

A Taste of SANS SEC575 Part I: Invasion of the Mobile Phone Snatchers

Mobile Device Security and Ethical Hacking
Today's Focus: Mitigating the Stolen Device Threat

Joshua Wright
jwright@willhackforsushi.com

Outline

- What is SANS SEC575?
- Mobile Device Loss
- Mobile Device Backup Recovery
- Bypassing PIN Authentication
- Mitigating the Impact of Lost Devices
- Mobile Device Security

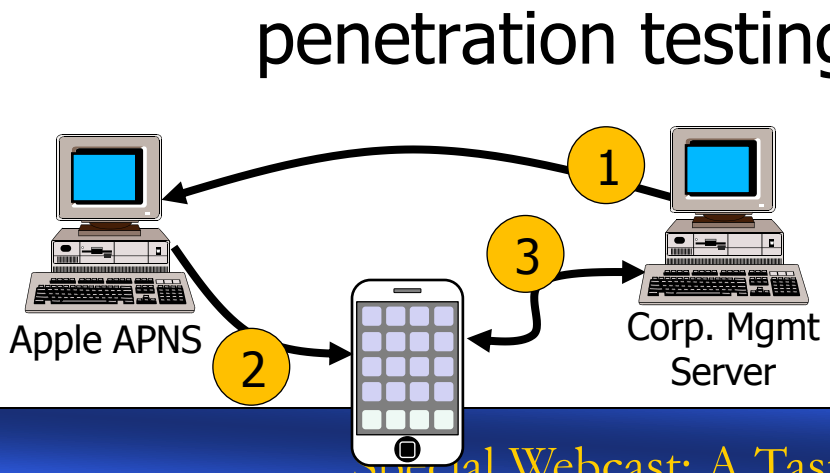
What is SEC575?

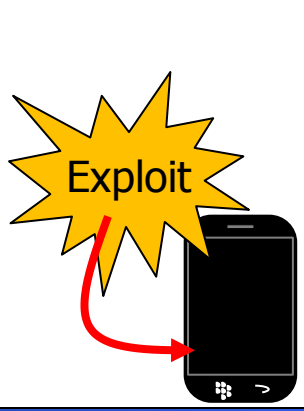
- A brand new 6-day course offering by SANS
- "Mobile Device Security and Ethical Hacking"
- Combining policy, architecture, defense and penetration testing
  - Hands-on exercises throughout, culminating in an in-depth Mobile Device Security Challenge event
- Covering Apple iOS (iPhone, iPad, iTouch), Android, BlackBerry and Windows Phone
- Written by Joshua Wright with leadership by Ed Skoudis as curriculum lead and advisor

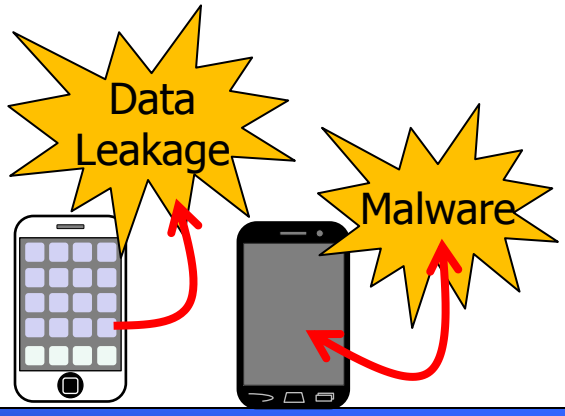
Building the skills necessary for effective mobile device security

Mobile Device Security Philosophy

- A secure mobile device deployment requires:
  - Policy that is practical and enforced
  - Device management and architectural controls
  - In-depth application analysis
  - Network, wireless, web and mobile device penetration testing







Sampling of Topics

- US and intl. law influence on mobile device policies
- Managing enterprise-owned, BYOD or combined deployments
- Weaknesses in the Apple permission management model
- Critical features to look for in MDM solutions
- Mobile malware threats on iOS, Android and BlackBerry
- Rooting and unlocking mobile devices
- Reverse-engineering iOS and Android applications for security analysis
- Mobile device wireless network scanning
- Defeating WPA2 security on mobile devices
- Exploiting web applications disguised as mobile apps
- Extracting data from mobile device backups (today!)

Outline

- What is SANS SEC575?
- Mobile Device Loss
- Mobile Device Backup Recovery
- Bypassing PIN Authentication
- Mitigating the Impact of Lost Devices
- Mobile Device Security

Mitigating the Stolen Device Threat

- Mobile devices will be lost or stolen
  - Employees will misplace devices
  - High-tech devices are a common theft target
- Stolen devices introduces risk to the organization
  - Information and system access threats with stored credentials
- Organizations can manage the threat through preparation, policy, and device management

Differentiating Mobile Device Loss

- Employee loses mobile device
  - Accidental exposure to the organization
  - Loss is not an IT threat until it is retrieved
- Stolen device as an opportunistic threat
  - Access to device and configured resources a curiosity investigation
- Stolen device, targeted threat
  - When executed properly, attacker steals device silently to retain the window of loss reporting
  - Hours to days of device and system access

From a risk perspective, stolen devices as a targeted threat carry the most risk, though it is difficult to differentiate the device loss scenario.

Loss Impact

What can an attacker do with a stolen device?

- Access device resources locally
- Extract data from external storage devices
- Synchronize device to a computer to access backup data
  - Potentially returning the device to avoid disclosure
- Jailbreak/unlock/root to access filesystem-level resources
  - Access locally-stored authentication credentials for further system exploitation
  - Backdoor device prior to return

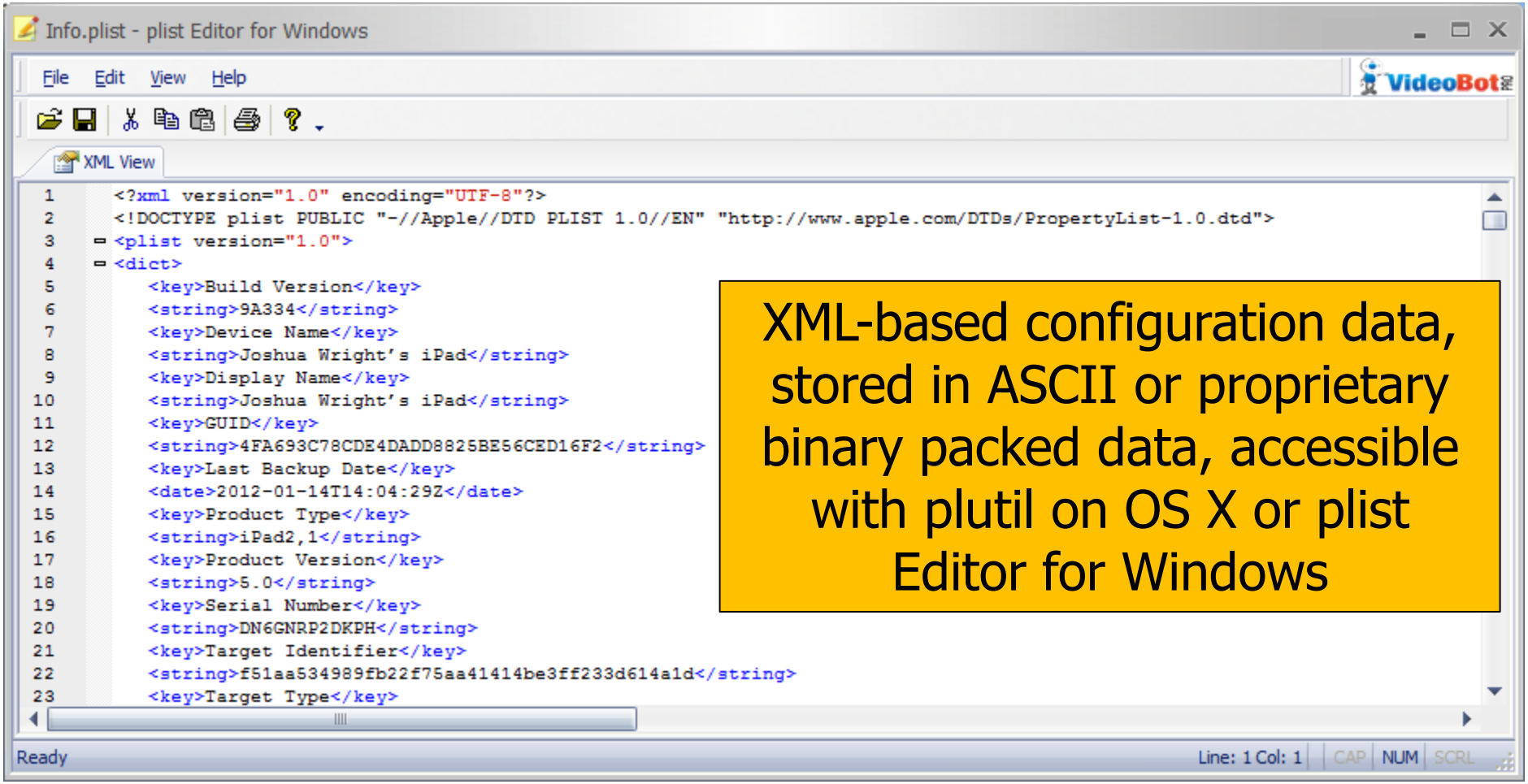
Outline

- What is SANS SEC575?
- Mobile Device Loss
- Mobile Device Backup Recovery
- Bypassing PIN Authentication
- Mitigating the Impact of Lost Devices
- Mobile Device Security

iOS Backup Resources

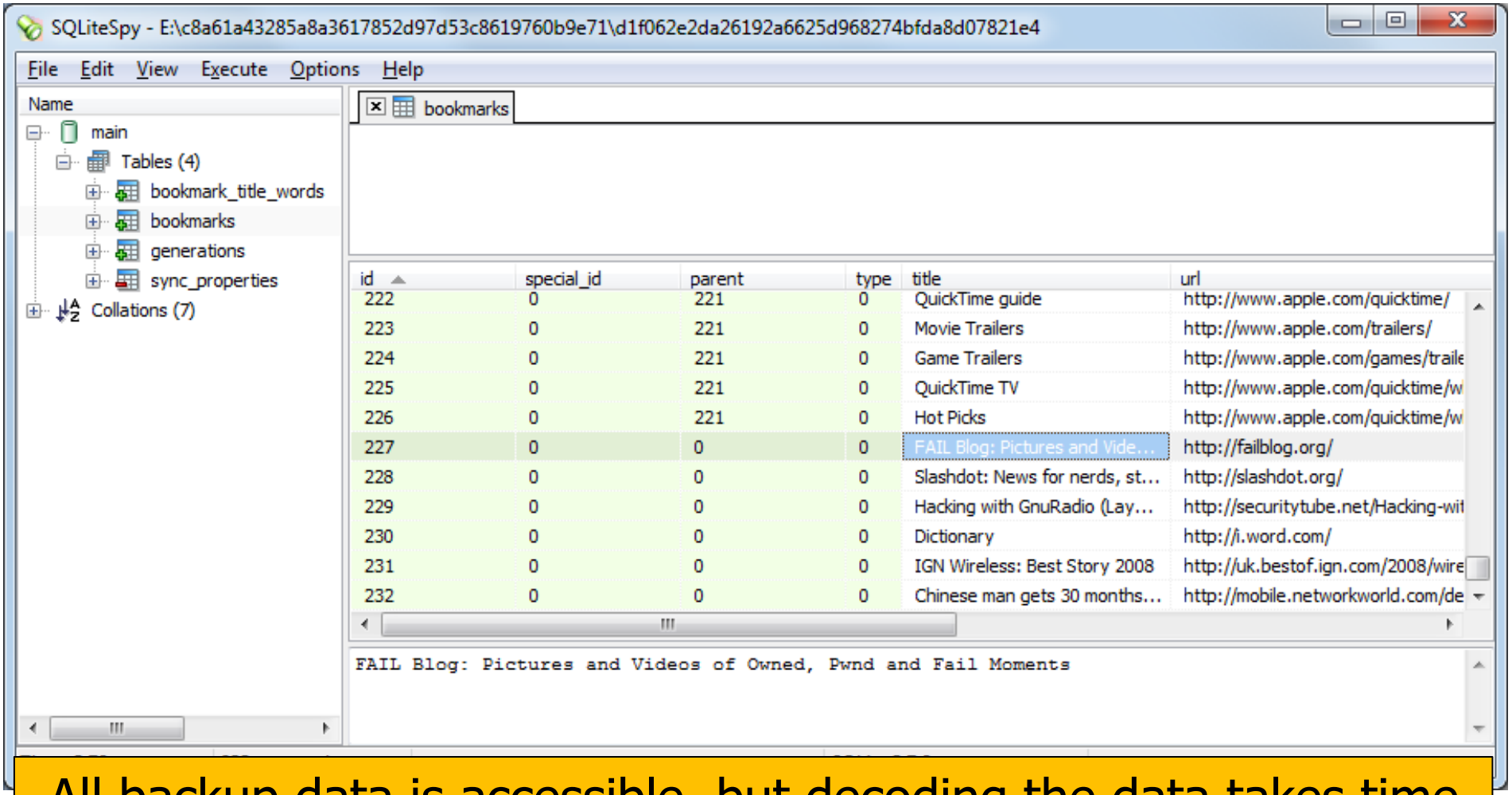
- `Status.plist` - Status of last backup including date and time
- `Manifest.plist` - Third-party app backup information including app version numbers
- `Info.plist` - iOS device information
  - ICCID (SIM serial number), IMEI, phone number
- `Mddata` files (hashed filenames) are backed up application resources
  - SMS database, contacts, etc.
  - Filename is a SHA1 hash of the full file path
- For encrypted backups, file content is protected

Viewing Plist Files



XML-based configuration data, stored in ASCII or proprietary binary packed data, accessible with plutil on OS X or plist Editor for Windows

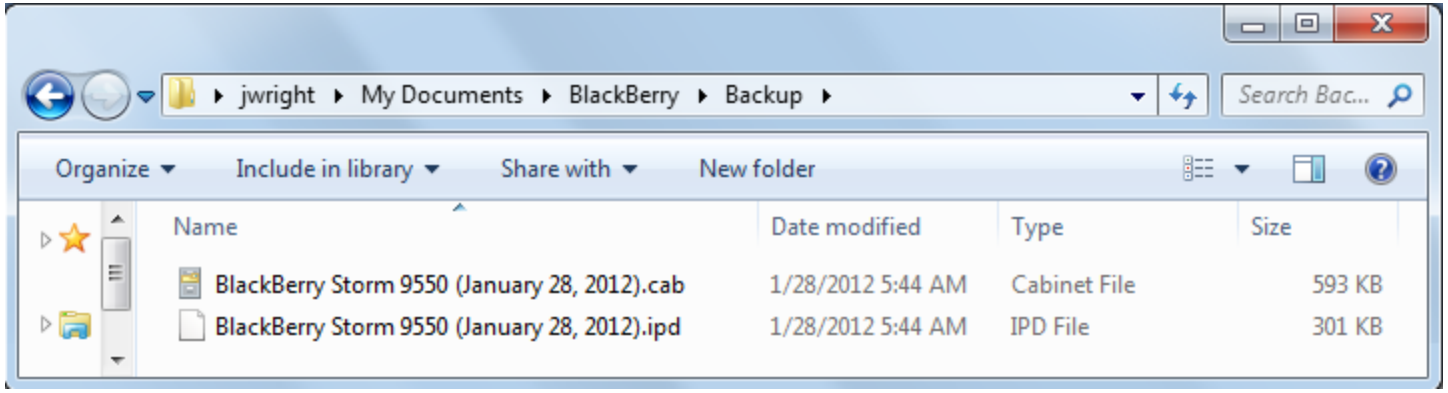
SQLiteSpy



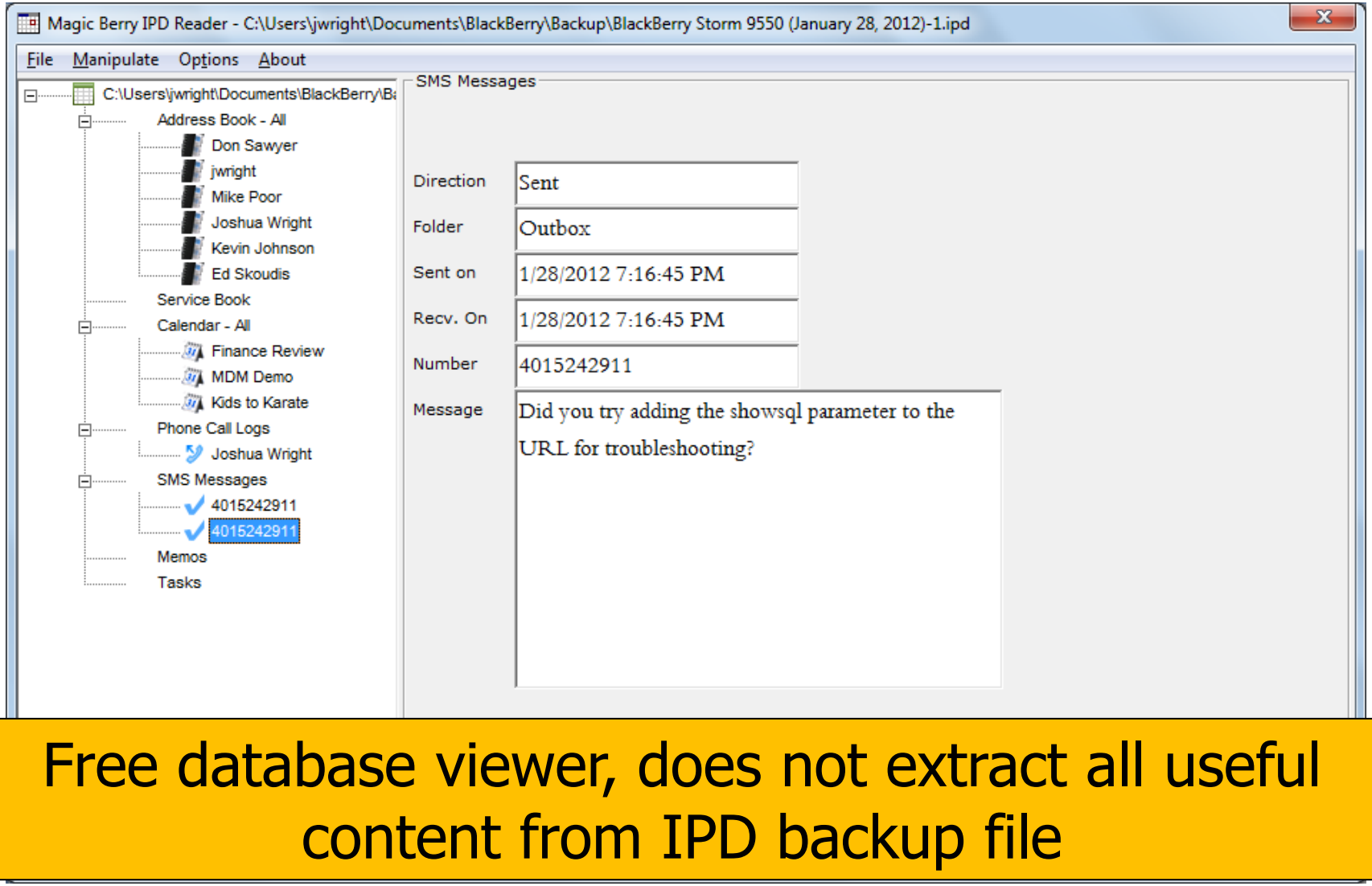
All backup data is accessible, but decoding the data takes time

BlackBerry Backup

- Transfers configuration, local e-mail, contacts, calendar, etc. (IPD file)
  - Optionally also includes media resources (CAB file)
- Stored in %USERPROFILE%\Documents\BlackBerry\Backup



Magic Berry IPD Reader



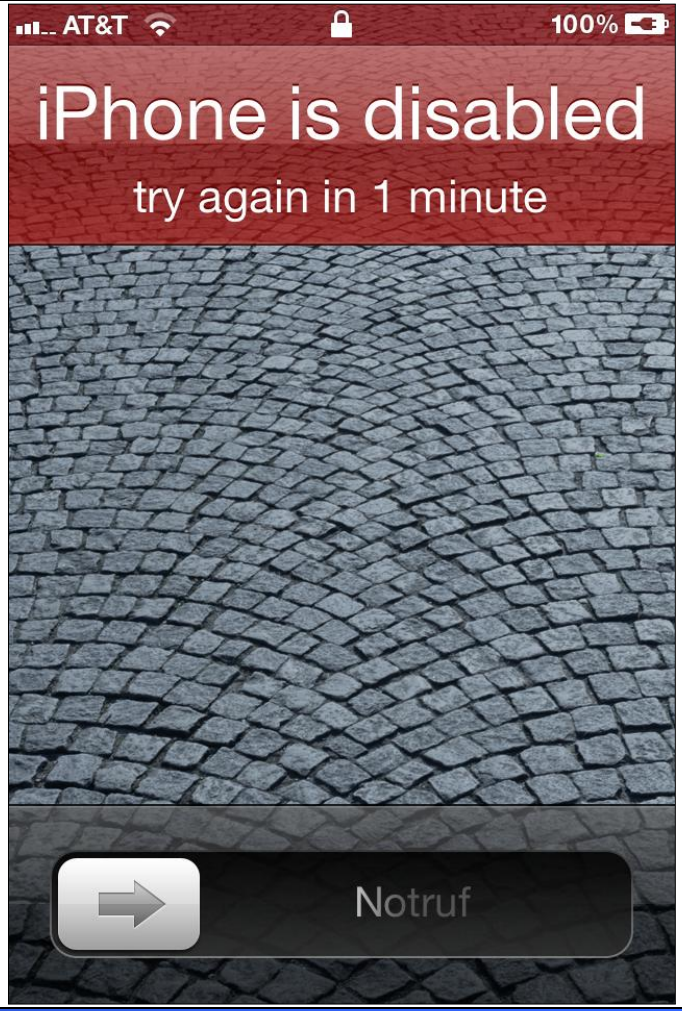
Free database viewer, does not extract all useful content from IPD backup file

Outline

- What is SANS SEC575?
- Mobile Device Loss
- Mobile Device Backup Recovery
- Bypassing PIN Authentication
- Mitigating the Impact of Lost Devices
- Mobile Device Security

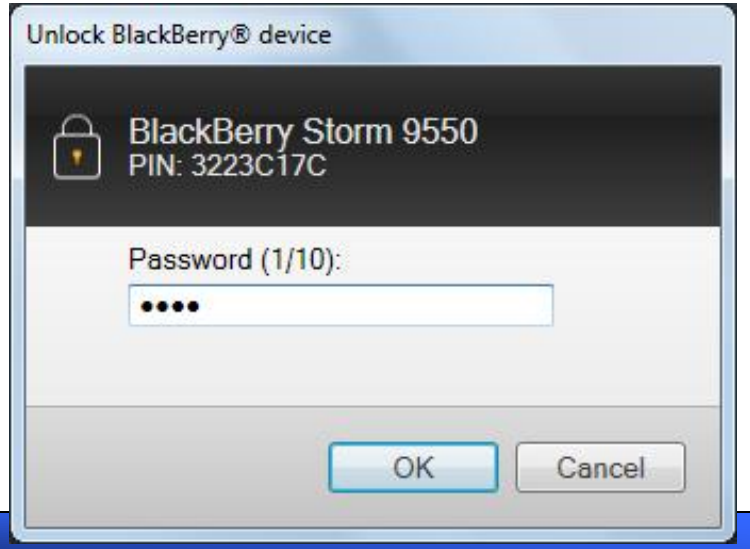
Device Passcodes

- To avoid lost device data loss, vendors provide a device passcode protection option
- Users enter device passcode each time they unlock the device
  - Limited number of failures before device wipe or exponential timer back-off
- Enforce device password requirement and passcode complexity with MDM
- Devices require password before backing up data



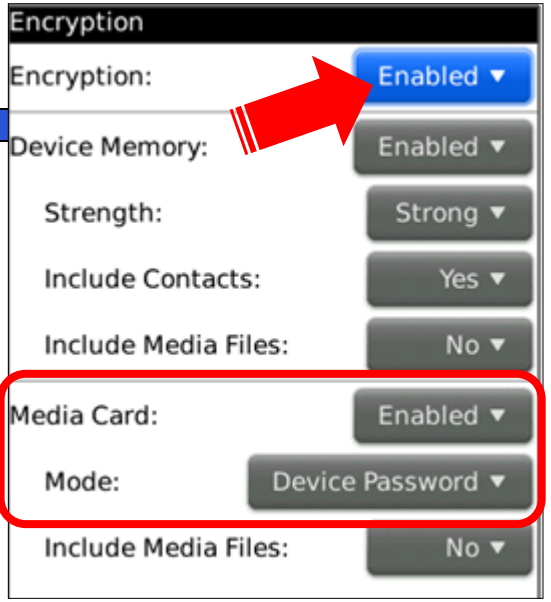
BlackBerry Device Passcode Attack

- When locked with a passcode, BlackBerry devices restricts access to the device
  - Must enter passcode to access device
  - Must enter passcode to backup on Windows
- Device passcode can be used to protect stored data on media card
- Attacker cannot access device or backup without passcode



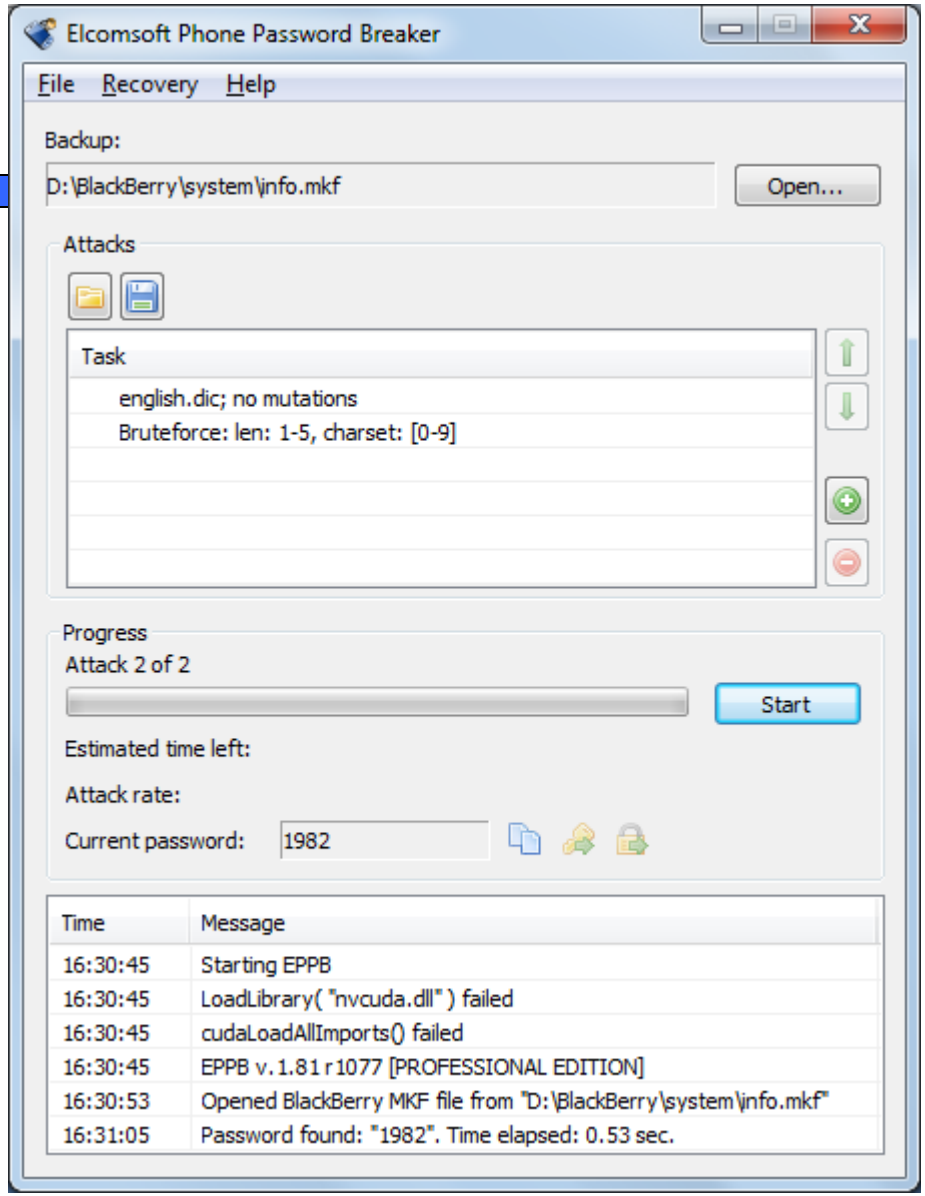
BlackBerry Device Passcode Recovery

- BlackBerry devices can encrypt both flash and media card
- Device passcode commonly used to encrypt media card
  - Media card is transferable
  - Key is protected with passcode
- When configured to encrypt media card, susceptible to offline wordlist attack



Elcomsoft Phone Password Breaker

- Read encrypted key in `\BlackBerry\System\info.mkf`
- Mount passcode attack
  - Not susceptible to wipe
- 4-digit PIN recovery in near real time
  - Can also attack longer PIN's and passcodes with wordlist attack mode
- Key recovery permits device backup to access data



iPhone Data Protection Tools

- Open-source project based on reverse-engineering iOS encryption
- Modifies official iOS firmware IPSW files to create alternate boot environment
- Python tools to mount PIN attack against a connected device
  - iPhone up to 4S, iPad 1 and 2 support
- Device must be susceptible to jailbreak

iPhone Data Protection Tools Setup and Attack

- Only supported on OS X, several steps for setup and configuration
- Outlined step-by-step at http://www.willhackforsushi.com/ios-key-recovery.pdf

```
$ ./demo_bruteforce.py
{'passcode': '1234', 'passcodeKey':
'2a98c5c7649352b5b90b9d69a8d213216b3693965ce15817cac11240aaaaaaaa'}
$ ./keychain_tool.py -d keychain-2.db 066ca6f0c178b7e7.plist
Keybag: SIGN check OK
Keybag unlocked with passcode key
Keychain version : 5
------------------------------------------------------------
                    Passwords
------------------------------------------------------------
Service :        EnhancedVoicemail
Account :        4015242911
Password :       1111
```

Tool output modified for space

Outline

- What is SANS SEC575?
- Mobile Device Loss
- Mobile Device Backup Recovery
- Bypassing PIN Authentication
- Mitigating the Impact of Lost Devices
- Mobile Device Security

Device Passcode Recommendations

- All devices must use a passcode to prevent unauthorized access, backup
- Length of passcode will be contentious within organizations
  - Should be designed to thwart attacker sufficiently for remote countermeasures to be issued
  - iOS 4 character PIN: 13 minutes to recover on average
- Consider alphanumeric passcodes for added entropy
- For BlackBerry, do not rely on device passcode alone for encryption
  - Use device passcode and device key

Device passcode alone will not thwart determined data access attempts against a lost or stolen device

Remote Wipe Strategies

- When lost, remote data wipe can be effective to limit data exposure
- For corporate devices, this is a simple calculation
- In BYOD deployments, remote wipe may not be an option to end-user
- Container MDM controls works well here, wiping only container data
  - Can be applied much more liberally, wiping corporate data following policy violation, etc.

It is common for end-users not to want to believe the mobile device is lost, delaying the reporting process and exposing the organization. A removed SIM card largely mitigates remote wipe effectiveness.

Encouraging Lost Device Reporting

- Educate users to a policy to report lost devices right away
- Promote policy through posters and other media in the organization
- Help users recognize that the penalty for lost devices is minimized when reported quickly

Outline

- What is SANS SEC575?
- Mobile Device Loss
- Mobile Device Backup Recovery
- Bypassing PIN Authentication
- Mitigating the Impact of Lost Devices
- Mobile Device Security

Mobile Device Security

- A growing skill set requirement for small and large organizations
- Required for deployment and rollout
  - Also required for on-going application analysis, incident response, maintenance, monitoring
- Rapidly changing area of information security
  - (Many past problems are repeated)
- Great opportunity for professional career development
  - Plus, it's a lot of fun, and we get to mess around with cool toys

Essential Skill Development

- Developing policies that meet business needs and user acceptance
- Adoption of security controls to mitigate attacks and common threat scenarios
- Analysis of network activity from mobile devices and applications
- Exploitation of wireless client implementation flaws
- Manipulation of mobile device apps and supporting servers

SANS Security 575: Building the skills necessary for effective mobile device security

Resources

- SANS SCORE Mobile Device Checklist - www.sans.org/score/checklists.php
- Plist Editor for Windows - www.icopybot.com
- iPhone Data Protection Tools - code.google.com/p/iphone-dataprotection
- Elcomsoft EPPB - www.elcomsoft.com/eppb.html
- Magic Berry IPD Reader - menastep.com
- SQLiteSpy - www.yunqa.de/delphi/doku.php/products/sqlitespy

Up-to-date information about SEC575 - www.sec575.org

SANS Security 575: Mobile Device Security and Ethical Hacking

- SANS Conference Events
  - VA Beach 8/20 - 8/25 (Joshua Wright)
  - Las Vegas 9/17 - 9/22 (Joshua Wright)
  - Baltimore 10/15 - 10/20 (Joshua Wright)
  - London 11/26 - 12/1 (Raul Siles)
- SANS vLive and OnDemand delivery coming soon

Thank You For Attending. Questions?