Hunting for the next IoT

Your vulns are not a paradigm shift

OWASP LA

September 26, 2018

Brian Knopf @DoYouQA

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

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

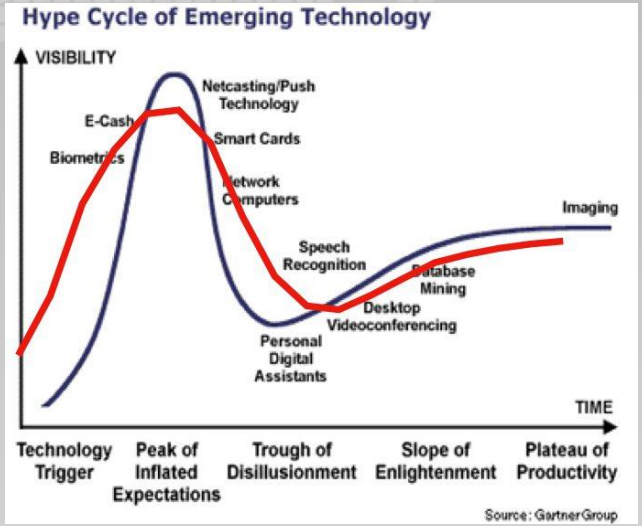
Security

Offense

Defense

Hype vs Reality

- Don't assume the hype around a product matches reality
- Too many recent examples
  - 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?



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

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 – The Reality

threat post Cloud Security / Malware / Vulnerabilities / Privacy

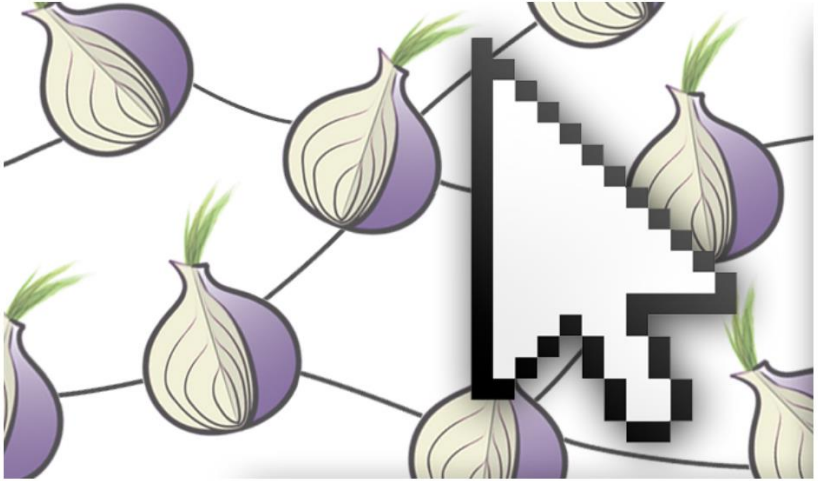
Tor Browser Users Urged to Patch Critical 'TorMoil' Vulnerability

Author:
Tom Spring

November 4, 2017
/ 7:00 am

1:30 minute read

Share this article:



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
https://threatpost.com/tor-browser-users-urged-to-patch-critical-tormoil-vulnerability/128769/

OWASP
Open Web Application Security Project

Tor – The Reality

The Register®
Biting the hand that feeds IT

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 5 SHARE ▼

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!

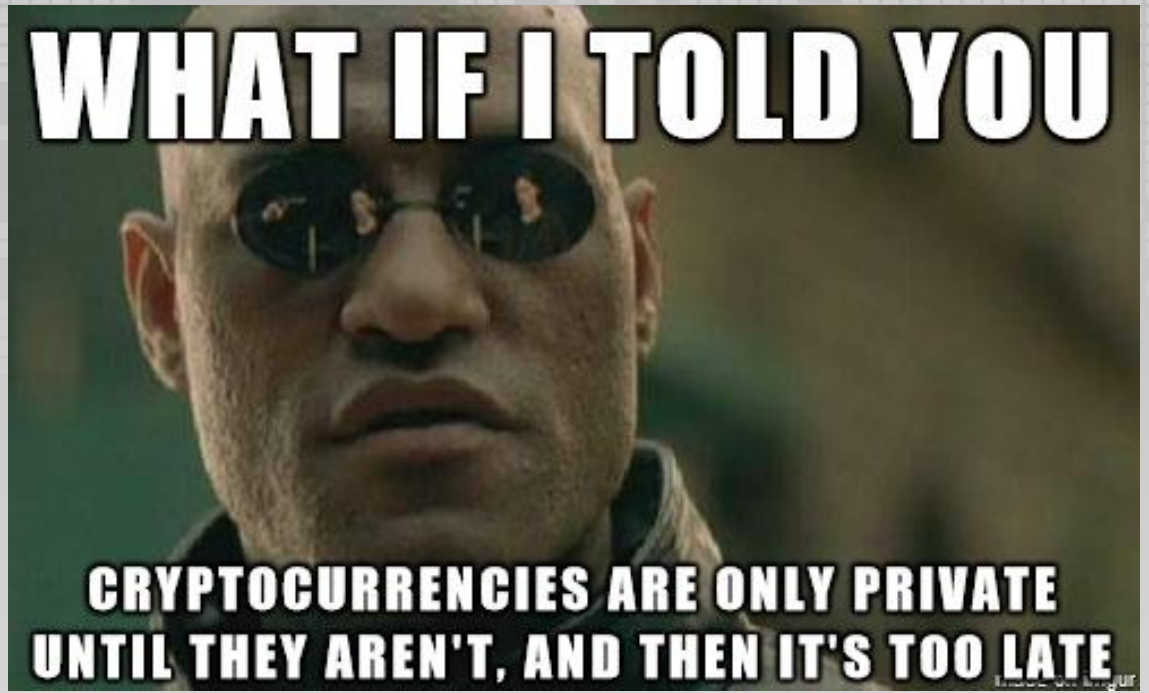
It’s all about the privacy!

Crypto Currency – The Hype

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

Source: https://medium.com/@harrypotter0/how-does-monero-work-17f18ea37652

Crypto Currency – The Reality



Source: https://www.secmeme.com/2018/03/the-blockchain-is-forever.html

Crypto Currency – The Reality

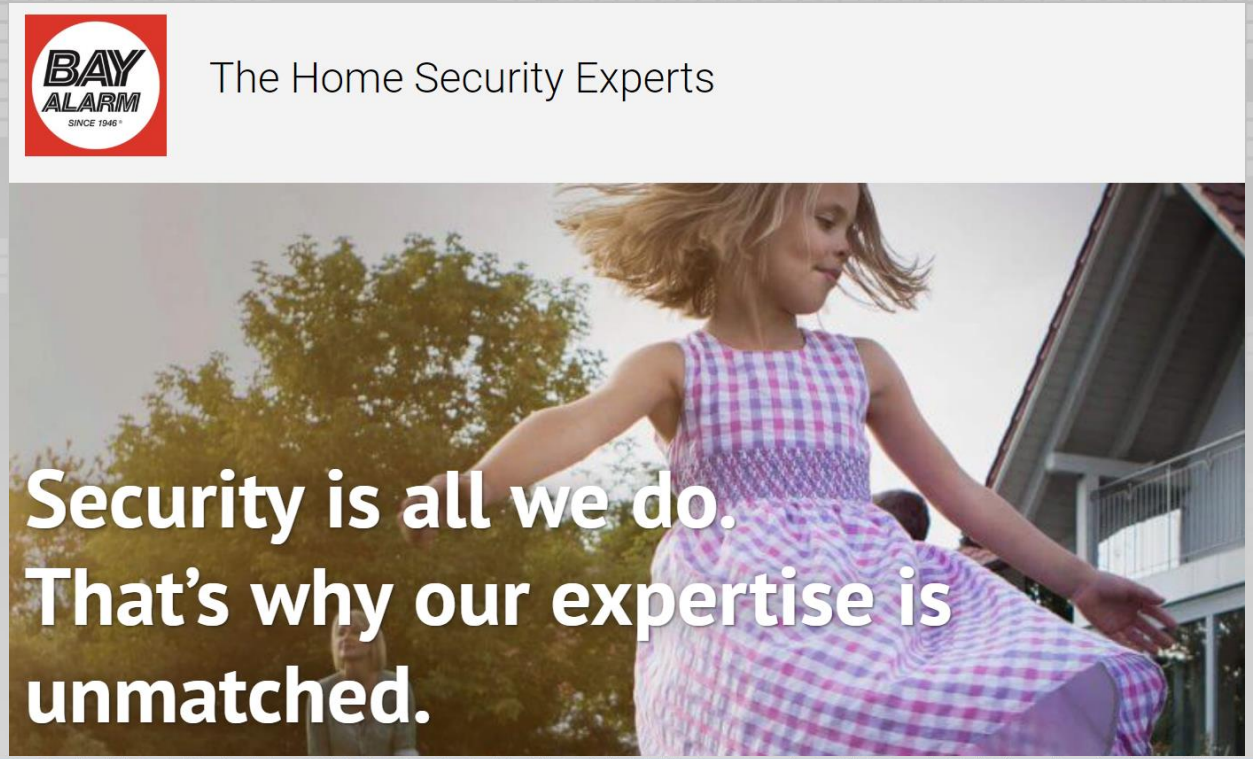
WIRED **The Dark Web's Favorite Currency Is Less Untraceable Than It Seems**

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.

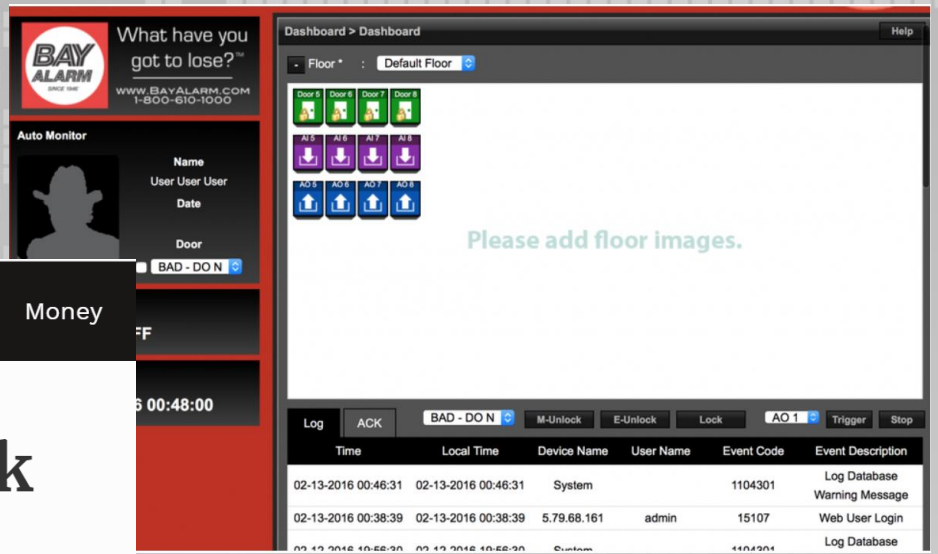
The researchers also found a second problem in Monero's

Source: https://www.wired.com/story/monero-privacy/

IoT Devices – The Hype



IoT Devices – The Reality



Forbes Billionaires Innovation Leadership Money

22,562 views | Feb 17, 2016, 10:26am

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
https://www.forbes.com/sites/thomasbrewster/2016/02/17/hacking-smart-security-alarms/

OWASP
Open Web Application Security Project

IoT Devices – The Reality

SHODAN | bay alarm | Explore | Developer Pricing | Enterprise Access | Contact Us

Exploits | Maps

TOTAL RESULTS

16

TOP COUNTRIES

United States	16

TOP SERVICES

HTTPS	7
8081	6
NAS Web Interfaces	1
HTTPS (8443)	1
8083	1

[redacted]

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=885215dd729627f006287a82b683361e; 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: ...
```

[redacted]

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

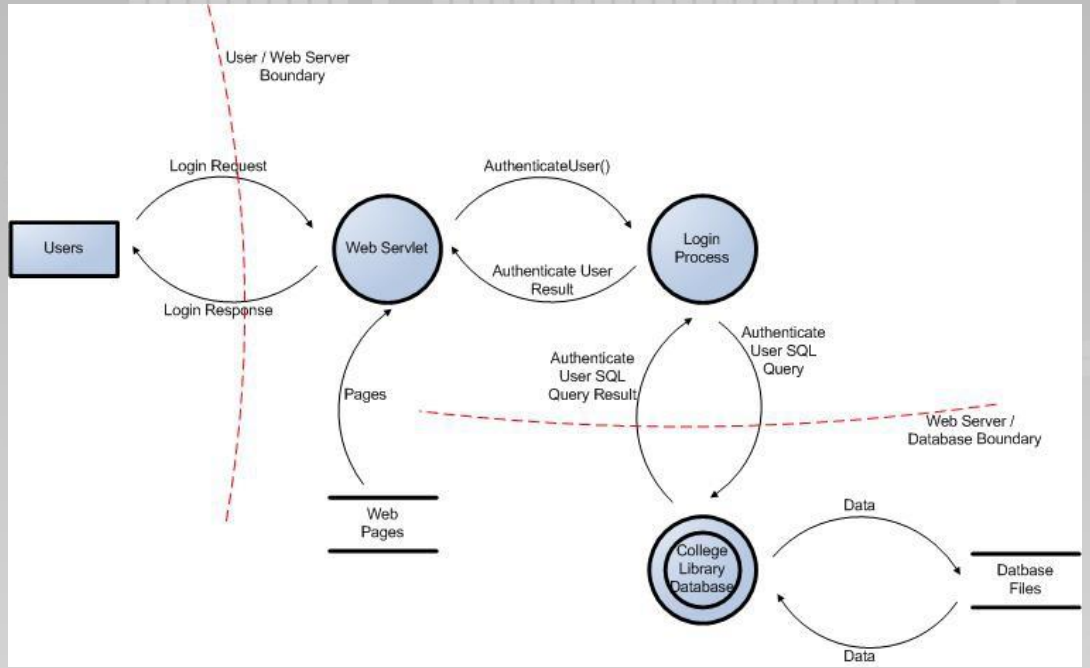
- Who controls the code for that plugin?
- What permissions does the plugin have?
- What happens when ownership is transferred?

OWASP
Open Web Application Security Project

Threat Model

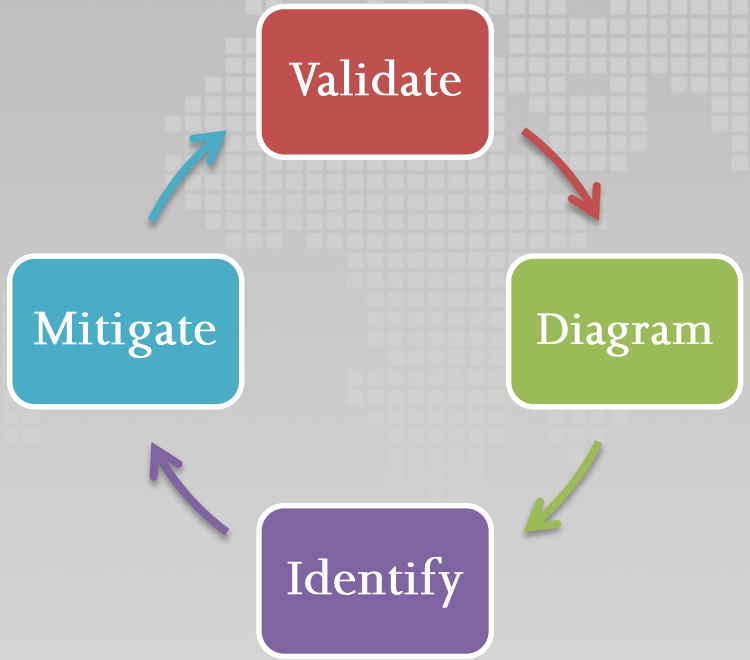
What is a Threat Model?

- 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



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

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

From *Uncover Security Design Flaws Using The STRIDE Approach*, MSDN Magazine

Security Properties

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

From *Uncover Security Design Flaws Using The STRIDE Approach*, MSDN Magazine

Threats and Security Properties

Threat	Security Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

From *Uncover Security Design Flaws Using The STRIDE Approach*, MSDN Magazine

Data Flow Diagrams (DFDs)

Item	Symbol
Data Flow	One way arrow
Data Store	Two parallel horizontal lines
Process	Circle
Multi-process	Two concentric circles
Interactors	Rectangle
Trust Boundary	Dotted line

From *Uncover Security Design Flaws Using The STRIDE Approach*, MSDN Magazine

Threats Affecting Elements

Element	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data Flows		X		X	X	
Data Stores		X		X	X	
Processes	X	X	X	X	X	X
Interactors	X		X			

From *Uncover Security Design Flaws Using The STRIDE Approach*, MSDN Magazine

Microsoft SD3+C

Secure by Design

- Secure architecture and code
- Threat analysis
- Vulnerability reduction

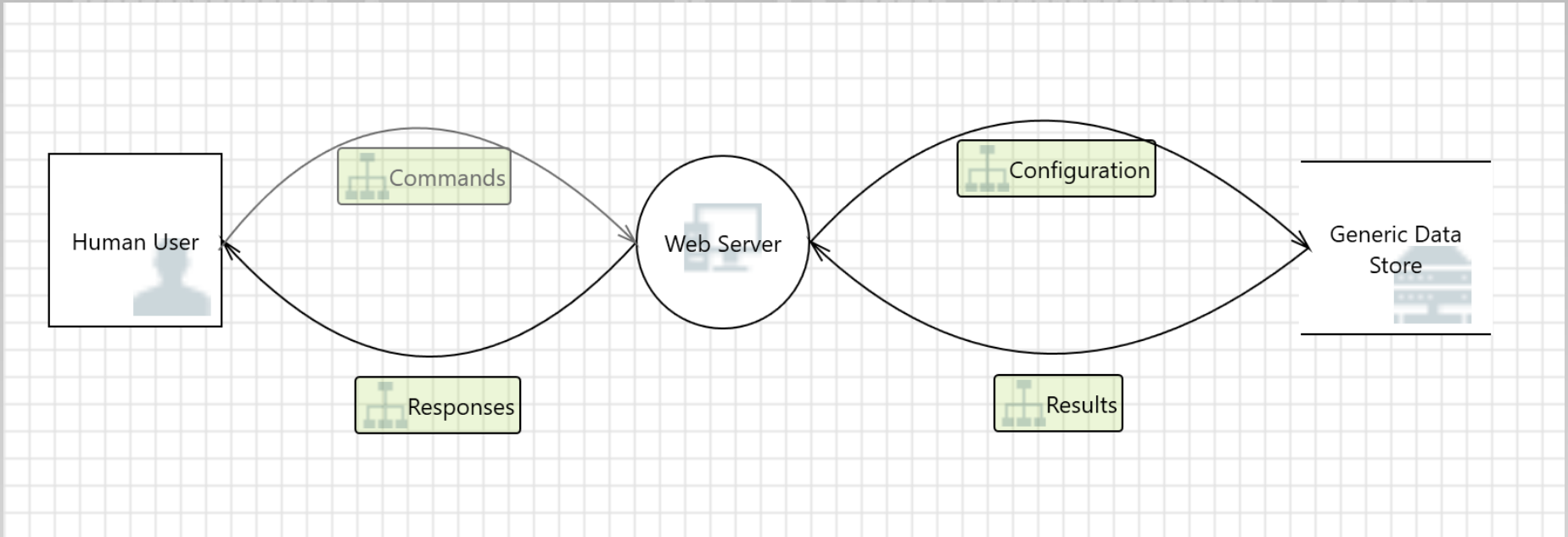
Secure by Default

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

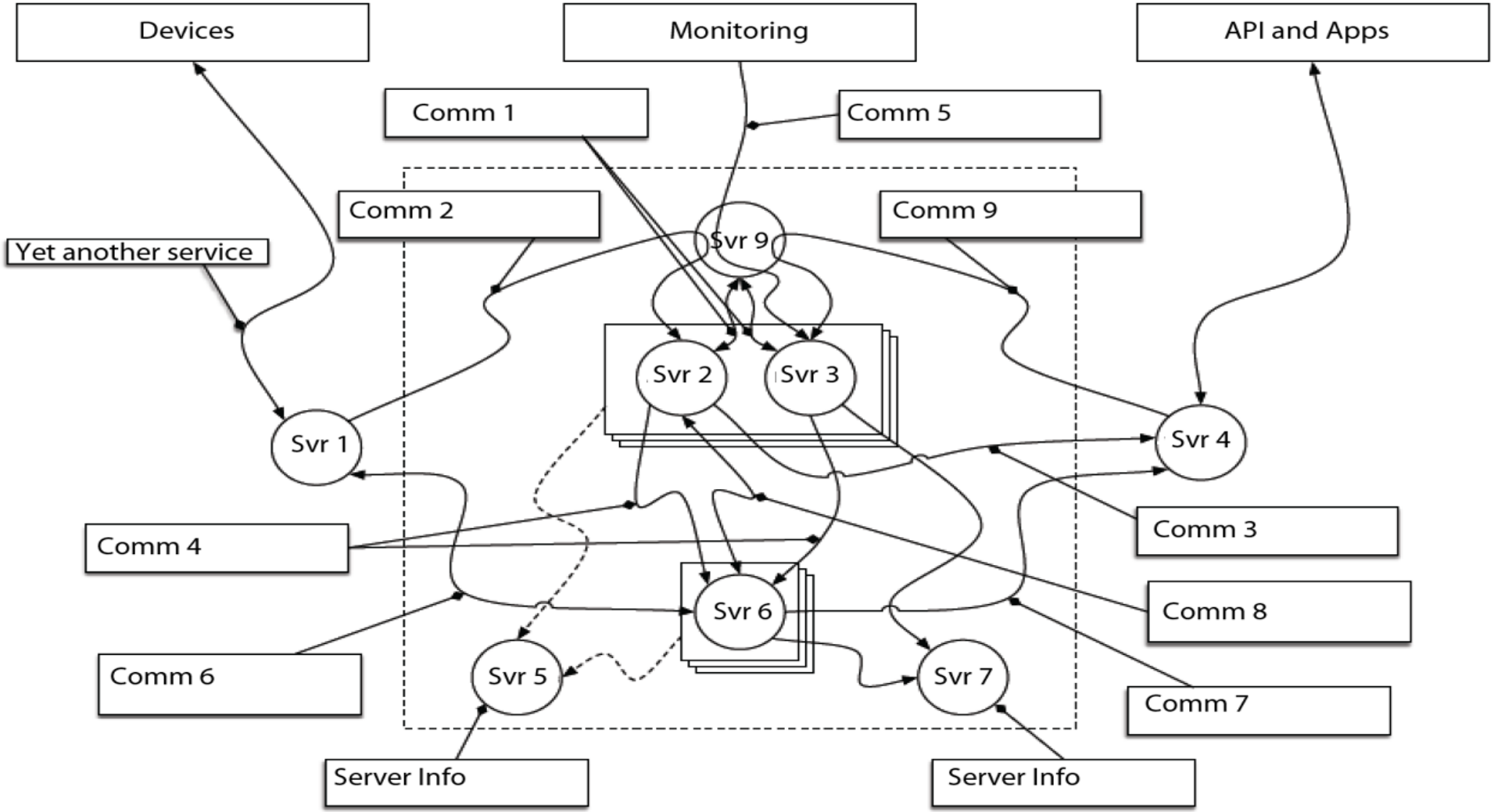
Secure in Deployment

- Protection: Detection, defense, recovery, and management
- Process: How to guides, architecture guides
- People: Training

Data Flow Diagram Example



From *Uncover Security Design Flaws Using The STRIDE Approach*, MSDN Magazine


Devices
Monitoring
API and Apps
Comm 1
Comm 5
Comm 2
Comm 9
Yet another service
Svr 9
Svr 2
Svr 3
Svr 1
Svr 4
Comm 4
Comm 3
Svr 6
Comm 8
Comm 6
Svr 5
Svr 7
Comm 7
Server Info
Server Info

OWASP
Open Web Application Security Project

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

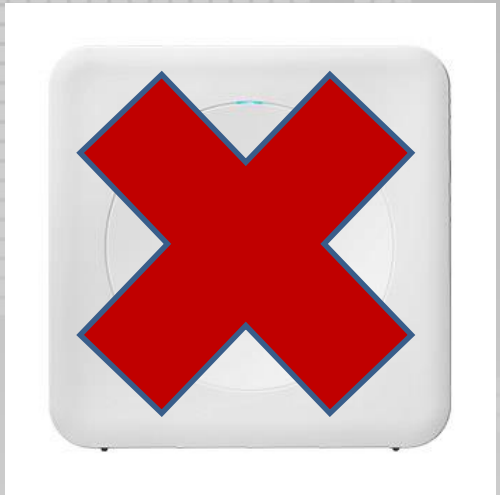
Case Study: Wink

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

What Else?

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
  - http://bit.ly/OWASP-BK1 (https://devops.com/threat-modeling-the-why-how-when-and-which-tools/)
- Microsoft Threat Modeling Tool
  - http://bit.ly/OWASP-BK2 (https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool)
- Microsoft Threat Modeling Web Applications
  - https://msdn.microsoft.com/library/ms978516.aspx
- Uncover Security Flaws Using the STRIDE Approach
  - http://bit.ly/MSDN-STRIDE (https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzZWN1cmVwcm9ncmFtbWluZ3xneDo0MTY1MmM0ZDI0ZjQ4ZDMy)
- Judicial Framework for Evaluating Network Investigative Techniques
  - https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques
- FBI NIT capabilities
  - https://www.documentcloud.org/documents/2166606-ferrell-warrant-1.html#document/p11/a227236
- The Dark Web's Favorite Currency Is Less Untraceable Than It Seems
  - https://www.wired.com/story/monero-privacy/
- 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/

OWASP
Open Web Application
Security Project

Q&A