AUTOMATED MOBILE SECURITY (ESUKOM)

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

DEMONSTRATION OVERVIEW

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 hard drive 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. TNC IF-MAP provides the possibility to interconnect different IT-security systems and provide an accurate representation of the health status of your IT network

The ESUKOM research project aims at leveraging IF-MAP to provide automated security in mobile device environments without the need for human interaction. The project will bring IF-MAP support to several key open-source products like Snort (intrusion detection), Iptables (firewall) 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.

The demonstration will show data from all systems listed above being published to the MAP server and an automated security response by the NCP VPN solution and Iptables to different threats originating from a smartphone.