

Mobile Device Security

Protecting the Edge of the Network

CTST 2009

Salvatore D'Agostino

IDmachines LLC

It's getting attention



What is a mobile device?

- Cell phone
 - NFC
 - Bluetooth
 - 802.11.x
 - 3G, 4G
- Laptop
- Rugged Devices
- Media Players
- Automobile, Aircraft
- Thumb Drives
- Smart Card



Attack Vector(s)

- Email
 - Attachments
- MMS
- SMS
- Could be anything on thumb drive...
- NIST SP-800-124

Device Identity, Another Take on Convergence

- Devices matters as much as individuals
- Need to be treated in a very similar manner
 - Enrollment
 - Registration
 - Issuance
 - Activation
 - Lifecycle Management

Can FIPS 201 address devices?

- Device certificates widely used
- Provides single method of authentication:
 - Doors
 - Desktops
 - Devices
 - Network gear
 - Desktops and Servers
 - Mobile devices
 - Programmable Logic Controllers
 - Smart Grid

Device Dilemma

- Need to manage device security
- Need to manage behavior of people that use it
 - Nearly half of people consider laptop their property
- Often don't have the expertise in the operating system (embedded)
- Roaming issue
- Now they can connect directly to the network
 - Not just the email server
- Many vendors

Mobile Device Applications and Solutions Expanding Rapidly

- Out of band authentication
 - One Time Passwords Delivered to the Phone
- Many vendors entering space
 - Verisign iPhone app
 - Battle.net mobile authenticator
 - Valimo
 - Payline
 - CORISECIO
 - Air France NFC boarding passes
 - A hundred more.....

Simple Things to Do

- Enable PINs and Passwords
 - Better if tied to x.509 digital certificate
- Enable hard reset and data wipe for lost devices
 - PIN lockout with CAC
- Lojack for phones
 - Ability to track lost devices
- Encrypt data
- http://csrc.nist.gov/publications/nistbul/Jan2009_Cell-Phones-and-PDAs.pdf