Hunting for the next IoT
Your vulns are not a paradigm shift

OWASP LA
September 26, 2018

Brian Knopf @DoYouQA
BlueVoyant
About Me

- Managed Security Services Head, IoT @ BlueVoyant
- 20+ years in Security, QA, Development & IT
- My home is an IoT research lab with 150 devices
- Invented PKI replacement framework with real-time revocation
- Acquired by oneID, then Neustar, then Golden Gate Capital
- Presented at Black Hat, DEF CON, BSides LA, ISC West, IEEE, ISSA
- Previously
  - Sr. Director of Security Research at Neustar
  - CEO at BRK Security
  - Principal Security Advisor at Wink
  - Director of Application Security at Belkin & Linksys
  - Principal Test Architect, Office of the CTO at Rapid7
  - Director of QA at MySpace
Reality of Security

• You will NEVER have enough resources
• You will NEVER have enough time
• You will NEVER be done
  – Learning
  – Evaluating
  – Teaching
Hype vs Reality

• Don’t assume the hype around a product matches reality
  – This is secure
  – It makes you anonymous
  – No one can track you
  – Your messages are ephemeral

• Get Dev, QA, PM, AppSec, Ops, on the same page
  – What’s the risk?
  – What’s the load?
  – What’s the contingency?
Examples are everywhere
Tor - The Hype

Anonymity Online
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android.
Tor Browser Users Urged to Patch Critical ‘TorMoil’ Vulnerability

The Tor Project released a patch for a vulnerability that leaks the real IP addresses of macOS and Linux users of its Tor Browser.

The Tor Project released a patch for a vulnerability that leaks the real IP addresses of macOS and Linux users of its Tor Browser. The patch was issued late Friday and fixes a vulnerability found in Tor Browser version 7.0.8. The patch is in an upgrade to Tor Browser 7.0.9.

Source: Tor Browser Users Urged to Patch Critical ‘TorMoil’ Vulnerability
Security

Tor(ched): Zerodium drops exploit for version 7 of anonymous browser

Bug allows malicious scripts to run even with protections active

By Shaun Nichols in San Francisco 10 Sep 2018 at 23:09

10 Sep 2018 at 23:09

Source: Tor(ched): Zerodium drops exploit for version 7 of anonymous browser
https://www.theregister.co.uk/2018/09/10/torched_zerodium_drops_exploit_for_version_7_of_anonymous_browser/
Crypto Currency – The Hype

It’s anonymous!

You can’t be tracked!

It’s all about the privacy!
# Crypto Currency – The Hype

<table>
<thead>
<tr>
<th></th>
<th>Monero</th>
<th>Bitcoin</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Founder</strong></td>
<td>Group of 7 core developers</td>
<td>Satoshi Nakamoto</td>
</tr>
<tr>
<td><strong>Release Date</strong></td>
<td>18 April, 2014</td>
<td>9 Jan 2008</td>
</tr>
<tr>
<td><strong>Release Method</strong></td>
<td>Crowdfunded group of 7 core developers</td>
<td>Genesis Block Mined</td>
</tr>
<tr>
<td><strong>Total Coin Supply</strong></td>
<td>18.4 Million XMR + 0.3 XMR/minute</td>
<td>21 Million</td>
</tr>
<tr>
<td><strong>Blockchain Protocol</strong></td>
<td>Proof of work</td>
<td>Proof of work</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td>Digital Currency</td>
<td>Digital Currency</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>Untraceable</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Trackable</strong></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Cryptocurrency Used</strong></td>
<td>Monero</td>
<td>Bitcoin(Satoshi)</td>
</tr>
<tr>
<td><strong>Cryptocurrency Symbol</strong></td>
<td>(XMR)</td>
<td>(BTC)</td>
</tr>
<tr>
<td><strong>Transaction Fee</strong></td>
<td>0.004-0.02 XMR/kB</td>
<td>Varies based on load on blockchain</td>
</tr>
<tr>
<td><strong>Algorithm</strong></td>
<td>CryptoNote</td>
<td>SHA-256</td>
</tr>
<tr>
<td><strong>Blocks Time</strong></td>
<td>120 seconds</td>
<td>at least 10 minutes</td>
</tr>
<tr>
<td><strong>Mining</strong></td>
<td>GPUs, CPU</td>
<td>Pools, ASIC miners</td>
</tr>
<tr>
<td><strong>Scalable</strong></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Source: https://medium.com/@harrypotter0/how-does-monero-work-17f18ea37652
Crypto Currency – The Reality

What if I told you

Cryptocurrencies are only private until they aren't, and then it's too late.

Source: https://www.secmeme.com/2018/03/the-blockchain-is-forever.html
The researchers first note that simple tricks allow an observer to identify some of the decoy mixins used to cover for a real coin being spent. In Monero’s first year, for instance, it allowed users to opt out of its privacy protections and spend coins with no mixins at all. (Today, Monero requires a minimum of four mixin decoys for every transaction.) The problem with that opt-out system: When an already spent and identified coin is later as a mixin, it can be easily plucked out of the mix to help identify the remaining coins. If that results in another coin being identified, and that coin is itself used as a mixin in a subsequent transaction, it can reduce the stealth of those later transactions, too.

The researchers also found a second problem in Monero’s...
IoT Devices – The Hype

The Home Security Experts

Security is all we do.
That’s why our expertise is unmatched.
Hacking The Doors Off: I Took Control Of A Security Alarm System From 5,000 Miles Away

Thomas Brewster  Forbes Staff

Security
I cover crime, privacy and security in digital and physical forms.

Source: Hacking The Doors Off: I Took Control Of A Security Alarm System From 5,000 Miles Away
IoT Devices – The Reality

SHODAN

TOTAL RESULTS
16

TOP COUNTRIES
United States 16

TOP SERVICES
HTTPS 8081 6
NAS Web Interfaces 1
HTTPS (8443) 8083 1

AT&T Services
Added on 2018-09-26 19:14:40 GMT
United States, Palo Alto
Details

HTTP/1.1 200 OK
X-Powered-By: PHP/5.2.14
Set-Cookie: PHPSESSID=885215d0729627f066287a82b668361e; path=/
Cache-Control: no-cache, must-revalidate
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: ...

HTTPS
Added on 2018-09-26 12:59:28 GMT
United States, San Jose
Details

HTTP/1.1 200 OK
Date: Wed, 26 Sep 2018 12:59:28 GMT
Server: Apache
Content-Type: text/html
Content-Length: 4725

<html>
<head><title>Dangers on the Ice Off the Coast of Labrador</title></head>

Source: https://www.shodan.io/search?query=bay+alarm
Browser Plugins

Browser Plugin Hype
• Make you more secure/efficient
• Improve the browsers abilities

Browser Plugin Reality
• Who controls the code for that plugin?
• What permissions does the plugin have?
• What happens when ownership is transferred?
Threat Model
What is a Threat Model?

- A way to assess risk of products
- Collaborative process for agreeing on highest risk areas
- Documentation of assessment at a specific point in time
- Should be a living document, with previous versions stored

This Photo by Unknown Author is licensed under CC BY-SA
Threat Model Process

1. Identify
2. Diagram
3. Mitigate
4. Validate

The process is cyclic, with each step leading to the next, and then back to the beginning.
Threat Modeling

• Think like an attacker
• Build defenses accordingly
• Start at the design phase, not testing
• Fits into the Security Development Lifecycle (SDL)
## Security Design Principals

<table>
<thead>
<tr>
<th>Principle</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open design</td>
<td>Assume the attackers have the sources and the specs.</td>
</tr>
<tr>
<td>Fail-safe defaults</td>
<td>Fail closed; no single point of failure.</td>
</tr>
<tr>
<td>Least privilege</td>
<td>No more privileges than what is needed.</td>
</tr>
<tr>
<td>Economy of mechanism</td>
<td>Keep it simple, stupid.</td>
</tr>
<tr>
<td>Separation of privileges</td>
<td>Don’t permit an operation based on a single condition.</td>
</tr>
<tr>
<td>Total mediation</td>
<td>Check everything, every time.</td>
</tr>
<tr>
<td>Least common mechanism</td>
<td>Beware of shared resources.</td>
</tr>
<tr>
<td>Psychological acceptability</td>
<td>Will they use it?</td>
</tr>
</tbody>
</table>
# Security Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Data is only available to the people intended to access it.</td>
</tr>
<tr>
<td>Integrity</td>
<td>Data and system resources are only changed in appropriate ways by appropriate people.</td>
</tr>
<tr>
<td>Availability</td>
<td>Systems are ready when needed and perform acceptably.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The identity of users is established (or you’re willing to accept anonymous users).</td>
</tr>
<tr>
<td>Authorization</td>
<td>Users are explicitly allowed or denied access to resources.</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Users can’t perform an action and later deny performing it.</td>
</tr>
</tbody>
</table>
## Threats and Security Properties

<table>
<thead>
<tr>
<th>Threat</th>
<th>Security Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Authentication</td>
</tr>
<tr>
<td>Tampering</td>
<td>Integrity</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Non-repudication</td>
</tr>
<tr>
<td>Information Disclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Availability</td>
</tr>
<tr>
<td>Elevation of Privilege</td>
<td>Authorization</td>
</tr>
</tbody>
</table>

From *Uncover Security Design Flaws Using The STRIDE Approach*, MSDN Magazine
# Data Flow Diagrams (DFDs)

<table>
<thead>
<tr>
<th>Item</th>
<th>Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Flow</td>
<td>One way arrow</td>
</tr>
<tr>
<td>Data Store</td>
<td>Two parallel horizontal lines</td>
</tr>
<tr>
<td>Process</td>
<td>Circle</td>
</tr>
<tr>
<td>Multi-process</td>
<td>Two concentric circles</td>
</tr>
<tr>
<td>Interactors</td>
<td>Rectangle</td>
</tr>
<tr>
<td>Trust Boundary</td>
<td>Dotted line</td>
</tr>
</tbody>
</table>

From *Uncover Security Design Flaws Using The STRIDE Approach*, MSDN Magazine
## Threats Affecting Elements

<table>
<thead>
<tr>
<th>Element</th>
<th>Spoofing</th>
<th>Tampering</th>
<th>Repudiation</th>
<th>Information Disclosure</th>
<th>Denial of Service</th>
<th>Elevation of Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Flows</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data Stores</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Processes</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Interactors</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Microsoft SD3+C

Secure by Design
- Secure architecture and code
- Threat analysis
- Vulnerability reduction

Secure by Default
- Attack surface area reduced
- Unused features turned off by default
- Minimum privileges used

Secure in Deployment
- Protection: Detection, defense, recovery, and management
- Process: How to guides, architecture guides
- People: Training
Case Study
Case Study: Wink

Before

• Some pentesting from outside resources
• Wink Hub rooted 1 month after shipping
• Developers were interested and willing to implement security
• Company bought in
Case Study: Wink

After

- Threat Models built by all devs
- Code reviews before launch
- Ongoing audits
- Bug bounty program
- Security contact site and email
- Vulns patched within hours on occasions
Case Study: Wink

Bug Bounty

• 1 full-time security staff (me)
• 1 product
• 26 well-known researchers
• 2-weeks (private)
• 14 unique submissions
• Total cost: $10k bounty + $4k fee + $1300 (for 26 devices) = $15,300
• Result: significantly more secure device
• We received 38 additional valid submissions in one week when public bounty
Case Study: Wink

The Massive Vuln — Delete All Hubs

• Found by @anshuman_bh
• Part of bug bounty program
• Could delete ALL Wink Hubs from all user accounts
• User was authenticated
• Hub was authenticated
• User belonging to that hub WAS NOT authenticated
• Patched in Prod in 1 HOUR
• @dakshxss found account takeover, also patched in 1 HOUR
Hello World

```python
>>> print("Hello World")
Hello World
>>> 
```
Securing the SDLC

- Implement Security Development Lifecycle
- Creating policies and procedures on how to secure code
- Training developers on secure coding techniques
- Training developers and QA on threat modeling
- Implementing SAST and DAST code scanning via automation
Conclusion

• No excuses
• Work with what you have
• Set the expectations appropriately
• Leverage other internal resources (Dev, PM, QA)
• Use threat models to catch vulns in the design phase
• Teach threat models, secure code, security testing
• Get Dev and PM to see the benefit of early detection
• Leverage external researchers
• Always thank researchers. DO NOT threaten them.
References

- DevOps.com – Threat Modeling Tools List
- Microsoft Threat Modeling Tool
- Microsoft Threat Modeling Web Applications
- Uncover Security Flaws Using the STRIDE Approach
  - http://bit.ly/MSDN-STRIDE (https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxZWN1cmVwcm9ncmFtbWluZ3xeDo0MTY1MmM0ZDI0ZjQ4ZDMy)
- Judicial Framework for Evaluating Network Investigative Techniques
- FBI NIT capabilities
- The Dark Web’s Favorite Currency Is Less Untraceable Than It Seems
  - https://www.wired.com/story/menbtc-privacy/
- Tor(ched): Zerodium drops exploit for version 7 of anonymous browser
Q & A