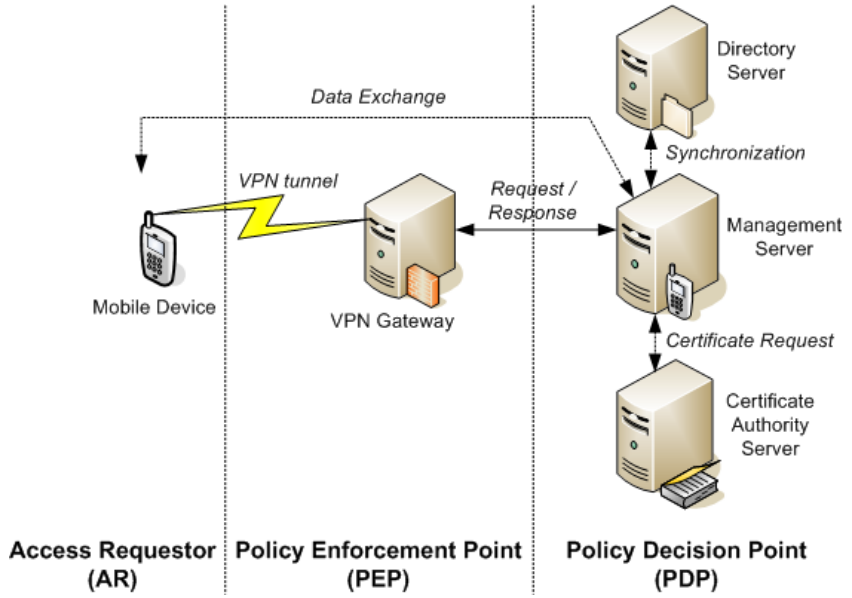
The VOGUE approach (1)

- Mobile OS systems like Android permits application development (open platform)
- Root-of-trust implementation via Mobile Trusted Module (MTM)
- MTM/TPM software emulation has been developed



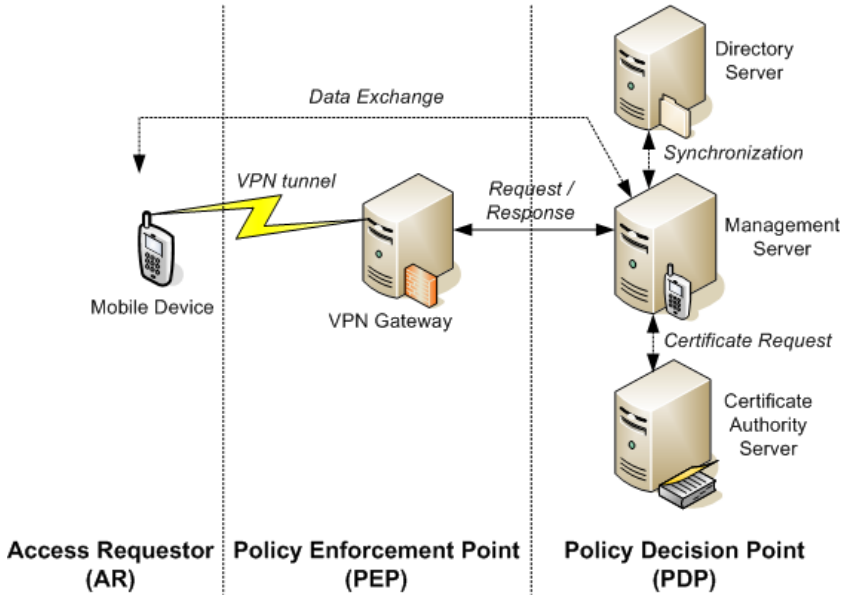
The VOGUE approach (2)

- Core elements of VOGUE are:
  - VPN Gateway
  - Management Server (e.g. RADIUS, TNC-Server)
  - Directory Server (e.g. LDAP)
  - CA-Server
  - TPM/MTM
  - TNC-Client on Android



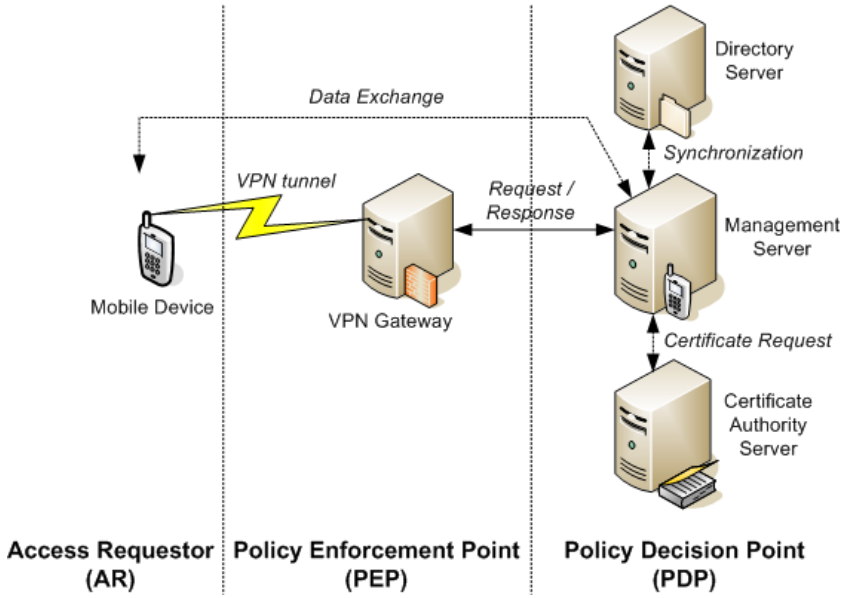
VOGUE`s mechanisms (1)

- Each user group has different security policies for different access rights
- The management system synchronizes continuously in intervals the user information with the directory server
- That includes that user from the directory server with VPN access rights, if they are not yet available on the management server, will synchronize with all user group membership automatically after one interval
- As an option a public certification authority (CA) can be adapted
- If a new user is created on the management server, a certificate will apply
- The management server platform is then a registration authority
- The VPN gateway has to be configured that all requested clients will be authenticate via the management server
- Therefore, the gateway site does not need adaptations for new user. That will be done automatically by the communication with the management server



VOGUE`s mechanisms (2)

- Next to the authentication of the user, the smartphone platform (hardware and software configuration) is checked according to the enterprise TNC's requirements
- After the establishment of a VPN connection, the network access of the mobile device is limited to the quarantine zone
- Within this area, it is only possible to update software components of the mobile device like anti-virus-software or operating system patches
- The access to other network areas of an enterprise network is forbidden
- Information about the status of the mobile device is available by the access requestor (AR) on the client-site
- The AR includes
  - Network Requestor (as a component of the VPN client)
  - TNC client (as an interface between the network access requestor and plug-in software)
  - Integrity Measurement Collector (describes the plug-ins which allows different software products like antivirus software to communicate with TNC)



The VOGUE approach (3)

- Summarized the following points will be initiate for a mobile device communication:
  - A VPN connection is established
  - The management server (TNC server) initializes an integrity check
  - The mobile device (TNC client) collects Integrity Measurements (IM) information using the local Integrity Measurement Clients (IMC) on the mobile device
  - The management server (TNC server) forwards the IM information for a check to the Integrity Measurement Verifier (IMV)
  - The Integrity Measurement Verifier (IMV) checks the IMs and sends the results with a recommendation to the management server (TNC server)
  - The management server (TNC server) takes access decision und forward this information to the VPN gateway (PEP) and the mobile device (AR)
  - The VPN gateway (PEP) allows or does not allow the access to the network for the mobile device (AR)

VOGUE

Project status of VOGUE

- The definition of the requirements and mobile scenarios have been finished
- The analyze of mobile operating system platforms like Android is on work
- The development of emulators for the use of TPM or MTM mechanisms have been finished, but have to be further develop if Android version 3.0 is available
- Actually different modules (OpenVPN, Funambol, FreeRADIUS, LDAP, libtnc) are testing for the platform
- The definition of the architecture of VOGUE has been finished
- The software platform will be specify in detail currently
- A first demonstrator will be available at the end of the year

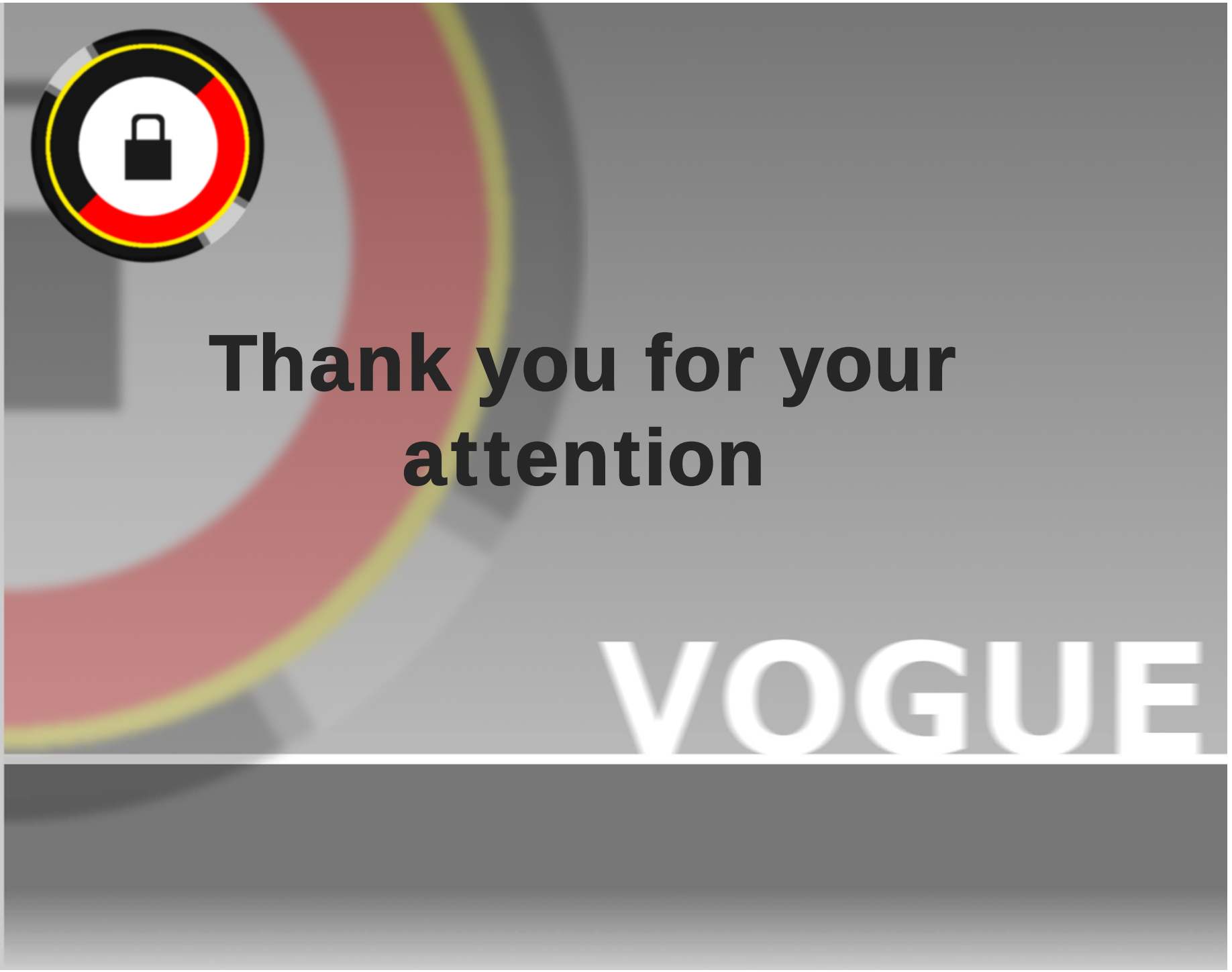
VOGUE

Conclusions

- The TNC approach within VOGUE is a viable solution to raise the security level in mobile networks
- Though the core specifications are already accomplished and various network components are available on the market, there are still shortcomings and manufacturers differ in their approaches
- Similar implementations are available: with Microsoft‘s “Statement-of-Health Protocol” future interoperability can be reached, but Cisco Systems will go its own way and will not be interoperable with the standard
- Further research projects have also interesting solutions like SIMOIT or TNC@FHH based on trusted computing approach
- The VOGUE project will improve existing TNC approaches with own developed TNC clients for mobile operating systems (e.g. Android) in order to extend the applicability beyond laptops or notebooks, since smartphones are widely used in corporate networks
- With this work, it is hoped, that the integration of smartphones for “Trusted Computing” will bring the TCG initiative one step further in the development and standardization process

VOGUE

Thank you for your attention



Copyright 2010

The project VOGUE (http://www.vogue-project.de) is funded by the Federal Ministry of Education and Research (BMBF) of Germany. The project started in October 2009 and will end at September 2011. The authors would like to thank the BMBF for their support. We also wish to express our gratitude and appreciation to all VOGUE partners for their strong support and valuable contribution during the various activities presented in this paper.

VOGUE