NCP
SECURE COMMUNICATIONS

Technical Paper
high security remote access

Automated Mobile Security (ESUKOM)

Leveraging Trusted Network Connect (TNC) IF-MAP to provide automated security for company networks and mobile devices

Network
Communications
Products engineering

USA:
NCP engineering, Inc.
444 Castro Street, Suite 711
Mountain View, CA 94041
Tel.: +1 (650) 316-6273
Fax: +1 (650) 251-4155

Germany:
NCP engineering GmbH
Dombuehler Str. 2
D-90449 Nuremberg
Tel.: +49 (911) 9968-0
Fax: +49 (911) 9968-299

Internet
http://www.ncp-e.com

Email
info@ncp-e.com

Support
NCP offers support for all international users by means of Fax and Email.

Email Addresses

helpdesk@ncp-e.com	(English)
support@ncp-e.com	(German)

Fax

+1 (650) 251-4155	(USA)
+49 (911) 9968-458	(Europe)

When submitting a support request, please include the following information:

- exact product name
- serial number
- version number
- an accurate description of your problem
- any error message(s)

Copyright
While considerable care has been taken in the preparation and publication of this manual, errors in content, typo-graphical or otherwise, may occur. If you have any comments or recommendations concerning the accuracy, then please contact NCP. NCP makes no representations or warranties with respect to the contents or use of this manual, and explicitly disclaims all expressed or implied warranties of merchantability or suitability of use for any particular purpose.
Furthermore, NCP reserves the right to revise this publication and to make amendments to the contents, at any time, without obligation to notify any person or entity of such revisions or changes. This manual is the sole property of NCP and may not be copied for resale, commercial distribution or translated to another language without the express written permission of NCP engineering GmbH.
All trademarks or registered trademarks appearing in this manual belong to their respective owners.

© 2011 NCP engineering GmbH, All rights reserved.

1. INTRODUCTION

The increasing use of mobile devices like smartphones and tablet PCs introduce new threats to enterprise IT networks. While most of the well known security programs such as desktop firewalls, antivirus and harddrive encryption work pretty well for laptops, they are still not available for these kinds of mobile devices. The only way to keep your network secure is by providing additional security on the central IT infrastructure.

The problem is, most of today's security systems work isolated from each other and if they offer interoperability they do so only to a limited extent, which is insufficient to counter the new threats network security faces every day. A new specification developed by the Trusted Computing Group (TCG) strives to solve this interoperability problem with the development of IF-MAP. IF-MAP provides the possibility to interconnect different IT-security systems and provide an accurate representation of the health status of your IT network. It even can automate security responses to network threats and enforce security without the need for human interaction.

The support for IF-MAP is steadily increasing, as more and more vendors and open source products are supporting the IF-MAP technology.

2. WHAT IS IF-MAP ?

IF-MAP stands for **I**nter**F**ace for **M**etadata **A**ccess **P**oints. You can think of IF-MAP as a central database for your IT-systems where they can store information or retrieve information from to get a real-time representation of the status of your network.

There are three basic functionalities an IF-MAP enabled component can do:

- **Publish**: Clients can store information for other clients to see
- **Search**: Clients can search for published data using search patterns
- **Subscribe**: : Clients can receive notification when other clients publish new data

To store information in the MAP there are two different data types available: Identifiers and Metadata. Identifiers act as "root hub" for information stored in the IF-MAP. There are only 5 identifiers available: Identity, IP address, MAC address, Access Request and Device.

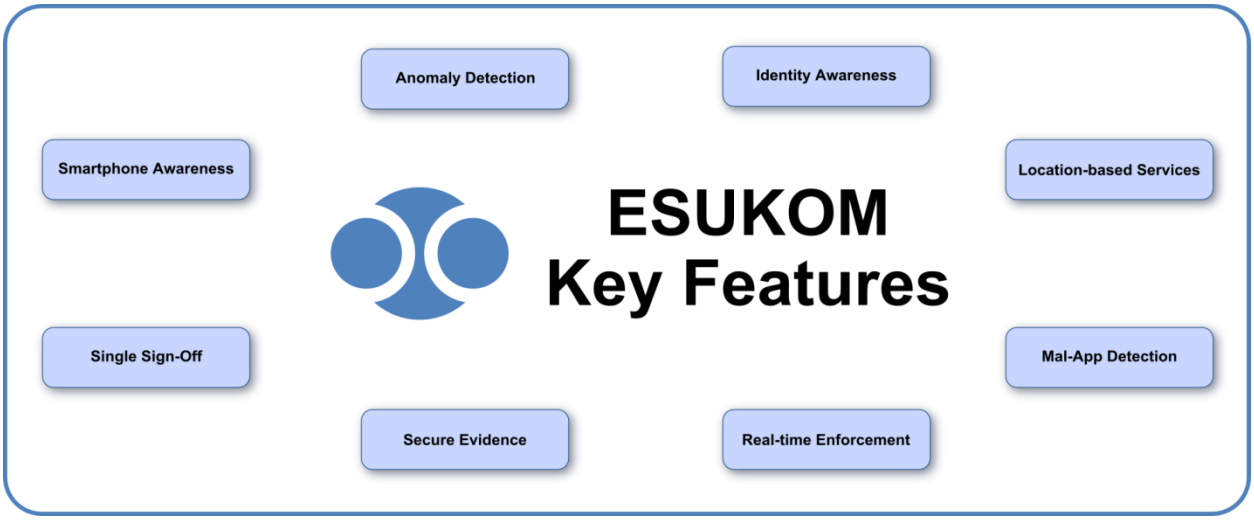
The other type of data is metadata, which has to be linked to at least one identifier but can also connect two identifiers.

Each client has to authenticate itself securely to the MAP Server either with username and password or certificate based authentication. All data is transmitted safely with SSL encryption.

3. WHAT IS ESUKOM ?

The ESUKOM research project aims at leveraging IF-MAP to provide security in mobile device environments. The project will bring IF-MAP support to several key open-source products like Snort (intrusion detection), IPtables (firewall), Nagios, FreeRADIUS and ISC DHCP server, to the products of two commercial vendors: NCP engineering (VPN software) and Mikado Soft (NAC solution) and provide an IF-MAP Android client. With this diversity of IF-MAP enabled components we try to provide example configurations for eight key features, which are the ultimate goal of this research project.

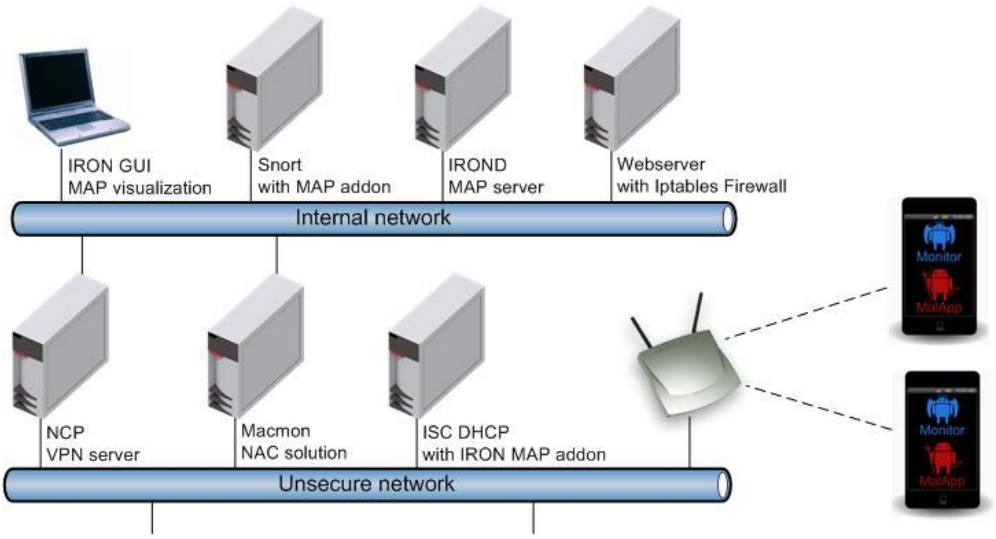
More information about this project can be found at http://www.esukom.de



4. REALTIME ENFORCEMENT USING IF-MAP

This example demo uses several of the ESUKOM developed IF-MAP compatible products. All open source products are available on www.esukom.de, the NCP VPN Server is still beta and not available on the web page, but can be made available for test environments by contacting tcg@ncp-e.com.

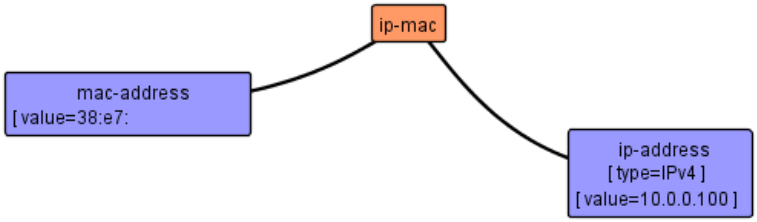
The following image shows a basic description of the network the demo uses:



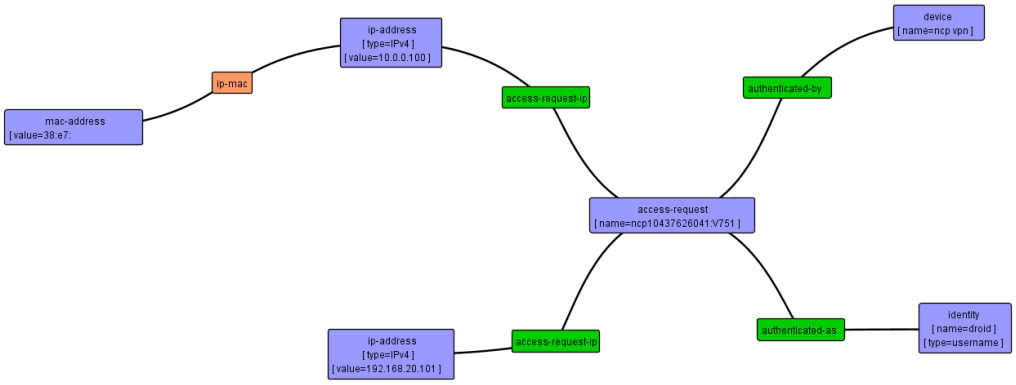
The network is separated into an unsecure network that can be accessed via WiFi and an internal network, which requires a VPN connection to gain access to. There is no direct access from the unsecure network to the internal network even though two components reside in both networks.

An Android device connects to the WiFi access point and receives a lease from an IF-MAP capable ISC DHCP Server. The IF-MAP Client will publish the lease information into the MAP database. The DHCP server has the information which MAC address is connected to which IP address.

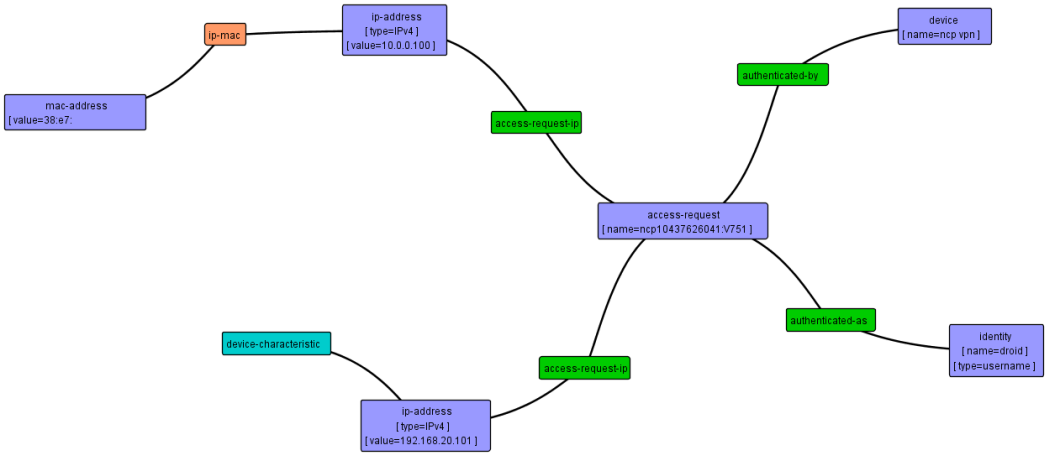
The IF-MAP graph will look like this after the information has been published:



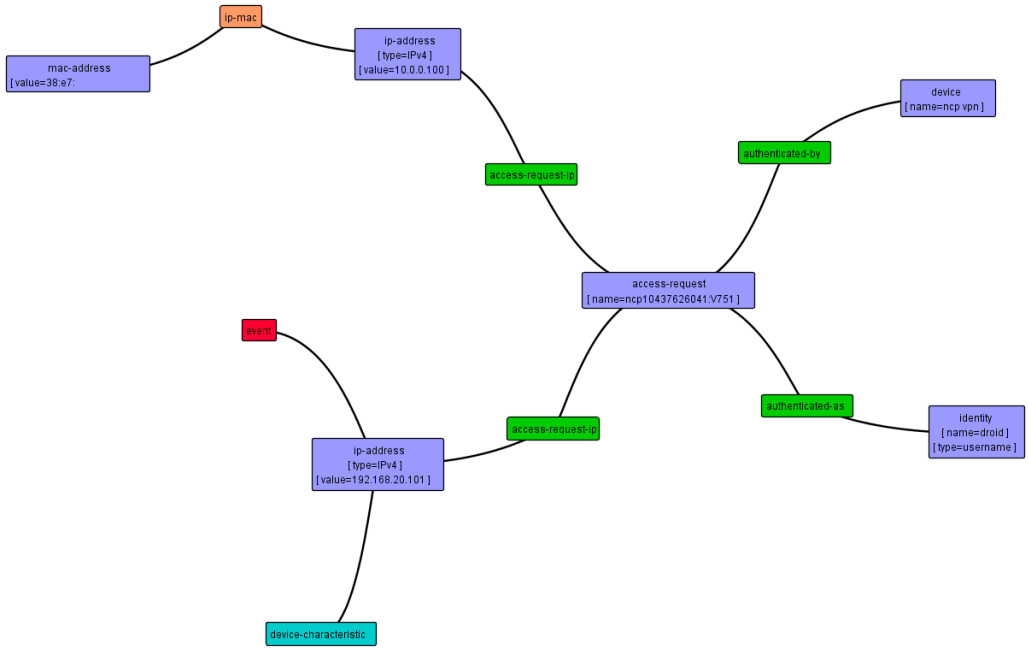
Now to gain access to the internal network the device has to establish a VPN connection. The VPN Server will publish information about the username used for the VPN connection, the device that has authenticated the request and what internal IP address the connection did receive and link that information to the already available information published by the DHCP server.



Now the IF-MAP app on the android phone is able to publish information about the device, for example the IMEI or if bluetooth is enabled. Optionally if a GPS signal is available the client can publish information about its current location.



Besides storing information the VPN Server is able to react on events published into the IF-MAP server by an intrusion detection system like snort.



The VPN Server offers two possible reactions to an event published: Quarantine or Disconnect a device. In this example graph the event is displayed to get a better understanding of the graph, in a productive environment it would be non-persistent, to keep the graph as clean is possible.

The VPN Server can react to a specific kind of event or it can react on a magnitude value each event is assigned. The magnitude has a potential spectrum of 0 to 100, where 100 is the most severe event. A less severe event could restrict the access to an important file server for example, while a critical event could disconnect the client and maybe even lock the account for further investigation by an administrator.