CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

Sharing Security Secrets: How to Encourage Security Advocates

Cailyn Edwards
Shopify

1. **The Basics**
    a. What
    b. Who
    c. Why
2. **How**
    a. Mangers
    b. Individual Contributors
3. **Examples**
    a. Security Reviews
    b. Security Self Assessments

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Cailyn Edwards

shopify

Senior Infrastructure Security Engineer

What are security advocates?

“Cybersecurity advocates attempt to reduce exposure to cyber attacks by promoting security best practices and encouraging security adoption.”

Cybersecurity Advocates: Discovering the Characteristics and Skills for an Emergent Role

ok.. wait

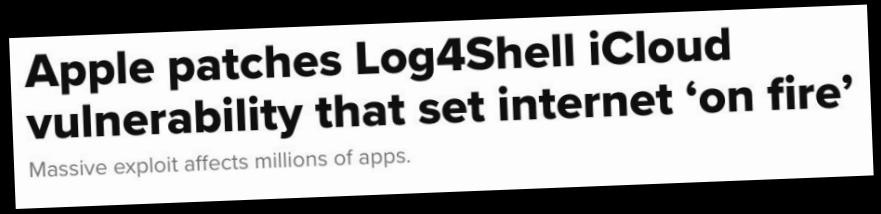
Who are (should be) security advocates?

They **don’t have** to be cybersecurity experts - or even work in a security org

We can’t do it all

Why do we need security advocates?


A Devastating Twitch Hack Sends Streamers Reeling
The data breach apparently includes source code, gamer payouts, and more.


Apple patches Log4Shell iCloud vulnerability that set internet ‘on fire’
Massive exploit affects millions of apps.


LastPass was hacked -- again
The good news is that no passwords appear to have been revealed from the password-saving site. The bad news is that its source code has been compromised.

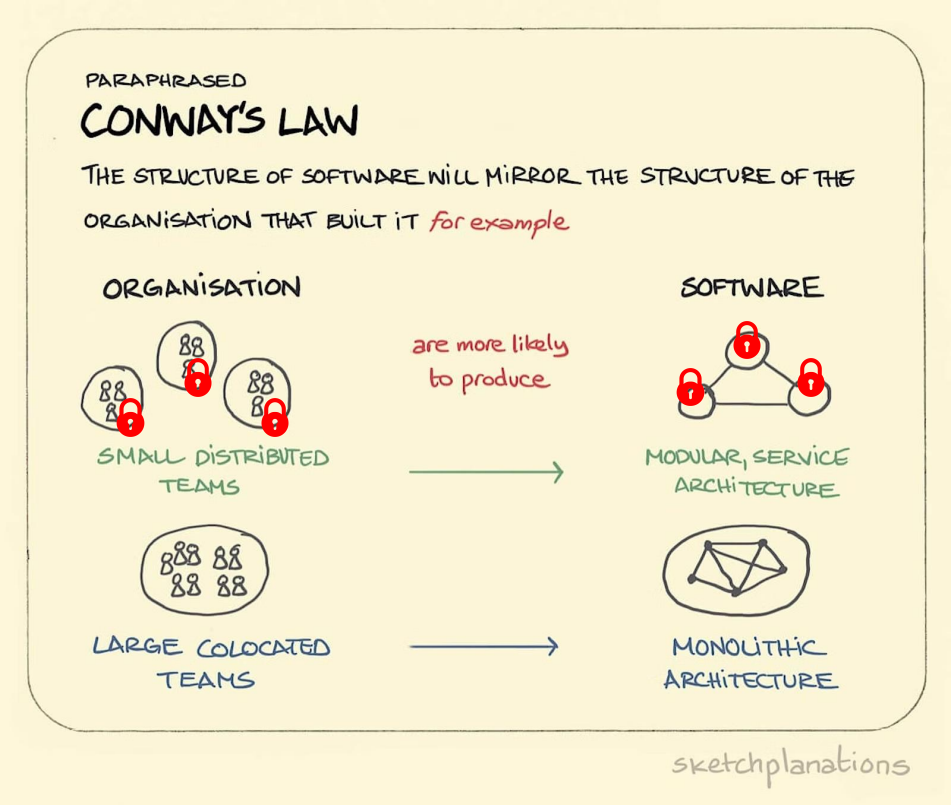

PlayStation Network hackers access data of 77 million users


The 2014 Apple iCloud Hack: What It Means for the Future of Our Personal Data

Uber Says It Was Likely Hacked by Teenage Hacker Gang LAPSUS$
The company also cleared up how the hacker was able to get around multi-factor authentication.

We are small fish in a big pond.

Photo by zhengtao tang on Unsplash



https://sketchplanations.com/conways-law

By integrating security as early as possible throughout the development lifecycle, or even earlier with **interactive developer training**, security organizations can enable preventative security rather than reactive security

- Cloud Native Security Whitepaper v2

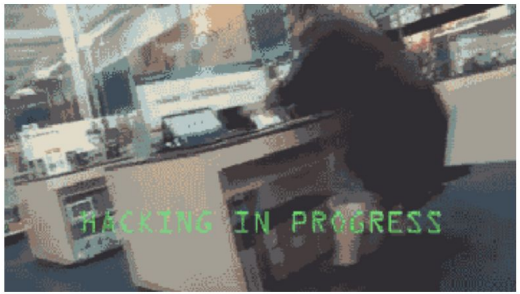
What can managers do?

Photo by Ameer Basheer on Unsplash

"I'm 100% behind it, but I'm swamped. Who can run with this?"

README.md

Learn to Hack!



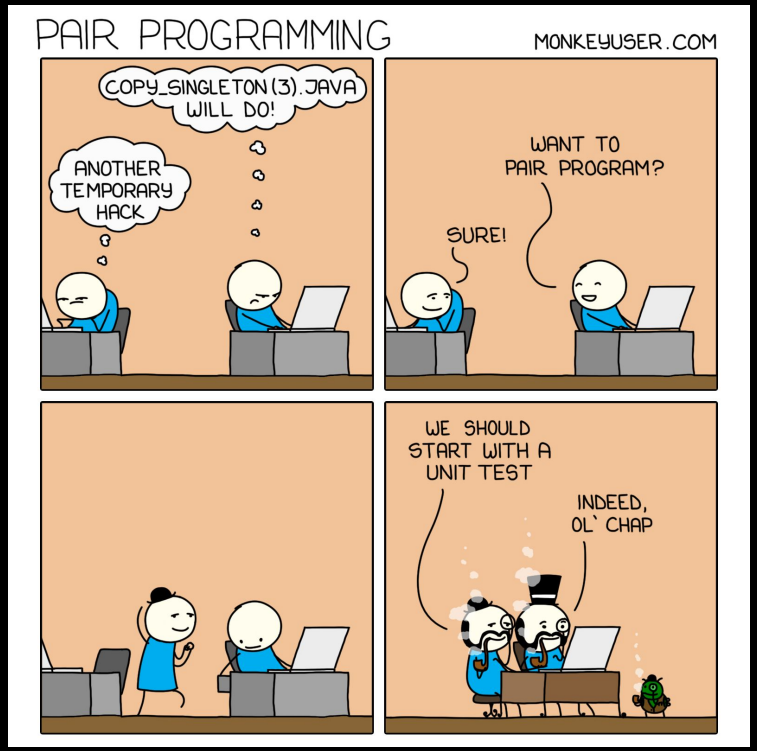
Purpose

This app was developed to show off various common vulnerabilities in web apps and to demonstrate how to solve them. We use it during our RnD Camp and RnD Summit workshops, but you can also explore the app on your own.

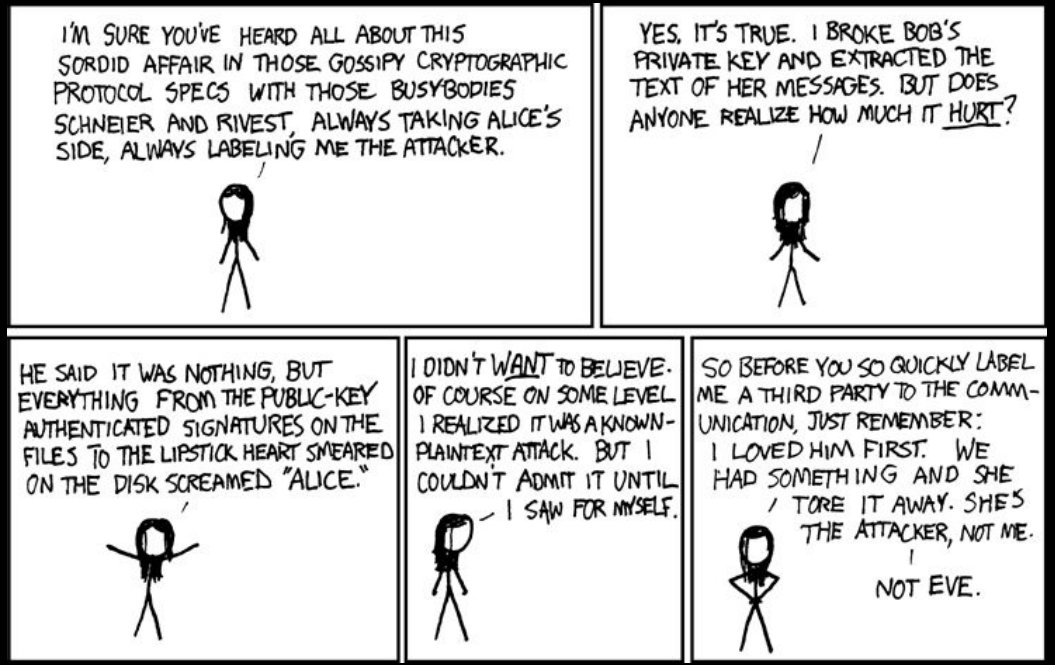
What can ICs do?

Be security advocates themselves.

Consult - don’t dictate.



Educate


I'M SURE YOU'VE HEARD ALL ABOUT THIS SORDID AFFAIR IN THOSE GOSSIPY CRYPTOGRAPHIC PROTOCOL SPECS WITH THOSE BUSYBODIES SCHNEIER AND RIVEST, ALWAYS TAKING ALICE'S SIDE, ALWAYS LABELING ME THE ATTACKER.
YES, IT'S TRUE. I BROKE BOB'S PRIVATE KEY AND EXTRACTED THE TEXT OF HER MESSAGES. BUT DOES ANYONE REALIZE HOW MUCH IT HURT?
HE SAID IT WAS NOTHING, BUT EVERYTHING FROM THE PUBLIC-KEY AUTHENTICATED SIGNATURES ON THE FILES TO THE LIPSTICK HEART SMEARED ON THE DISK SCREAMED "ALICE."
I DIDN'T WANT TO BELIEVE. OF COURSE ON SOME LEVEL I REALIZED IT WAS A KNOWN-PLAINTEXT ATTACK. BUT I COULDN'T ADMIT IT UNTIL I SAW FOR MYSELF.
SO BEFORE YOU SO QUICKLY LABEL ME A THIRD PARTY TO THE COMMUNICATION, JUST REMEMBER: I LOVED HIM FIRST. WE HAD SOMETHING AND SHE TORE IT AWAY. SHE'S THE ATTACKER, NOT ME.
NOT EVE.

Focus points when planning a security education talk at your company

talk about security incidents

What security incidents has your company faced? How did they go? What did you learn

how to threat model

This is a great way to teach non security folks to look at their services through a security mindset! It can also lead to actionable solutions.

cover the basics

Don’t assume any prior knowledge. Go over the basics, limit acronyms and make sure everyone leaves knowing what cyber security is.

explain the security org

How does security work in your company? What’s the size? Are the multiple teams with varied responsibility?

go over security tools

What tools do you use internally for security? How can attendees use them more effectively?

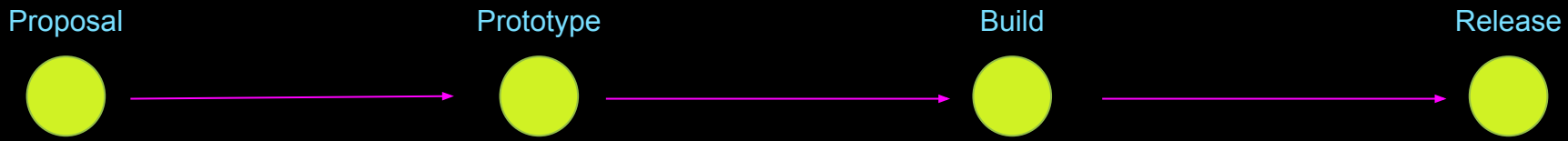
Make it Relevant

Make it Informative

Security Reviews

Goal:
Infrastructure Security Everywhere

GSD at Shopify



This very often results in the creation of a new service
or major change to an existing service

Starting Goals

30%

shorter lead time for security reviews

⅓

Fewer tier move blocking change requests

70%

Faster team onboarding to review process

∞

Better relationships with service owners

Wins

01

Security Concerns Surfaced in Github UI

Promotes security awareness at CI, rather than waiting to surface concerns at deploy time or worse: allow vulnerable workloads to run in production. It empowers developers and allows them to make informed decisions.

02

Report Generated for Service Owners

The review results in a list of vulnerabilities for the service. Our extensive documentation explains each potential vulnerability and how it should be addressed.

03

Issues Opened from Scan Results

We now also surface vulnerabilities via Github issues for project owners/maintainers. This is another avenue of communication with devs and ensures security work is tracked.

Security Self Assessments

Programs by TAG Security and k8s SIG-Security

The Self-assessment is the initial document for projects to begin thinking about the security of the project, determining gaps in their security, and preparing any security documentation for their users.

TAG Security Docs

TL;DR (takeaways)

How to Encourage/Build a Security Advocate Culture

- ✅ Attend this talk (start looking at how other companies do it)
- ❑ Start advocating yourself - tell people about the cool things you are doing
- ❑ Get support and buy in from managers
- ❑ **DO NOT GATEKEEP**, share security basics openly and often!
- ❑ Make security education relevant to your audience
- ❑ Create opportunities for hands on learning
- ❑ Stop, Collaborate and Listen!
- ❑ Get security goals at the top level (OKRs, company mission, guiding themes)

Thank you

Find me on twitter: @CailynEdwards, github: @cailynse or in the Kubernetes slack: @cailyn_codes

Feedback is a gif

Q and E