iPad/iPhone Security Awareness

for individuals and business

Erik Couture

GIAC (GSEC GCIH GCIA GCFA GCNA)

August 2011

What's the threat?

- Threats to the device (data at rest)
  - Physical Theft
  - Remote Access
  - Remote Code Execution (malware)
- Threats to the comms channel (data in motion)
  - Wi-Fi attacks
  - GSM attacks
  - Email sniffing
  - Web traffic sniffing and MITM

What can a user do?

- Secure the data at rest
  - Use a PIN code and set lockscreen timeout
  - Stored data Encryption (iOS 4+)
  - Enable remote-wipe capability (iOS 4.2+)
- Secure the data in motion
  - Don't use untrusted Wi-Fi, or at least…
  - Use secure VPNs.
  - Turn on secure SSL email

What can the Enterprise do?

- Centralized security configuration and provisioning
  - 3rd party iDevice management
    - AirWatch
    - Sybase Afaria
    - McAfee Mobility Management
    - many more…
- Limit access to network corporate network resources to managed devices only
- Employ secure VPNs to protect data, end-to-end

A note on Jailbreaking

- Def'n – **Jailbreaking**: Unlocking of the phone to allow non-official software to run
- Why do people do it? Primarily to pirate software
- Usually accomplished by exploiting an iOS vulnerability
- Risks
  - Allows *all* non approved software (incl. malware) to run
  - Opens 'backdoor' with default password which enables a remote hacker to subvert the phone
- Def'n - **Irony**: Hacking your phone makes it easier to get your phone hacked