LA-UR- 11-03994

Approved for public release;
distribution is unlimited.

Title:	Enterprise Mobility ~~at Los Alamos~~ - Finding the Right Balance Mobile Computing at Los Alamos
Author(s):	Anil Karmel
Intended for:	Gartner Catalyst 2011

Los Alamos
NATIONAL LABORATORY
EST. 1943

Form 836 (7/06)

Enterprise Mobility: Finding the Right Balance

Mobile Computing at Los Alamos

Anil Karmel

Solutions Architect

Network & Infrastructure Engineering
Production Systems

Los Alamos NATIONAL LABORATORY EST. 1943

Outline

- Why Enterprise Mobility?
  - Business Case
  - Problems we need to solve
- RIM Blackberry
  - Security Posture
  - Accomplishments and Statistics
- Apple iPad and Google Android
  - Good Mobile
  - Other Use Cases
- Infrastructure Monitoring & Control
- Key Takeaways / Considerations

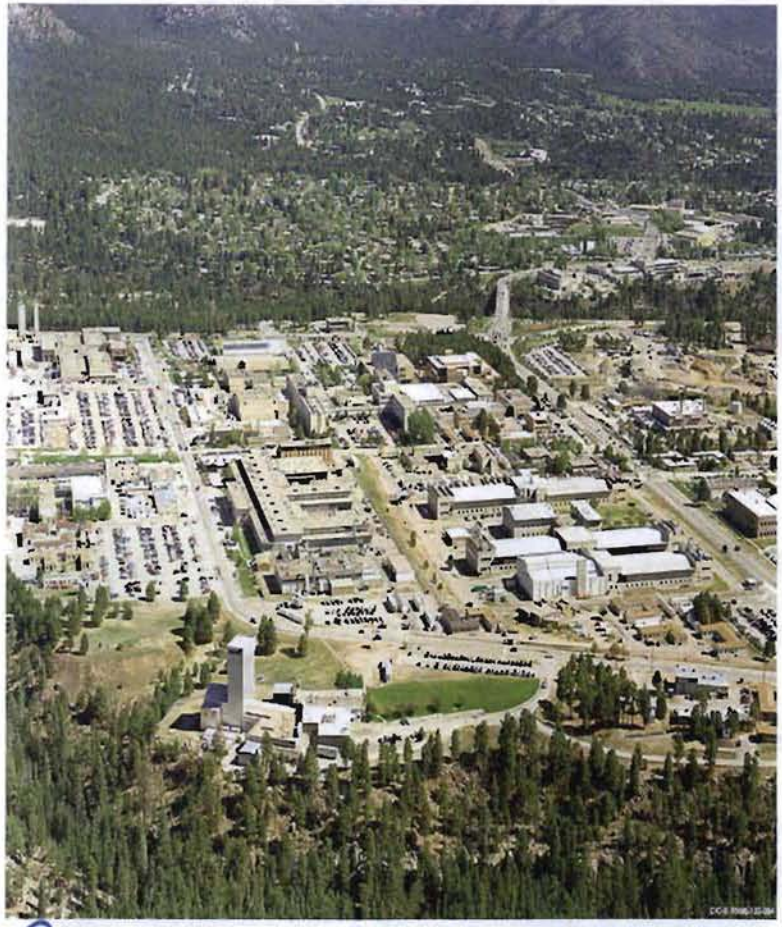
Why Enterprise Mobility?
Where's the right balance?

- Key Drivers
  - Rapid innovation driving smartphones into the enterprise
  - Users are increasingly mobile and require access to enterprise resources
- Key Issues
  - Malware
  - Application Architecture
  - Mobile Content Delivery
- Key Considerations
  - Corporate vs. Personally owned devices
  - Help Desk Support

Background
Los Alamos National Laboratory

- LANL applies its expertise in defense science and technology to the broad spectrum of DOE requirements from basic research to ensuring the safety and reliability of the U.S. nuclear weapons stockpile

Background
Los Alamos National Laboratory



- Located in northern New Mexico
- Elevation – 7500 feet
- 42 square mile campus
- 10,000 employees
- Unclassified Protected Network Stats
  - ~ 20,000 devices
    - ~ 14,000 Windows Systems
    - ~ 3,000 Apple Systems
    - ~ 1,500 *Nix Systems

Los Alamos NATIONAL LABORATORY EST. 1943

NNSA

Why Enterprise Mobility?
Where's the right balance?

- Key Drivers
  - Rapid innovation driving smartphones into the enterprise
  - Users are increasingly mobile and require access to enterprise resources
- Key Issues
  - Malware
  - Application Architecture
  - Mobile Content Delivery
- Key Considerations
  - Personal vs. Corporate owned devices
  - Help Desk Support

LANL Blackberry Deployment
Current Environment

- Security
  - Secured with DISA/DoD Secure Technical Implementation Guide
  - Transmissions & Data fully encrypted (FIPS 140-2 compliant)
- Devices
  - Blackberry 9650 Bold (no camera or WiFi)
- Ability to remotely wipe a Blackberry if it is lost or stolen

LANL Blackberry Deployment
Security Posture

- Blackberry can't connect to a foreign wireless network (no WiFi)
- Only a LANL-supplied SIM can be used on the device
- No third party applications allowed
- USB port and microSD card slot disabled
- Blackberry "Home" Screen locked on all smartphones
- Web Traffic routed through LANL infrastructure
- 24/7 phone number to call if Blackberry is lost or stolen

LANL Blackberry Deployment
Current Statistics

- Customer Pilot launched May 2008
  - 50 Users
- Release to Production - October 2008
  - 300 Users
- Blackberry / SMIME encryption complete March 2010
  - 600 Users
- Blackberry in Secure Areas complete April 2010
  - 1800 Users

Apple iPad and Google Android
Consumer-Oriented devices in the Enterprise

- End Users demand functionality – IT requires security
- How does IT deliver solutions and yet secure consumer-oriented devices?

Why Enterprise Mobility?
What's LANL's balance?

- Key Drivers
  - Security
  - Mobility for scientists and managers
- Key Issues
  - Malware : found right partners
  - Application Architecture :
  - Mobile Content Delivery : mobile web portal
- Key Considerations
  - Corporate owned devices

Good Mobile
Apple iPad and Google Android

- Enterprise-class Email, Calendar & Contacts
  - Consistent feature set across all platforms
  - Message indicators for reply/forward, high importance, meeting invites, etc.
  - Accept/Decline meeting requests from Inbox and view conflicts
  - Access to Global Address List (GAL)
- Launcher Bar
  - Provides quick access to apps

Good Mobile
Security Posture

- Security
  - Secured with DISA/DoD Secure Technical Implementation Guide (draft)
  - Transmission & Data fully encrypted (FIPS 140-2 compliant)
- Devices
  - Motorola Droid Pro, Droid X, Droid 2 Global
  - Motorola Xoom – Google Android tablet
  - Apple iPhone 32GB and iPad 2 64GB with Verizon MiFi
- Secure Enterprise Container
  - IT keeps corporate data secure
  - End users get to keep their personal apps
  - Ability to remotely wipe the application / data if it is lost or stolen

Good Mobile

Sandbox Protection on a Consumer-Oriented Device

Sandboxed Protection

Personal Data

Devices remain personal

- Untouched by enterprise

Freely access your data

- Third Party Applications
- Pictures
- Videos

Protected Data

Enterprise data lockdown

- Data encryption
- Password
- Remote wipe

Access corporate apps

- Email, attachments & PIM
- Intranets
- Document repositories
- Corporate IM

Los Alamos NATIONAL LABORATORY EST. 1943

NNSA

Good Mobile
Device Level Security

- Apple-supplied device restrictions
  - Device Level Password / Wipe
  - Camera
  - Safari
  - iTunes / App store and installing apps
  - Explicit content from the iTunes Store
  - YouTube
  - Screen Capture Block
  - WiFi & VPN controls

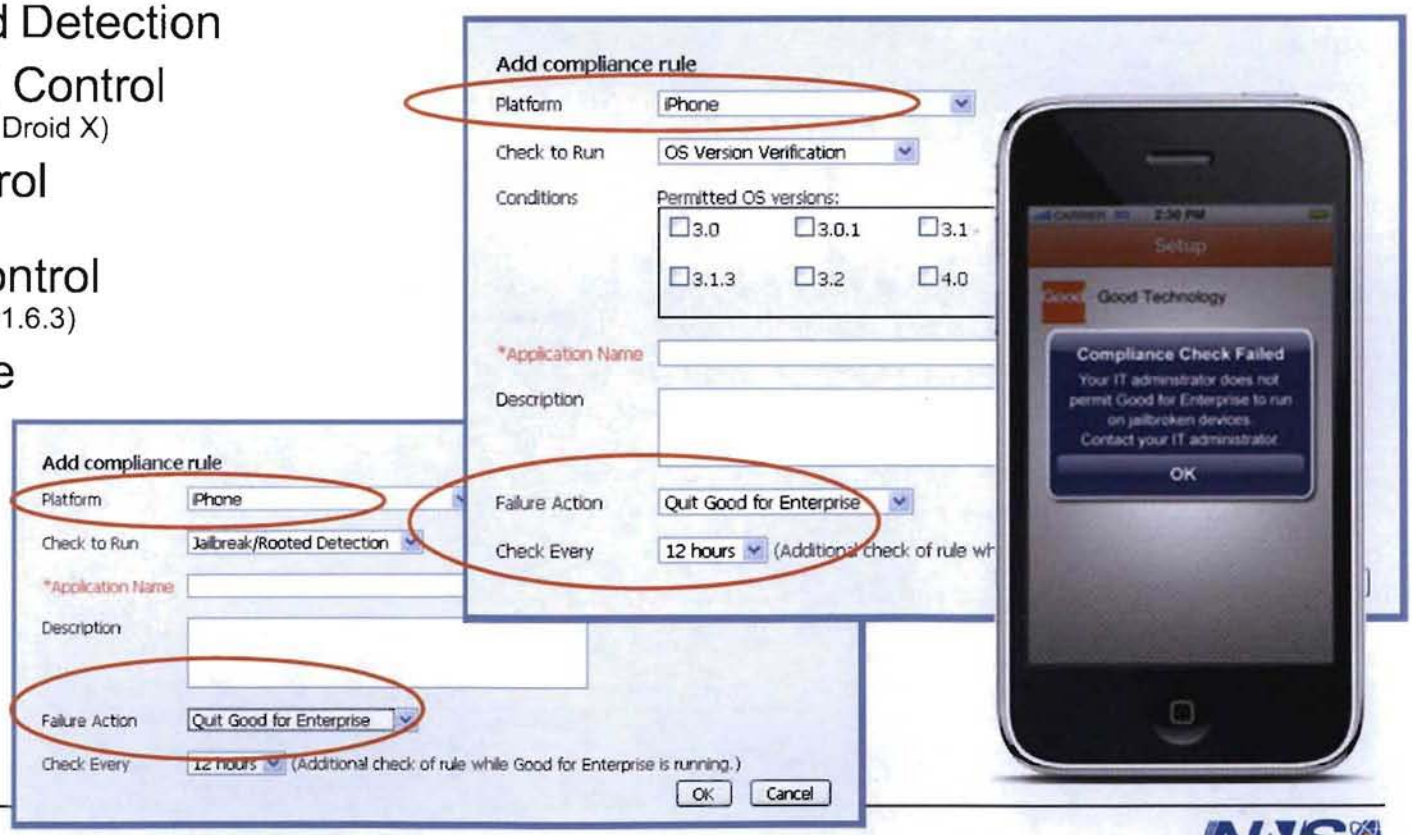
- Good-supplied device restrictions – iOS & Android
  - Control for Device type (3gs, 4.0, iPad) / OS type / Good Version type
  - "Jailbreak" detection – Good app block or wipe
  - "Timebomb" app wipe

Good Mobile
Compliance Manager

Compliance Manager
Checked during provisioning, at startup and on an interval basis.

Compliance Rules
- Jailbreak/Rooted Detection
- Hardware Model Control
  (Example: iPhone 4, iPad, Droid X)
- OS Version control
  (Example: 1.5, 3.1.2, 4.0)
- Client Version control
  (Example: v1.6.0, v1.6.1, v1.6.3)
- "Timebomb" wipe

Failure Action
- Quit Good for Enterprise
- Wipe Enterprise Data



Los Alamos NATIONAL LABORATORY EST. 1943

NNSA

Apple iPad
Additional Use Case

- Remote access to your Desktop
  - VMware View Client for iPad (Virtual Destops)
  - Remote Desktop Client for iPad (Physical Desktops)

Infrastructure Monitoring and Control
Boxtone

- Enterprise Monitoring
  - Monitor end-to-end system health and performance of Blackberry and Good infrastructures
- Security
  - Encryption configuration (device, SD)
  - Feature enable/disable (camera, SD, Bluetooth, WiFi, apps, app store, iTunes, cookies)
  - Password enforcement
  - Remote lock
  - Data/access quarantine
  - Selective (corporate) and full wipe

Key Takeaways / Considerations

- What's Your Security Posture?
- Create cross-functional teams
  - Technical
  - Customer
- Manage User Expectations
  - Give users new features rather than take them away
  - Start small, scale quickly

Mobile Computing at Los Alamos

Secure Enterprise Mobility Solutions to enhance User Productivity