Prioritizing Trust while Creating Applications

Jennifer Davis, Cloud Advocate
she/her

@sigje
Trust
https://haveibeenpwned.com/
Agenda

• Establish Common Context
• Build Foundations
• Advancing Principles
Confidentiality

Availability

Integrity
Bug versus Flaw
Motivations

- Financial Gain
- Espionage/Strategic Gain
- Fun/Ideology/Grudge
Build Foundations

- 78% vulnerabilities in indirect dependencies
- 37% of open source developers no security testing in CI
- 54% docker image no security testing
- Top 10 docker images contain > 30 vulnerable system libraries

Source: https://snyk.io/opensourcesecurity-2019/
#WOCinTech Chat Attribution 2.0 Generic (CC BY 2.0)
• What can a user see? do?
• What information is logged?
• Approach for failed logins

OWASP: Application Security Verification Standard Project
Threat Modeling
Architectural Trade-offs
<table>
<thead>
<tr>
<th>Responsibility</th>
<th>On-Prem</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data classification &amp; accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client &amp; end-point protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity &amp; access management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application level controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- **Cloud Customer**
- **Cloud Provider**
Testing Code
Static Code Analysis
static OSSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                  uint8_t *signature, UInt16 signatureLen)
{
    OSSStatus err;
    ...

    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
    goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...

Source:
https://www.imperialviolet.org/2014/02/22/applebug.htm
Coding Standards

Lint/AmbiguousOperator:
   Enabled: true
Lint/AmbiguousBlockAssociation:
   Enabled: true
Lint/AmbiguousRegExpLiteral:
   Enabled: true
Lint/AssignmentInCondition:
   Enabled: true
Layout/BlockAlignment:
   EnforcedStyleAlignWith: start_of_block
   Enabled: true
Lint/CircularArgumentReference:
   Enabled: true
Layout/ConditionPosition:
   Enabled: true
Lint/Debugger:
   Enabled: true
Layout/DefEndAlignment:
   Enabled: true
Lint/DeprecatedClassMethods:
   Enabled: true
Secure Code Reviews
Planning for Security Escalations

• Identify
• Assess
• Remediate
Incident Response Resource

- Building a Minimum Viable Response Plan: jhand.co/CreateResponsePlan
Leverage your platform's services
Recognize your platform's limits
Discovery

Monitor

Development

Deploy

Build

Release
Advancing Principles
Bug Bounty Programs
Capture the Flag (CTF)

- CTF with Google
- CTF Circle - CTF distributed team for Nonbinary Folks and Women
Red Team Exercise

“Fundamentally, if somebody wants to get in, they’re getting in...accept that. What we tell clients is: Number one, you’re in the fight, whether you thought you were or not. Number two, you almost certainly are penetrated.

- Michael Hayden, Former Director of NSA & CIA
What's Next?

- Identify your security maturity
- Assess valuable practices
- Encourage learning security skills
- Incorporate feedback
- Update threat models
Security is everybody’s job!
Thank you

Email: jennifer@modernoperations.org

@sigje