OWASP Mobile Top 10

OWASP Korea Day 2013

July 13, 2013

Beau Woods
http://beauwoods.com
@beauwoods

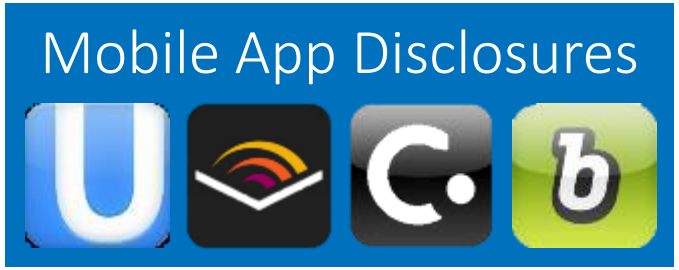
About Me

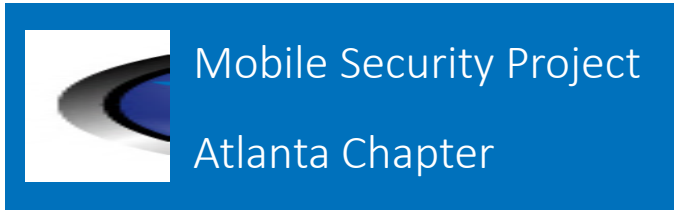
35 yo American

In S. Korea since February

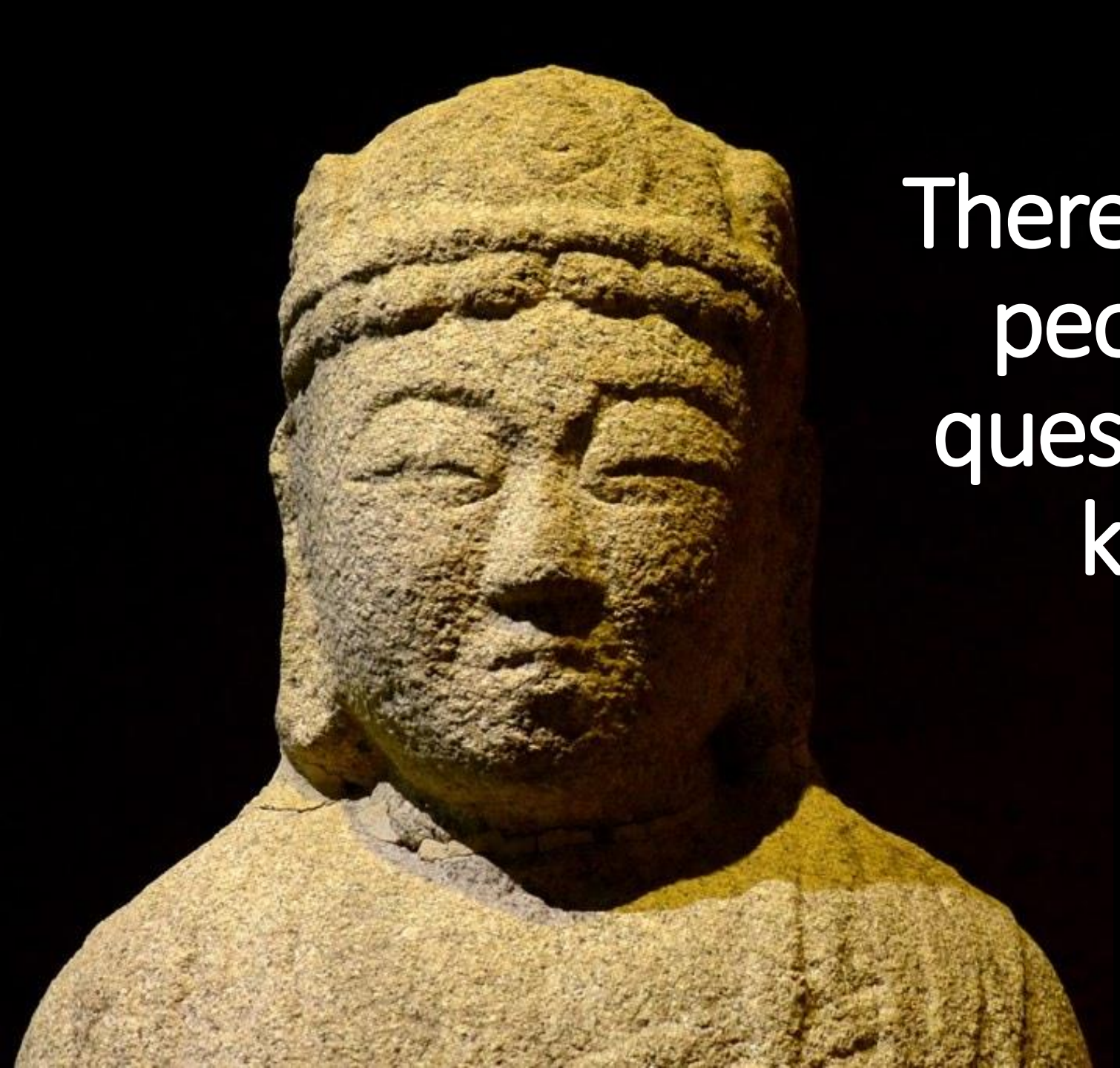
17 years in IT & Information Security

Recovering Technologist





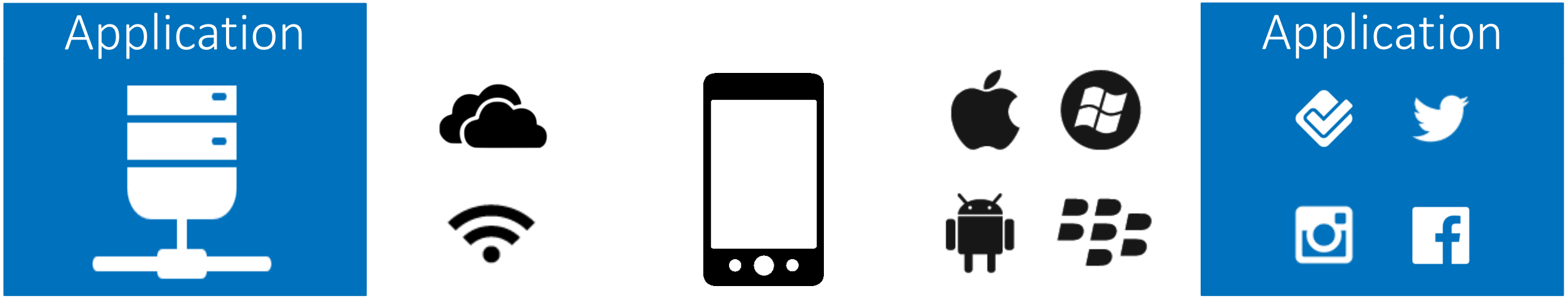
Passionate about travel, security…and Korean food



There are two types of people who have no questions. Those who know nothing and those who know everything.

-Korean Proverb

Mobile Elements



Server Network Hardware Platform Client

Mobile Considerations

	Use models	Capabilities	Hardware	Platform
Mobile Devices	Always on Always connected Omnipresent	Communications Limited resources Highly variable	Extensive RF & SSD Highly variable Not upgradable	Highly variable Limited options Variable security
Traditional Devices	Frequently off Disconnected Location-bound	Many resources Robust platform Well documented	Limited RF & HDD Highly variable Highly upgradable	Standardized Well understood Robust security

OWASP Mobile Top 10 Risks

M1 Insecure Data Storage

M2 Weak Server Side Controls

M3 Insufficient Transport Layer Protection

M4 Client Side Injection

M5 Poor Authorization and Authentication

M6 Improper Session Handling

M7 Security Decisions via Untrusted Inputs

M8 Side Channel Data Leakage

M9 Broken Cryptography

M10 Sensitive Information Disclosure

Alpha Documentation

Mobile Security Project

- Top 10 Risks
- Top 10 Controls
- Threat Model
- Testing Guide
- Tools
- Secure Development

M1 Insecure Data Storage

Sensitive data

Authentication data
Regulated information
Business-specific information
Private information

Examples

Recommendations

Mobile Controls 1, 2 & 7

Business must define, classify, assign owner & set requirements
Acquire, transmit, use and store as little sensitive data as possible
Inform and confirm data definition, collection, use & handling

Protections

1. Reduce use and storage
2. Encrypt or hash
3. Platform-specific secure storage with restricted permissions

M2 Weak Server Side Controls

Mobile App Servers
RESTful API
SOAP
Web Service
Web XML

Recommendations

Mobile Controls 5 & 6

Always validate input
Don't trust the client
Harden mobile app servers & services
Beware information disclosure
Understand host & network controls
Perform integrity checking regularly

OWASP Top 10 Web Application Risks 2013

A1 Injection
A2 Broken Authentication and Session Management
A3 Cross-Site Scripting (XSS)
A4 Insecure Direct Object References
A5 Security Misconfiguration
A6 Sensitive Data Exposure
A7 Missing Function Level Access Control
A8 Cross-Site Request Forgery (CSRF)
A9 Using Components with Known Vulnerabilities
A10 Unvalidated Redirects and Forwards

M3 Insufficient Transport Layer Protection

Impact

Expose authentication data

Disclosure other **sensitive information**

Injection

Data tampering

Examples

Recommendations

Mobile Controls 3

Use platform-provided cryptographic libraries

Force strong methods & valid certificates

Test for certificate errors & warnings

Use pre-defined certificates, as appropriate

Encrypt sensitive information before sending

All transport, including RFID, NFC, Bluetooth Wifi, Carrier

Avoid HTTP GET method

M4 Client Side Injection

Impact

App or device compromise

Abuse resources or services (SMS, phone, payments, online banking)

Extract or inject data

Man-in-the-Browser (MITB)

Recommendations

Mobile Controls 9

Always validate input

Don’t trust the server

Harden mobile app clients

Beware information disclosure

Perform integrity checking regularly

M5 Poor Authorization and Authentication

Impacts

Account takeover

Confidentiality breach

Fraudulent transactions

Examples

Most common methods

Account name

Password

Oauth

HTTP Cookies

Stored passwords

Unique tokens

Recommendations

Mobile Controls 4

Use appropriate methods for the risk

Use unique identifiers as additional (not primary) factors

Differentiate between client vs. server authentication

Ensure out-of-band methods are truly OOB (this is hard)

Hardware-independent identifiers

M6 Improper Session Handling

Impacts

Account takeover

Confidentiality breach

Fraudulent transactions

Most common methods

Oauth

HTTP Cookies

Stored passwords

Unique tokens

Recommendations

Mobile Controls 4

Allow revocation of device/password

Use strong tokens and generation methods

Consider appropriate session length (longer than web)

Reauthenticate periodically or after focus change

Store and transmit session tokens securely

M7 Security Decisions via Untrusted Inputs

Description

Reliance on files, settings, network resources or other inputs which may be modified.

Examples

DNS settings
Cookies
Configuration files
Network injection
Mobile malware
URL calls

Recommendations

Validate settings and files with checksums
Validate all inputs
Encrypt communications
Ensure trusted data sources

M8 Side Channel Data Leakage

Side channel data

Caches

Keystroke logging (by platform)

Screenshots (by platform)

Logs

Examples

Recommendations

Mobile Controls 1, 2, 3, 6 & 7

Consider server-side leakage

Reduce client-side logging

Consider mobile-specific private information

Consider platform-specific data capture features

Securely cache data (consider SSD limitations)

M9 Broken Cryptography

Cryptography

…is not encoding

…is not obfuscation

…is not serialization

…is best left to the experts

"The only way to tell good cryptography from bad cryptography is to have it examined by experts."

-Bruce Schneier

Examples

Recommendations

Mobile Controls 1, 2 & 3

Use only well-vetted cryptographic libraries

Understand one-way vs. two-way encryption

Use only well-vetted cryptographic libraries (not a typo)

Use only platform-provided cryptographic storage

Use only well-vetted cryptographic libraries (still not a typo)

Protect cryptographic keys fanatically

Use only well-vetted cryptographic libraries (seriously - always do this)

M10 Sensitive Information Disclosure

Side application data

API or encryption keys

Passwords

Sensitive business logic

Internal company information

Debugging or maintenance information

Recommendations

Store sensitive application data server-side

Avoid hardcoding information in the application

Use platform-specific secure storage areas

Case Study

M1 Insecure Data Storage

- Account number & passcode stored in flat text file

Risks & mitigating factors

- Passcode not used for other systems
- App contained and accessed sensitive and private information

Case Study

M5 Poor Authorization & Authentication

- Account name and password in plain text
- Used HTTP GET method (logged to server)

M8 Side Channel Data Leakage

- Logged password to client and server

M9 Broken Cryptography

- First attempt to fix issue obfuscated password

Risks & mitigating factors

- Same password used for web application
- Password reuse likely
- Stored password securely

Case Study

M1 Insecure Data Storage

- Account number & password stored in flat text file

Risks & mitigating factors

- App contained and accessed private information
- Password reuse likely
- App used by Arab Spring protests

DIY Vulnerability Discovery

- Explore files on mobile devices and backups
- Search for passwords
- Sniff network connections
- Downgrade SSL

OWASP Resources

- WebScarab
- GoatDroid
- iGoat
- MobiSec
- iMas
- Mobile Testing Guide

Beau Woods

http://beauwoods.com

@beauwoods