

**Mobile Apps**

**Auditing & Forensics**



**Aman Bhar**

**Training & Solutions  
Director,  
Lancelot Institute**

aman@lancelotinstitute.com

**Agenda**

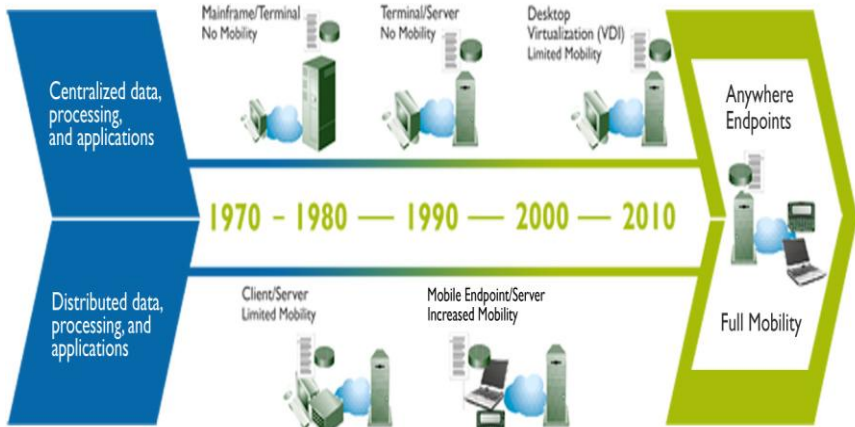
- Governing the Use of Apps on Mobile Devices
  - ✓How did we get here?
  - ✓Where are we now?
  - ✓So now what do we do?
- Policy Implementation
- Auditing Apps & Devices Against Policy
- Detecting & Dissecting Malware via Mobile Forensics



# Governing the Use of Apps on Mobile Devices



## How Did We Get Here?



## How Did We Get Here?



- June, 2004: Cabir, first of its kind
- Sept, 2004: Brador & Duts, attacking PocketPCs
- Dec, 2004: Skulls, overwrites files on the mobile device
- Feb – Sept, 2005: Cabir variants, detected in > 30 countries
- Oct, 2005: CommWarrior, causes unwanted billing
- Nov, 2005: Fontal, makes mobile device unusable after reboot
- March, 2006: Flexispy, commercial spying application
- June, 2006: SD Dropper, installs Skulls on the mobile device

## How Did We Get Here?



- Sept, 2008
- Mobile Malware billed as *new* threat, developed by organized criminals, growing rapidly,
- Observed changes in user behavior:
  - ✓ Increased use of 'always-on' broadband access & wireless hotspots
  - ✓ Increased use of networked applications e.g. instant messaging, VoIP
  - ✓ Increased sharing of files e.g. music, video, software
  - ✓ Increased workforce mobility
  - ✓ Increased use of multiple connected devices e.g. PDAs, mobile phones

## How Did We Get Here?



☐ Sept, 2008....

- ✓ Any device, Any time, Any where was born
- ✓ Users not interested in security, they want to trust, not to be trusted
- ✓ Any unprotected device connected to both the Internet & and company LAN poses a security risk

## How Did We Get Here?



*Case Study* ☺

### **Mobile Device Spying Tools**

- ☐ Apps installed on mobile devices that send info out
- ☐ NOT illegal in many countries
- ☐ Use cases
  - ✓ Managers spying on employees
  - ✓ Industrial spies

## How Did We Get Here?



- SMS/MMS
  - ✓ Sender & Receiver phone numbers
  - ✓ Phone Book names
  - ✓ Content
  
- E-mail traffic
  - ✓ Sender & Receiver addresses
  - ✓ Text & Attachments
  
- SIM Info
  - ✓ Sends out the SIM IMSI & phone number when SIM inserted
  
- Calls
  - ✓ Incoming & Outgoing call numbers
  - ✓ Time & Duration of calls
  - ✓ Setting covert conference call to listen to either all or specific number-based calls

## How Did We Get Here?



- Voice Recording
  - ✓ Records all phone calls to a memory card
  - ✓ Sends recording over Bluetooth, HTTP or via MMS
  
- Location Tracking
  - ✓ Sends GSM cell ID & Signal info
  - ✓ Sends GPS coordinates
  
- Key Presses
  - ✓ Logs & Sends user key presses via SMS
  
- Power Management
  - ✓ Ability to kill processes, e.g. AV processes ☺
  
- Flexispy did most of the above, was **Symbian Signed**, and passed audit ☺

## Where Are We Now?



- Shifting from email-centric to including *critical* corporate apps
- Acts as mobile office, social tool & entertainment centre ☺
- Becoming the “7<sup>th</sup> sense” ☺

## Where Are We Now?



Case Study One ☺

### Growth in Mobile Malware via “enticing” Apps

- 8000 iOS & Android users joined a mobile device botnet
  - ✓ Via a weather app
    - Grabbed GPS coordinates
    - Grabbed tel. numbers
    - Gave botmaster potential control over devices
- >1,000,000 Android users leak info
  - ✓ Via a wallpaper app
    - Leaked the following to a China-based server:
      - ❖ Phone numbers
      - ❖ Subscriber identifiers
      - ❖ Voicemail numbers
- MMS Bomber affected “millions of Chinese”

## Where Are We Now?



Case Study Two ☺

### The following moving to Mobile Devices

- Targeted Attacks
  - ✓ Email attachments
  - ✓ MMS attachments
  - ✓ Embedded Url
  - ✓ Instant messenger
- Social Engineering (that easily fool sophisticated users)
- 0-day Vulnerabilities
- Rootkits
- Innovative Attack Toolkits

## Where Are We Now?



Case Study Three ☺

### Legitimate App Infections

- Android.Pjapps,
  - ✓ Opens a backdoor
  - ✓ Installs apps
  - ✓ Navigates to websites
  - ✓ Adds bookmarks
  - ✓ Sends SMS messages
  - ✓ Blocks SMS responses
  - ✓ Sends IMEI, DeviceID, SIM, Line Number to Cloud-based C&C

## Where Are We Now?



*Case Study Four* ☺

### **Mobile Banking App Flaws**

- Wells Fargo
- BofA
- USAA
  - ✓ Stores the following in device memory
    - Usernames
    - Pwds
    - Security question answers
    - Page images
    - Account balances
    - Routing numbers
- 12 MM Americans actively use mobile banking services ☺

## Where Are We Now?



*Case Study Four* ☺

### **Near-Field Communications**

- Similar to passive card readers
- NFC is able to both read and transmit
  - ✓ Wireless Payments
  - ✓ Prompted PCI to Form Mobile Payments Task Force
    - PCI DSS for traditional architectures
    - PCI DSS for virtualized architectures
    - PCI DSS for "mobile architectures"? ☺

## Where Are We Now?

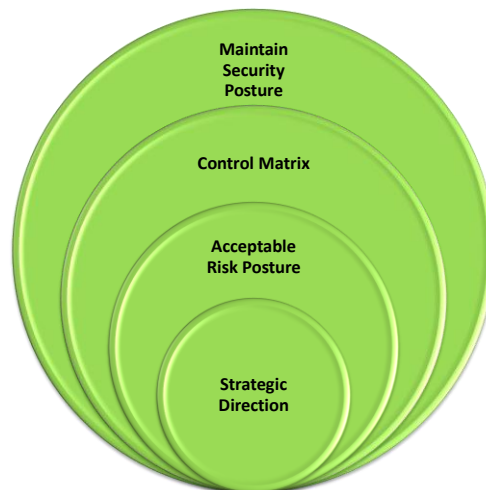


Case Study Five ☺

### App Development for Non-Developers ☺

- Step 1: Envision app features
- Step 2: Develop using SDKs
- Step 3: Test & Debug (for functionality)
- Step 4: Distribute in approved marketplaces

## So Now What Do We Do?



What are you  
*really* protecting?



Your  
*value proposition*



Assessing  
**risks...**

.... to these  
*critical business functions*



- 1. Threats x Vulnerabilities
  - Quantitative
    - SLE
    - ALE
  - Qualitative
    - Scenarios
- 2. Acceptable Risk Position
- 3. Residual Risk
  - a) PoNC
  - b) PoC



Implement an appropriate **response....**

6



.....to these **risks...**

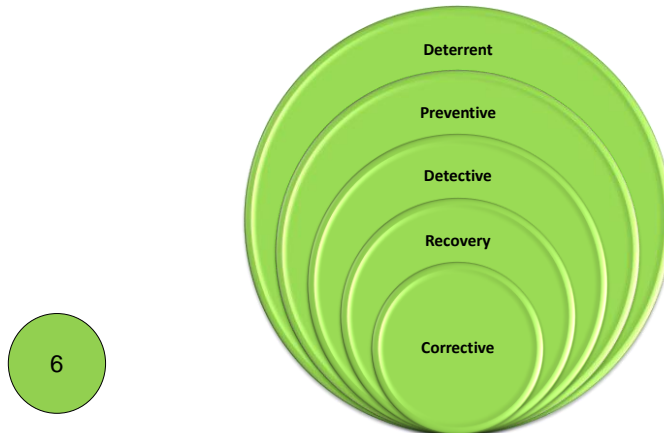
- a) Accept
- b) Transfer
- c) *Mitigate* .....
- d) Avoid

.....**Mitigate** via appropriate **controls....**

6



- Physical
- **Administrative**
- **Technical**

**6 Steps to Defense-in-Depth**


*Compensating (PAT) at every level*

**Mobile Device Recommended Controls**

- Solid mobile device policy
  - ✓ Enforce lockout policies
  - ✓ Enforce remote wipe
  - ✓ Even if BYOD ☺
  
- Provisioning policy
  - ✓ BYOD?
  - ✓ Standardized devices?
  - ✓ Access levels?
  - ✓ Access classification?
  - ✓ Absorb, subsidize or pass on cost of handsets to users?
  - ✓ How do you manage the shipment & transmission of devices & credentials to users?
  
- User Education Policy
  - ✓ Only use regulated app marketplaces for downloading & installing apps
  - ✓ Enable settings to stop installation of non-market apps
  - ✓ Monitor comments in marketplace for apps
  - ✓ Check access permissions requested during app install

## Mobile Device Recommended Controls



- Sandboxing
- Controlled app distribution
- Controlled app removal
- Backup & Recovery
- New Authentication options
  - ✓ But all still based on Types 1-3
- Modify support processes
  - ✓ An interesting example ☺
- Keep devices current with latest OS upgrades
  - ✓ E.g. iOS4.1.2 & 3 are security upgrades
- Choose the correct distribution model ☺
- Ensure forensics skill sets are a-ok ☺

## Mobile Apps Distribution Models



- Mobile Device Management Server
  - In-house
  - 3<sup>rd</sup>-party
  - Step 1: Silent communication with device
  - Step 2(a): Device communicates with server
  - Step 2(b): Device performs tasks requested by server
    - Updating policies
    - Providing info
    - Removing settings
    - Removing data
- Enroll devices
  - Wired via USB port
  - Wireless
    - Over-the-air' via a "secure" web portal ☺
      - User & device authentication
      - Certificate provisioning
      - Device config via SSL

## Mobile Apps Distribution Models



- Mobile Device Management Server
  - Configure Devices via signed, encrypted & locked Configuration Profiles
    - XML files ☺
    - So now.....
      - Only trusted users are accessing corporate services ☺
      - Their devices are properly configured with established policies

---

## Mobile Apps Distribution Models



- Mobile Device Management Server
  - Policy Examples
    - Require passcode
      - Allow simple value
      - Require alphanumeric value
      - Length
      - Nos. complex characters
      - Nos. unique passcode prior to passcode reuse
    - Aging
    - Clipping level
      - Lockout
      - Remote wipe
    - Time before auto lock-out
    - User ability to remove config profile

## Mobile Apps Distribution Models



- Mobile Device Management Server
  - Restriction Examples
    - App installation
    - App store access
    - Camera use
    - Screen captures
    - Mail synching
    - In-app purchasing
    - Backups
    - Music/Podcast/MP4s/Videos
    - Youtube
    - Browser restrictions

## Mobile Apps Distribution Models



That's all good for users (devices) under corporate control

- Employees
- Contractors

But what about users (devices) not under corporate control? ☺

- Clients
- Community
- Prospective Clients
- Public-at-large

## Mobile Apps Distribution Models



### Secure & not-so-secure app marketplaces/stores

#### Clouds ☺

•“Some experts say that mobile and the cloud may be a match made in heaven!”

•Virtualizing all apps and granting access to the services provided by those apps via a simple client...

- Lost devices = ?
  - It's just a device without sensitive info on it...

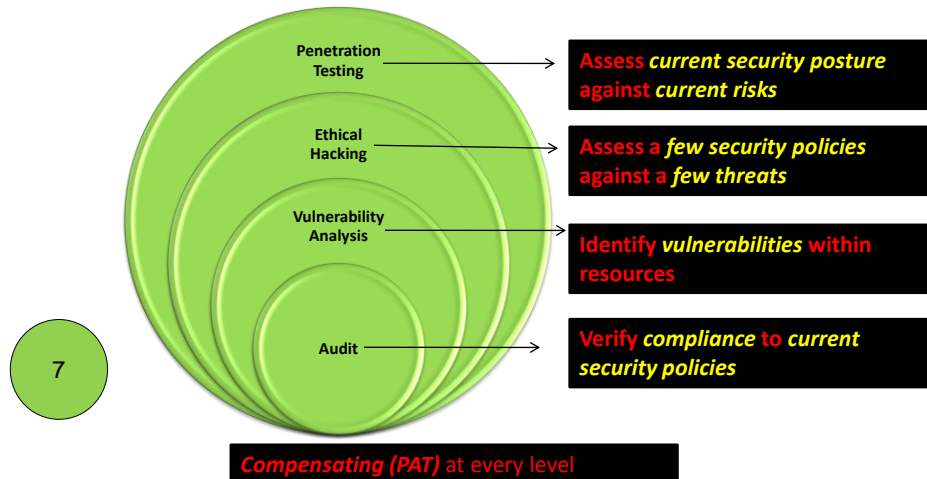
•Remember BYOD? ☺



## Maintain organizational *security posture*



- Audits
- Ethical hacks
- Vulnerability assessments
- Penetration tests



## Mobile Devices in the Cloud **Lancelot** INSTITUTE

- Mobile Device in the Cloud 😊
  - What do auditors investigate?
  - Who are the key players?
  - How do we meet IT functional objectives?
  - Personnel R & R
  - Service level management
  - Outsourcing IT functions
  - Monitoring the status of controls
  - Capacity management
  - Problem management

## Mobile Devices in the Cloud **Lancelot** INSTITUTE

- Performing service-level management
  - Via an SLA
    - System availability
    - Service definition
    - Personnel qualification
    - Security requirements
    - Data integrity
    - SLA performance reporting
    - Right to audit ☺
    - SLA change procedures
    - Cost of service

37

## Mobile Devices in the Cloud **Lancelot** INSTITUTE

- Outsourcing IT functions
  - 4 parts to a contract of minimum standard
    1. Prior to negotiation
    2. Specific details
    3. Performance during execution
    4. Changes and resolution of issues

38

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 1. Systems monitoring controls
  - 2. Log management controls
  - 3. System access controls
  - 4. Data file controls
  - 5. Application processing controls
  - 6. Antivirus software controls
  - 7. Active content & mobile code controls
  - 8. Maintenance & change management controls
  - 9. Separate testing environment controls
  - 10. Administrative management controls

39

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 1. Systems monitoring controls
    - Hardware
    - Software
    - Syslog
    - Network device monitoring
    - Uptime-downtime reporting
      - Uptime
      - Downtime

40

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 2. Log management controls
    - 6 requirements
      1. Enable logging for security-related events
      2. Enable logging in application software
      3. Enable logging in the operating system
      4. Configure syslog to export logs from the device to be watched
      5. Configure a syslog server to receive the log files
      6. Read the log files ☺

41

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 3. System access controls
    - User login & account management ☺
    - Privileged login accounts
    - Maintenance login accounts

42

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 4. Data file controls
    - 4 types
      1. Standing data controls
      2. System control parameters
      3. Logical access controls
      4. Transaction processing controls

43

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 5. Application processing controls
    - Input controls
      - Unique login & password
      - Source document signatures
      - Client workstation / terminal identification
    - Processing controls
      - Batch totals
      - Total number of items
      - Transaction logs
      - Limit checks
      - Exception reporting
      - Job cost accounting
    - Output controls
      - Report generation & distribution
      - Negotiable instruments
      - Report retention
      - Event logs

44

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 6. Antivirus software controls
    - How are users acquiring AV updates?
    - Are IT staff testing updates on devices similar to what users are using?
    - Update issue and install time delays?

45

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 7. Active content & mobile code controls
    - Ah, a few of my favorite things... 😊
      - Web browser functions
      - MIME
      - Mobile software
        - » Java
        - » ASP
        - » Mobile code security policy
          - Disallow functionality?
          - Allow functionality from internal servers?
          - Allow functionality from trusted external servers?
          - Open season? 😊

46

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 8. Maintenance & change management controls
    - Backup & recovery
    - PM (maintenance is a mini project ) ☺
    - Change control review
      - » Configuration control
      - » Change authorization
      - » Emergency changes

47

## Cloud Auditing



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - 9. Separate testing environment controls
    - Separation of duties
    - PoNC

48

## IT Operations Management



- Monitoring the status of controls
  - Auditors need to gather evidence regarding the proper implementation of .....
  - Administrative management controls
  - Software licensing
  - Asset & media tracking
  - Asset disposal
  - User training
  - Procedures versus 'actual work' ☺
  - Ineffective / Inefficient controls
  - Compensating controls
    - » Job rotation, Auditing, Reconciliation, Exception report, Transaction logs, Supervisor review

49

## Cloud Auditing



- Capacity Management
  - "Monitoring of computer resources and planning for future availability"

50

# Cloud Auditing



- Problem Management
  - Digital forensics
    - Acquisition
      - Volatile data
      - Non-volatile data
      - Avoid use of keyboard
      - Create multiple images of files

51

# Cloud Auditing



- Problem Management
  - Digital forensics
    - Examination
      - Live data files
      - Deleted files
      - Memory contents
      - Network connections
      - Network shares
      - Strings
      - Directories
      - Configuration files
        - OS
        - User passwords
        - Process runs
        - Jobs
      - Log files
        - System events
        - Audit records
        - Command history
        - Previously accessed files
      - Application files
      - System swap files
      - Dump files
      - Temporary files
      - Hibernation files

52

## Cloud Auditing



- Problem Management
  - Digital forensics
    - Utilization
      - Correlate events to discover what happened, when

53

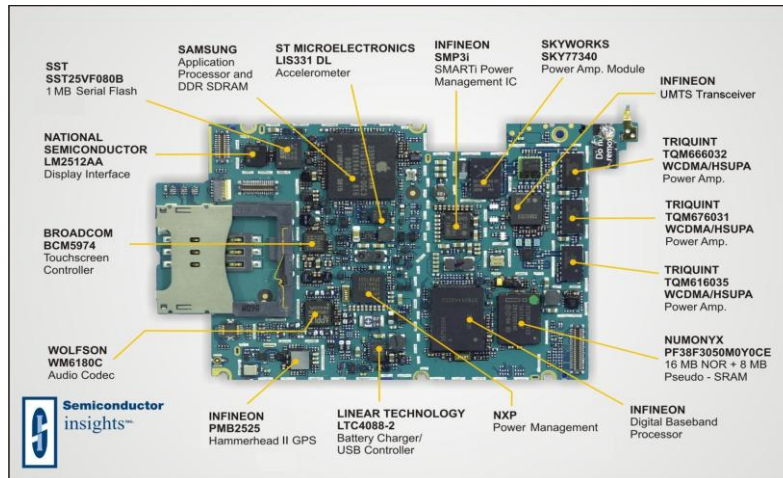
## Cloud Auditing



- Problem Management
  - Incident handling
    - Centralized team
    - Distributed team reporting to central authority
    - Coordination team providing guidance to first responders
  - Incidence response
    - Preparation
    - Detection and analysis
    - Containment, eradication, recovery
    - Post-incident activity

54

## Challenges of Mobile Device Forensics



## Challenges of Mobile Device Forensics



- Differing data types
  - Email
  - Text Messaging
  - Photos
  - Videos
  - Audio
  - Web History
  - Call History
  - Application Data
  - eBooks
  - Maps
  - Location History
- OS changes
  - E.g. iOS 4.x – 6 updates in 5 months
- Proprietary hardware
  - Some devices only allow access to logical information, not system databases or unallocated spaces
- Frequent device replacements
- Data volatility
- Data corroboration

**Questions?**

At Your Service 😊



**Aman Bhar**

Training & Solutions  
Director,  
Lancelot Institute

[aman@lancelotinstitute.com](mailto:aman@lancelotinstitute.com)