OWASP Mobile Project 2012 Goals

All,

This is a starting point. Please add whatever you think is missing. Want to get this right so we can start improving how stuff is communicated through the project. Need to make it easier for people to contribute. Plan to publish this to the wiki for everyone to see and most importantly, contribute to.

This is basically a list that should grow of everything we plan to achieve at <some point> in time. This is not prioritized yet, but must be so that we can focus our resources on attacking the most important things first.

1) Engage with groups:

carriers

software development groups

app store curators

device manufacturers

mobile OS companies/developers

framework developers

academic research community

ENISA

GSMA

Government

2) Besides create documents, pretty top 10 lists, tools, and all of that....what do we want to ACHIEVE?

Raise awareness.

3/24 Don W: maybe write an article in Security publication/blog promoting accomplishments

Bring visibility to the right issues, not FUD or product hype (sorry product peeps ;-))

Pull together smart people to solve problems across verticals, continents, etc.

Revisit Top 10 Mobile Risks and update with current threats

2/17/13 Don W. is this still managed by Jason Haddix? as if so would be good to setup shared document for community input. I updated this t reflect the Top 10 Mobile Risks name as it appears on the site. Do we maybe want to add brief description of the threats following the list? If so and Jason still manages this I would like to be included when the doc is shared out.

3) Get someone to step up to take ownership over:

Wiki updates - Jim Manico will do this

4) To complete or work on:

Formal Top 10

JM- This would be a Top 10 Risks based on the previous year’s Top 10...OR, we focus our efforts on exploring the overall threat surface a bit more. I think high quality, living cheat sheets based on the Top 10 would be more useful to the world. Pick an issue from the Top 10, write an Android, IOS, RIM, etc cheat sheet on how to identify it and mitigate it. Very useful, easier to recycle material + extend.

Top 10 Controls Document

Giles Hogben?

This needs tons of examples and will take quite a bit of effort to nail down.

Cheat Sheet Series (Mike Zusman = owns this)

Authentication Cheat Sheet

How should I authenticate users in my mobile application?

Should I store credentials on the device? If so, how?

Dangers of Rooting/Jail breaking Cheat Sheet (Sukie M, Talha Tariq, , Brandon Clark and Billy Graham - completed and released)

What is “jail breaking”?

Why can it be dangerous?

What if a user jail breaks a device with my application on it?

Sensitive Data Cheat Sheet - all platforms

Should I store sensitive data on the device?

How do I store data securely on a device? (Sukie M, Talha Tariq, Brandon Clark and Billy Graham - Peer Review)

Infrastructure Cheat Sheet

Should I use REST, RESTful, HTTP, SOAP?

Platform Specific - each platform sub-bullet is a cheat sheet

Android

Manifest (Jack Mannino)

https://docs.google.com/document/d/1m\_APGfVWt1bsPs\_XWY4I2TaBIJUYUg2hxQOf7ERH9dM/edit

Android Dynamic Analysis Cheat Sheet

Secure IPC Cheat Sheet

Android Static Analysis Cheat Sheet

Android Decompilation & Byte Code Static Analysis Cheat Sheet

iOS (Sukie M, Talha Tariq, Brandon Clark and Billy Graham - ownership)

Key Chain Cheat Sheet (Sukie M, Talha Tariq, and Billy Graham - ownership)

iOS Dynamic Analysis Cheat Sheet (We will synthesize what the ‘Testing Guides’ team comes up with here)

iOS Static Analysis Cheat Sheet (We will synthesize what the ‘Testing Guides’ team comes up with here)

iOS Secure Coding Cheat Sheet (Sukie M, Talha Tariq, and Billy Graham - ownership)

Windows Phone

RIM

Continue Supporting Project Tools

GoatDroid

MobiSec

?? new ones

Tools List- aggregate lots of good tools, testing tricks, and papers -- Swapnil Deshmukh is ready to work on this. -- Tom Eston also has tools/papers to contribute

Testing Guides

Mobile Testing Methodology - iOS

https://docs.google.com/document/d/1PJZOdXtqjLErCNpZ2W8aDCrIszmNPTxHVJ\_vx2SqpwQ/edit

Mobile Testing Methodology - Android

https://docs.google.com/document/d/1vReyi5fwr6UOxhE8WDqzho\_8BecP8UGLtKJCzcAOIrI/edit

Mobile Testing Methodology - Windows Phone

https://docs.google.com/document/d/1Fl1kac2V2\_YEfs5YgaRadWPCKpbltCeAqKauLDy2Scw/edit

Static

Dynamic -- Swapnil Deshmukh is ready to work on this.

-- Tom Eston has a detailed testing methodology to contribute (platform agnostic). I’d like to get others interested in working on this (Swapnil?) together soon to help formalize.

Threat Model -- Tom Eston will take ownership

This is a very high priority to complete IMHO. Would love for someone to take ownership of this =)

Mobile Device Management -- Tom Eston has information to contribute around free and/or low cost MDMs + list of commercial solutions

Curation Best Practices

Mobile Telecommunications (that affect development)

Carrier services

"In Scope" technologies

tablets

smart phones

?? entertainment (smart tvs)

?? cars

mobile payment devices -- Swapnil Deshmukh has worked on this (passive NFC) and has a document that he is working on and will post it soon.

Platform Specific Information

Permissions + security models

APIs of interest

Examples of vulnerable code

authentication

authorization

data at rest

session management

injection

encryption

algorithms

APIs

Identify roadmap to building Mobile ESAPI-like project

##############################################################################

Prioritized...what do we do first, second, third, etc. Why?

<don w comment>

0) Could just be me yet when accessing the OWASP mobile landing page via IE browser I noticed the site redirects to HTTPS and users (at least for me) are presented with the annoying warning below. So it appears there may be at least one element on the page which is ‘http:’. I briefly checked yet did not locate the culprit(s).

Anyone get this error?

</don w comment>

1) Complete in-depth, detailed mobile threat model and publish it

we started this last year but came nowhere near close to finishing it

Comments from Mike Boberski

My #1 suggestion is to update the mobile top 10 using an architecture not metrics approach as we’ve chatted briefly (i.e. take my suggestions and make them look right to your eyes), then create a set of project artifacts that are exactly equivalent to Dave’s top ten in terms or presentation and content, and basically defer anything else for now.

Then, put out a RFC for industry comment (leaders list, e.g. WASC mail list, etc.) with a relatively short and finite time period, and then perhaps bend Dave’s ear a little bit for suggestions on how to promote a final release.

Then, perhaps bend Dave’s ear further for his suggestions as to how to go about getting an OWASP home page blue banner link to “Top Ten (Mobile)”.

Generally, mobile appears to be “what’s next” after web applications. I’m not sure if the dropping of “web” from “the free and open application security community” was a great idea (NIST, NSA, DISA are where I look for non-web app stuff for example, OWASP can’t compete with those sources), but someone elsewhere decided to dilute OWASP’s focus in this way, so why not see if they meant it, in a productive way. A mobile top ten has potential and you’ve got a worked example with the OWASP Top 10 2010.

FWIW. I can maybe help out a little bit.

– Mike

//Suggestions for Top 10 Modifications

One minor refinement looking over my note below again, I’d perhaps delete #6 in trade for adding SQL injection as the new #9 or 10.

1. CWE-506: Embedded Malicious Code

· An Android example: Installed apps of unknown pedigree.

2. CWE-442: Web Problems

· An Android example: Ajax apps running on the mobile browser.

· Additional notes: Yes, broad, but: I think it’s not well understood that there aren’t only “apps” (and associated potential issues) and a full-fledged web browser (and associated potential issues), there are both (and associated potential issues of having both). And all the potential mobile middleware issues. And all the potential associated enterprise app and web service issues.

3. CWE-357: Insufficient UI Warning of Dangerous Operations.

· An Android example: for enterprise apps, for policy management applications, the user workflow to bootstrap a device into a configuration.

4. CWE-310: Cryptographic Issues

· An Android example: data at rest and in transit on devices depends on crypto being present and also working correctly. FIPS 140-2...

5. CWE-19: Data Handling

· An Android example: Another broad one, I think out of necessity along the lines of the extended comment above.

6. CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)

· An Android example: Calls from Ajax applications in the browser to exposed managed code.

7. CWE-497: Exposure of System Data to an Unauthorized Control Sphere

· An Android example: Calls from Ajax applications in the browser to exposed managed code.

8. CWE-470: Use of Externally-Controlled Input to Select Classes or Code

· An Android example: Calls from Ajax applications in the browser to exposed managed code.

9. CWE-770: Allocation of Resources Without Limits or Throttling

· An Android example: Broadcast receivers.

10. CWE-120: Classic Buffer Overflow

· An Android example: C/C++ libraries called from app code using JNI.

– Mike

//END OF MIKE BOBERSKI COMMENTS

Appsec DC Mobile Working Session