Drivers for a Secure Mobile App Development Framework

Authors: Marijke Coetzee, Christoff Jacobs

Presenter: Christoff Jacobs, University of Johannesburg, toffie_cj@yahoo.com
• Christoff Jacobs
• Software developer
• +18 years software development experience
• Insurance, healthcare, stock trading, vehicle and banking
• Focus on mobile security and software development architecture and best practices
• Current PhD
1. Article introduction
2. Presenter
3. Presentation
4. The end
Introduction

• AI generated - Midjourney

• Using mobile, guardian, portal, end of the world
Introduction

- Pandemic implications
- Ubiquitous app deployment
- Trends in cybersecurity threats
- Urgency in security measures
- Methods of authentication
- Absence of standardized approaches
- Friction in software development
- Requisite specialization
- Limitations in existing frameworks
- Imperative for a secure development framework
Mobile app ecosystem (example)
Mobile app ecosystem

- The mobile application ecosystem
- Elevated risk factors
- Elements within the ecosystem
- Critical integration nodes
- Extending beyond user interface
- The centrality of security
- Validation through testing
- Deployment for customer use
- Facilitating network communication
- Exploring alternative approaches
Secure software development for mobile apps

- The lack of mobile application SDLC models
- Predominance of technical emphasis over lifecycle consideration
- Constraints of conventional SDLC methodologies
- Security predicaments within traditional SDLC
- Depletion of secure development frameworks
- Proliferation of generalized frameworks
- Advocacy for a holistic security lifecycle approach
Secure software development for mobile apps

- Recommendations on industry standards
- Myriad security imperatives
- Requisite for a coherent framework
Secure software development for mobile apps

<table>
<thead>
<tr>
<th><strong>NIST</strong></th>
<th><strong>OWASP</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST regulatory updates</td>
<td>OWASP’s significance in advancing mobile app security</td>
</tr>
<tr>
<td>NIST 800-163 framework</td>
<td>Emphasis on security aspects</td>
</tr>
<tr>
<td>Application security requirements</td>
<td>Thorough examination and constructive input</td>
</tr>
<tr>
<td>Customized mobile app security</td>
<td></td>
</tr>
<tr>
<td>NIST 800-218 SSDF</td>
<td></td>
</tr>
</tbody>
</table>
Secure software development for mobile apps

- **OWASP**
  - Vulnerability domains defined by MASVS
  - Endorsement by CREST alliance

- **MITRE ATT&CK**
  - MITRE's ATT&CK knowledgebase
  - Platform-specific security topics
  - Enhancing mobile app security expertise
  - Practical examples
Secure software development for mobile apps

- DEVSECOPS
  - DevSecOps overview
  - Key DevSecOps practices
  - Challenges in implementation
  - Identification of security drivers
  - Comprehensive approach
Security drivers for a secure software mobile software development framework

- Introduction -> mobile app ecosystem -> standard security frameworks
- Issues still exist in identifying security drivers for a secure mobile software development framework
Security drivers for a secure software mobile software development framework

1. Management of software developers for security
2. A structured security approval strategy for security vendors
3. Integrate security education into secure software development
4. Standardised secure software development practices and coding principles
5. A baseline set of standardised security mechanisms for mobile apps
6. Standardised threat modelling approach
Security drivers for a secure software mobile software development framework

7. Standardise testing schedule

8. Standardised mobile app vetting system for an industry

9. Regulated security reporting and collaboration
# Evaluation

## TABLE 1. COMPARISON OF SECURE DEVELOPMENT FRAMEWORKS AND SECURITY DRIVERS

<table>
<thead>
<tr>
<th>Security drivers</th>
<th>NIST</th>
<th>OWASP</th>
<th>MITRE</th>
<th>DEVSECOPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of software developers for security</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>A structured security approval strategy</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrate security education for secure software development</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Standardised secure software development practices and coding principles</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A baseline set of standardised security mechanisms for mobile apps</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standardised threat modelling approach</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standardise testing schedule</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Standardised mobile app vetting system for an industry</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulated security reporting and collaboration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Customization for specific industries
• Identification of research gap
• Security Driver evaluation
• Robustness of OWASP

• NIST’s contribution
• MITRE ATT&CK's Unique Perspective
• Emphasis on DevSecOps
• Critical insights from framework comparison
• Prospects for future framework development
Conclusion and future work

• Intricacies within the mobile ecosystem
• Dilemmas encountered in security mechanism implementation
• Limitations of current frameworks
• Research contribution and prospects for future endeavors
The end