MOBILE NETWORK SECURITY

Kondia Kan, CISSP
Regional Product Manager, APAC
24th June 2011

AGENDA

1. MOBILE MARKET & TRENDS
2. THREATS TO MOBILE DEVICES, USERS & ASSETS
3. ADDRESSING TODAY'S MOBILE THREATS
4. SUMMARY

AGENDA

1. MOBILE MARKET & TRENDS
2. THREATS TO MOBILE DEVICES, USERS & ASSETS
3. ADDRESSING TODAY'S MOBILE THREATS
4. SUMMARY

THE MOBILE INTERNET IS THE NEW INTERNET

Proliferation of Devices

Number of smartphones sales to exceed PC sales in 2012*

Connected Socialization

Content Consumption

*Source: Morgan Stanley, 2010

TODAY'S MOBILE WORKFORCE

Unmanaged Devices

Diverse Users/Locations/ Networks

Critical Resources

How do you ensure devices are secure and ONLY the right users are accessing your resources?

SECURING CONNECTIVITY

Providing anyone a secure experience from any device from any location to any resource

AGENDA

1. MOBILE MARKET & TRENDS
2. THREATS TO MOBILE DEVICES, USERS & ASSETS
3. ADDRESSING TODAY'S MOBILE THREATS
4. SUMMARY

TODAY'S SHIFTING THREAT LANDSCAPE

The Sophisticated Cybercriminal

- Cybercriminals - from students to well paid organized professionals.
- APT's – Advanced Persistent Threats – Sophisticated and strategic efforts aimed at intelligence gathering and espionage

The Threat from Within

- Insiders with and without malicious intent
- The mobile device as "Trojan Horse"

SECURITY'S EVOLVING AND EXPANDING BATTLEFRONTS

The Decentralized Nature of Attacks

Inadequate security on mobile devices

Diverse user profiles

Device and OS proliferation

Increasing implementation points

THE MOBILE SECURITY GAP

40%
use their smartphone for both personal and business

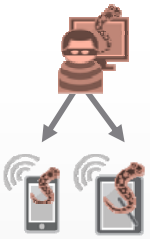
72%
share or access sensitive info such as banking, credit card, social security, medical records

80%
access their employer's network without permission – 59% do it everyday

50%+
are very concerned about loss, theft and identity theft resulting from their mobile usage

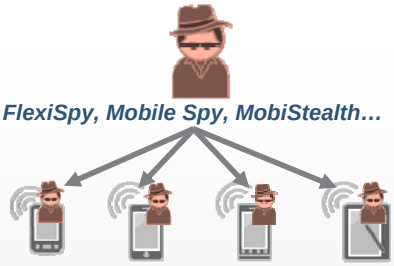
Sources: KRC Research and Juniper Mobile Threat Center

EVOLUTION OF MOBILE MALWARE



Criminals now using PC-style malware attacks to infect mobile devices

Greatest mobile malware risk comes from rapid proliferation of applications in app stores



Mobile spyware is prevalent and now commercialized

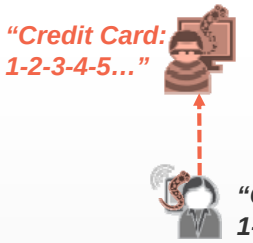
Between 2009 and 2010, reported increase in mobile threats of 250%*

*Information obtained from analysis of Junos Pulse Mobile Security Suite virus definition database dated 10/15/2010

FAST PROLIFERATING MOBILE MALWARE THREATS

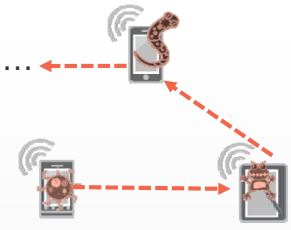
Trojans that send SMS messages to premium rate numbers

Background calling apps that rack up exorbitant long distance bills



Keylogging applications that compromise passwords and credit card or bank account numbers

Self-propagating code that infects devices and spreads to additional devices listed in a user's address book



Malware growing more sophisticated, now with polymorphic attacks

MOBILE DEVICE LOSS AND THEFT

A survey of consumer users found that one out of every three users lost their mobile device[1]

Approximately 2 million smartphones were stolen in the U.S. in 2008[2]

Over 56,000 mobile devices were left in the back seats of the city of London taxi cabs during 6 month period between 2008 and 2009

Over the 2010 holidays, in the U.K. alone, a total of 5,100 smartphones and 3,844 notebook computers were lost at 15 different airports[3]

In Paris, 75% of 991 violent crimes that took place in October 2010 happened because of mobile phone theft[4]

[1]*Information obtained from Junos Pulse Mobile Security Suite internal transaction logs;* [2]*Forrester Research;* [3]*Credant Technologies;* [4]*The Sydney Morning Herald, 12/10/10*

WHY IS MOBILE DEVICE LOSS AND THEFT AN ISSUE?

Bookmarked bank accounts with passwords set to auto-complete

Contacts with pictures and addresses tied to the contact

Pre-connected personal data compilation sites

Social media accounts

Calendar events

Personal photos

Pre-connected e-mail accounts

Sensitive corporate data and IP

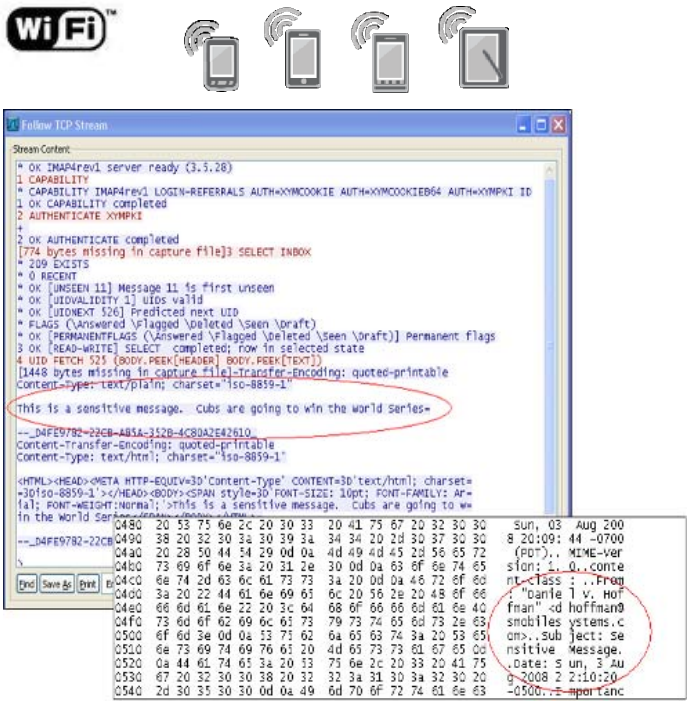
COMMUNICATION INTERCEPTION

Approximately 50% of all smartphones today are Wi-Fi capable[5]

Estimated 90% of all mobile devices will be Wi-Fi capable by 2014[5]

Risk of Wi-Fi sniffing and interception increases as number of Wi-Fi capable mobile devices increase

Once mobile device switches to a Wi-Fi network, it is susceptible to man-in-the-middle (MITM) attacks[6]



[5]*http://www.wi-fi.org/news_articles.php?f=media_news&news_id=969;*
[6]*http://threatcenter.smobilesystems.com/?p=1587*

WIDE-SPREAD IMPLICATIONS

Personal mobile devices are "sneaking" on to enterprise networks

Mobile threat vectors are increasing in number, complexity and sophistication

IT staffs are fast becoming overwhelmed or lack mobile experience

[1]Forrester Research; [2] IDC

AGENDA

1. MOBILE MARKET & TRENDS
2. THREATS TO MOBILE DEVICES, USERS & ASSETS
3. **ADDRESSING TODAY'S MOBILE THREATS**
4. SUMMARY

MINIMUM REQUIREMENTS FOR ADDRESSING TODAY'S MOBILE THREATS

Proactive malware protection

- Protect mobile devices against malware and viruses delivered via any transmission means
- Frequent virus definition updates
- Real-time scanning of incoming files
- Scan of internal memory, memory cards, and entire device with ability to generate automated alerts

Loss and theft protection

- Integrated mobile device management capabilities
- Use GPS to identify the location of missing device
- Restore data to any subsequent device, regardless of mobile OS
- Remotely control devices, including initiating backups, locking, and data wiping

MINIMUM REQUIREMENTS FOR ADDRESSING TODAY'S MOBILE THREATS *(CONTINUED)*

Safeguards against communication interception

- Employ VPN that encrypts communications between mobile devices and corporate networks
- Establish and enforce corporate mobility policies
- Disable infected mobile device access

Device monitoring capabilities

- Protect company from lawsuits for inappropriate communications
- Ensure only appropriate apps have been downloaded

ADDITIONAL CONSIDERATION FOR ADDRESSING TODAY'S MOBILE THREATS

Broad Device and Mobile OS Support

- Smartphones, tablets, netbooks, and notebooks are complementary in nature
- Need to account for a broad set of devices
- Same type of multi-factor authentication should be supported on all devices

Integrated Mobile Device Management (MDM) and Security Policy Enforcement

- Centralized control of disparate mobile device platforms and types
- Cohesive MDM and security policy enforcement
- Enforce granular, role-based access control to corporate applications
- Deliver seamless, cross-platform authentication for all users, regardless of device

Minimize End User Requirements

Leverage Self-Help Models to Reduce Overhead

SECURE MOBILE CONNECTIVITY

Cover range of application access requirements

- Web VPN (browser-based applications)
- Secure Email (secure ActiveSync proxy)
- Full Layer 3 Tunnel

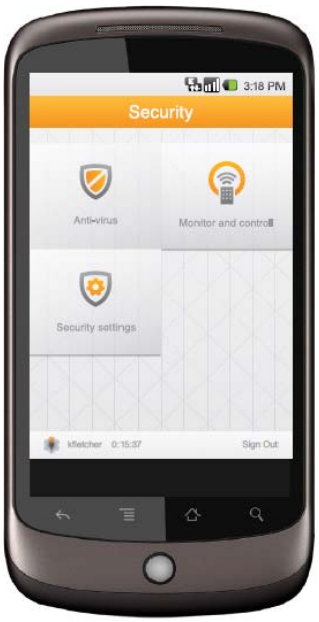
Unparalleled “Data in Transit” Security

- Leverages SSL VPN
- Multi-factor authentication
- Granular auditing and logging

SECURITY AGAINST MALWARE

Comprehensive Smartphone
Device Management and Security

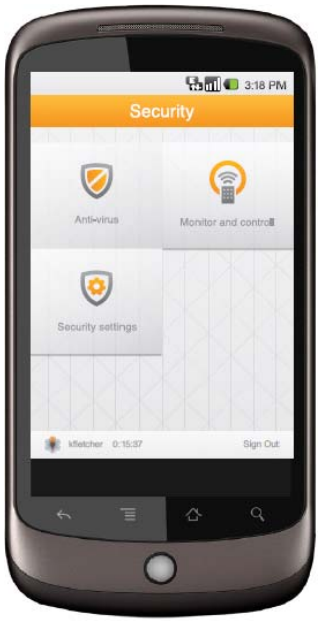
- Antivirus
- Firewall
- Anti-Spam
- Loss and Theft Protection
- Compliance Mandated Monitoring and Control



PREVENT AGAINST LOSS OR THEFT

Comprehensive Smartphone
Device Management and Security

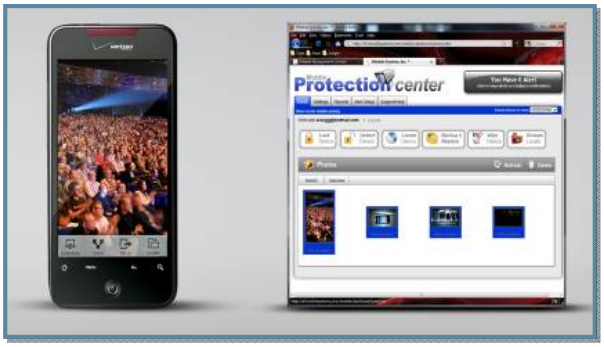
- Antivirus
- Firewall
- Anti-Spam
- Loss and Theft Protection
- Compliance Mandated Monitoring and Control

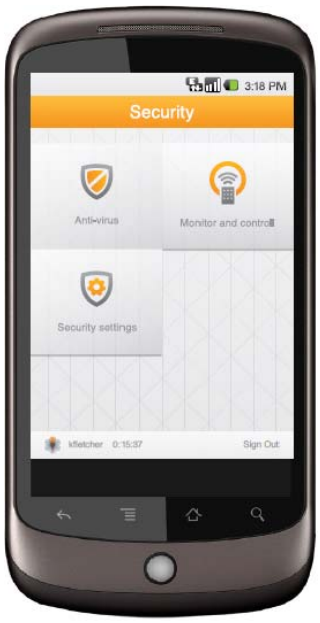


COMPLIANCE

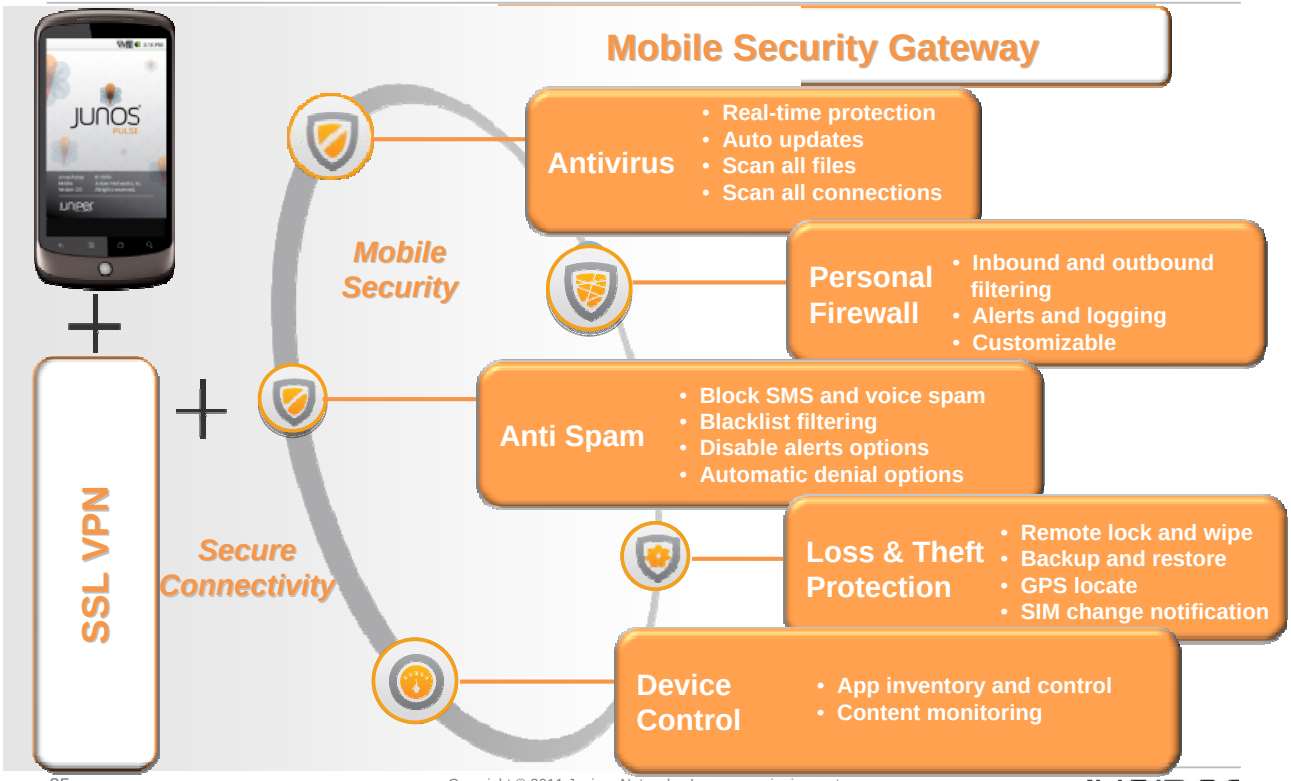
Comprehensive Smartphone
Device Management and Security

- Antivirus
- Firewall
- Anti-Spam
- Loss and Theft Protection
- Compliance Mandated Monitoring and Control



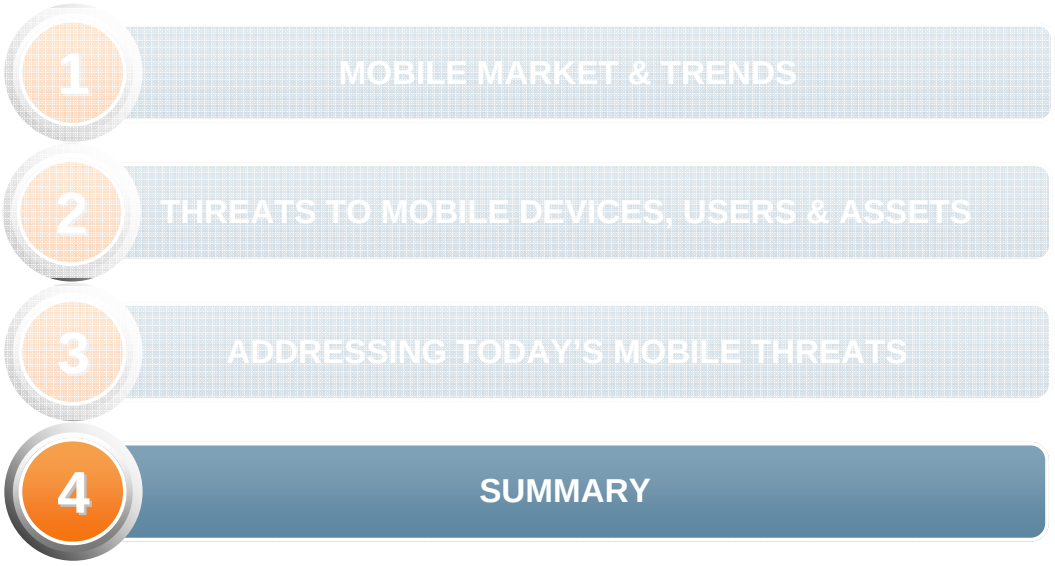


MOBILE SECURITY SUITE



SECURITY FOR ALL SMARTPHONE MARKETS AND USERS

AGENDA



CHALLENGES OF SUPPORTING A MOBILE WORKFORCE

Enable secure corporate access for smartphones, tablets and other mobile devices

Enforce the same existing authentication methods and security settings for personal mobile devices as corporate managed systems

Deliver secure, remote access for mobile devices, while enforcing granular access control

Adapt mobility and security policies to allow for personal mobile devices

SECURE, SCALABLE MOBILITY

Mobile device threats are pervasive and escalating

Malware, loss and theft, exploitation and misconduct, communication interception, and direct attacks

Cost effectively guard against current and emerging threats while retaining optimal productivity and flexibility in mobile device use

- Scalable VPN infrastructure
- Scalable mobile security infrastructure
- Broad range of mobile platform support covering all leading mobile platforms

everywhere