OWASP

Open Web Application Security Project

OWASP Mobile Top Ten 2015 Strategic Roadmap

Agenda

- OWASP Mobile Top Ten Context
- Key Goals / Strategies for 2015
- Produce a final roadmap of Objectives / Tactics for 2015

CONTEXTUAL OVERVIEW

Important Definitions

- Goals – Broad primary outcomes
- Strategy – Approach taken to achieve a goal
- Objective – A measurable step taking to achieve a strategy
- Tactic – A tool that is useful to achieve an objective (associated with a goal)

OWASP Mobile Top Ten 2014

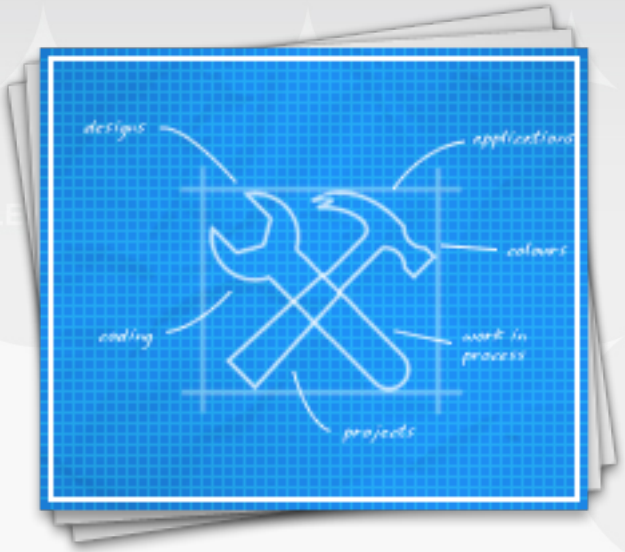
- Goals of 2014:
  - [G1] Guide technical audiences around mobile appsec technical risks;
    - Associated Strategies:
      - [S1] Publish a Mobile Top Ten list that prioritizes what organizations should address for mobile app risks
      - Associated Objectives:
        - [O2] Group data logically into 10 categories
        - [O4] Publish Top Ten 2014 list in April 2014
  - [G2] Establish the group as an authoritative source for mobile technical guidance that is trustworthy to technical communities
    - Associated Strategies:
      - [S2] Follow an evidence-based (rather than purely prescriptive) approach to recommendations
      - Associated Objectives:
        - [O1] Generate / gather vulnerability data by January 2014
        - [O3] Gather feedback from OWASP community over 90 days (supports S1+S2)

Successes of 2014

- Objective Outcomes for 2014:
  - Data was successfully gathered [O1] by January 2014;
  - Data was successfully grouped and presented [O2] at AppSec California 2014;
  - List was finalized [O4] in August 2014
    - Feedback window was not acted upon within 90-day window [O3]; hence delay of finalization
- Strategic Outcomes for 2014:
  - Publication of list [S1] was achieved;
  - An evidence-based approach to data collection [S2] was executed
- Goal Outcomes for 2014:
  - Guiding technical audiences around mobile appsec risk [G1] was achieved
  - Attaining source legitimacy [G2] was achieved through execution of methodology

Lessons Learned from 2014

- Ways to improve goals:
  - Goal of providing clear guidance [G1] was a partial success
    - Execution of grouping vulnerabilities [O2] was difficult within group; attaining consensus was difficult
    - Difficulty in understanding who exactly the primary consumer of the list is
  - Goal of establishing source legitimacy [G2] was a partial success
    - General consensus within group is that data collection objective [O1] was not executed well enough (not enough data sources)
    - Execution of feedback incorporation [O3] was not done within agreed upon timeframe
    - Missing strategies around encouraging other OWASP projects to participate



OWASP MOBILE TOP TEN 2015 STRATEGIC ROADMAP

Primary Goals

- Are the 2015 goals the same as 2014?

  [G1] Guide audiences around mobile appsec risks

  - Who is our audience for 2015?
    - Do we want to stick to technical or include/switch to business risk?

  [G2] Establish the group as an authoritative source for mobile risk guidance that is trustworthy to broader communities

  - What does an authoritative source look like?
  - What does a trustworthy source look like?

- Are there any new goals / outcomes not already mentioned here?
  - [G3] Gain adoption as a security standard

Primary Strategies

- Do we need to add new strategies to support our 2015 goals?
  - New ways to improve guidance [G1]:
    - [S3] Understand the audience in greater detail;
    - [S4] Communicate more specifically to a particular audience rather than be a generalist?
    - [S5] Clarify how the data groupings occurred?
    - [S6] Clarify how the prioritization occurred?
  - New ways to improve legitimacy [G2]:
    - [S7] Increase number of data sources
    - [S8] Expose sanitized form of data to audience
    - [S9] Expose data collection methodology
  - Ways to increase adoption [G3]:
    - [S10] Cross-promote with other OWASP projects
      - OWASP Top Ten; DroidGoat; iGoat
      - Promote tools that identify Mobile Top Ten risks
    - [S11] Associate with other sources outside of OWASP
    - [S12] Show relevance by highlight attacks known to be part of Mobile Top Ten

Primary Objectives

- Do we tweak existing objectives?
  - [O1] Generate / gather vulnerability data
  - [O2] Group data logically into 10 categories
  - [O3] Gather feedback from OWASP community over 90 days
  - [O4] Publish Top Ten 2014 list in April 2014

- New objectives?
  - [O5] Conduct survey of the potential audience
    - Supports [S3]
  - [O6] Publish a cheat-sheet series for final 2015 list;
    - Supports [S4]
  - [O7] Publish videos that illustrate attack vectors associated with particular risks;
    - Supports [S4];
  - [O8] Declare grouping and prioritization strategy
    - Supports [S5] [S6]
  - [O9] Publish audience-specific editorials on the final list
    - Supports [S4]
  - [O10] Sanitize and publish data
    - Supports [S8];
  - [O11] Provide more open-source tools to evaluate exposure to Mobile Top Ten
    - Supports [S10];
  - [O12] Publish blog series that highlights particular attacks and relevance to Mobile Top Ten
    - Supports [S12];

Tweak Existing Tactics

- Do we need new tactics for existing objectives?
  - [O1] Generate / gather vulnerability data
    - Change ‘sales’ tactics to improve participation by industry players
  - [O2] Group data logically into 10 categories
    - Perform grouping using a pure risk or a pure vulnerability approach
    - Mimic OWASP Top Ten
    - Leverage another standard that is already widely adopted
  - [O3] Gather feedback from OWASP community over 90 days
    - Send out periodic reminders that the window is closing?

Conclusions

- A lot of great stuff happened in 2014
  - Greater participation
  - Finalized list
  - Greater adoption in industry
- There are many potential goals, strategies, objectives, and tactics that are possible for 2015.
  - These must be explicitly agreed upon to make for a smooth ride for everyone