BYOD SOLUTIONS WELL IN HAND: STANDARDS-BASED MOBILE SECURITY

DEMONSTRATION OVERVIEW

BYOD security is a hot topic for the enterprise - end users want to work from their shiny new smartphones and tablets, and corporations desire the productivity gains and cost reductions associated with permitting them. But with greater flexibility comes increasing threat - mobile devices are at a higher risk of compromise than traditional desktop operating systems due to limited security software and exposure to web-based malware and malicious mobile applications. How do we ensure that these devices play well with others once we allow them on our networks?

TNC IF-MAP based interoperability for security automation enables a mobile security solution in which:

- A Pulse Secure Policy Secure policy server (TNC MAP Client) authorizes a BYOD device to connect to the network.
- A DECOmap Android client from DECOIT GmbH (TNC MAP Client) gathers data from the device and publishes it to the MAP service.
- A Snort intrusion prevention system, with TNC MAP Client functionality developed by DECOIT GmbH, monitors behavioral activity on the network.
- IF-MAP based security automation - coordinated by Trust@HsH's irond TNC MAP Server - enables the Snort IPS to signal the Pulse Secure policy server if the mobile device is out of compliance or misbehaving, so the policy server can isolate or restrict the mobile device.
- A Trust@HsH VisITMeta data visualizer (TNC MAP Client) enables a security administrator to investigate activity, and communications partners, of the offending mobile device.