GitHub Hacks and Software Supply Chain Security

Amanda Crofton and Randy Gingeleski
DTC Security Office Hours
2022 May 31

Agenda

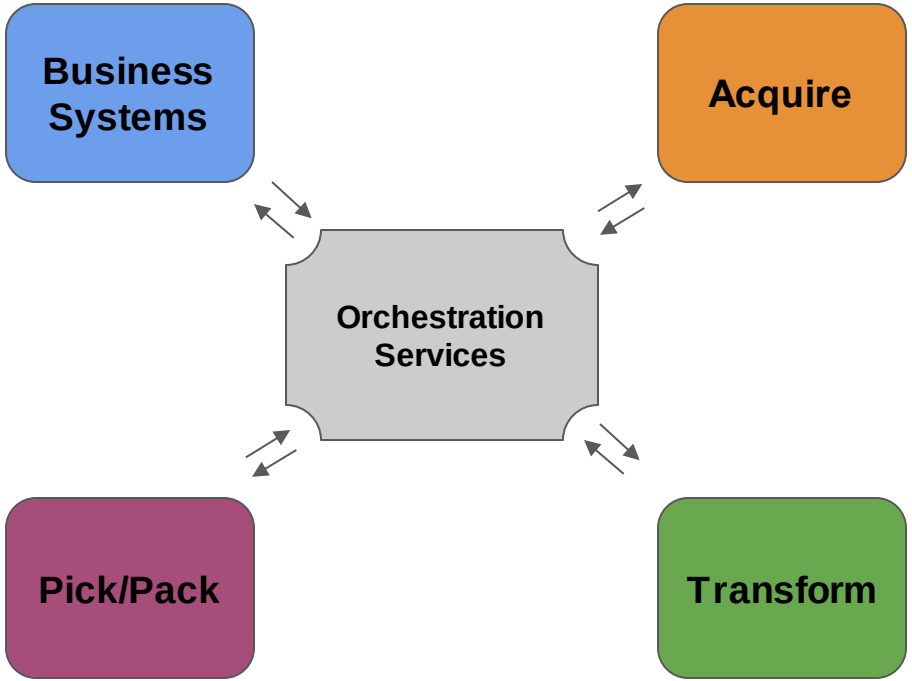
- **Supply chain security's moment**
- **What is the supply chain for HBO Max?**
  - **Media** and **software**
- **GitHub in the supply chain**
- **GitHub security challenges and features**
- **New initiatives**
  - GPG key and code signing initiative
  - * Your idea here * because we'd like your help 💔

Supply chain security's moment

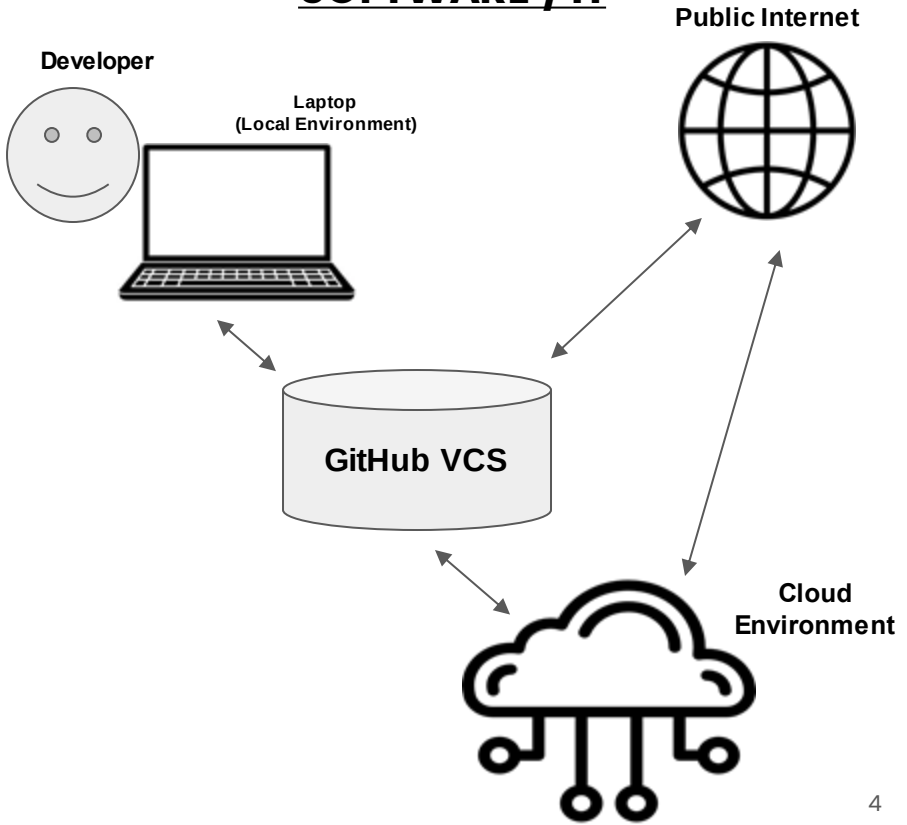
- **NIST and MITRE software supply chain initiatives recently** (<30 days ago)
  - NIST Special Publication 800-161 Revision 1
  - MITRE System of Trust (SoT) prototype framework
- **Libraries getting compromised left and right**
  - Log4J / Log4Shell, UAParser.js 💀
- **New technologies attempting to get ahead of CVE publication** (Twitter?)
  - i.e. Socket.dev
- **Everyone feeling vulnerable** 😓

What is the supply chain for HBO Max?

MEDIA/CONTENT



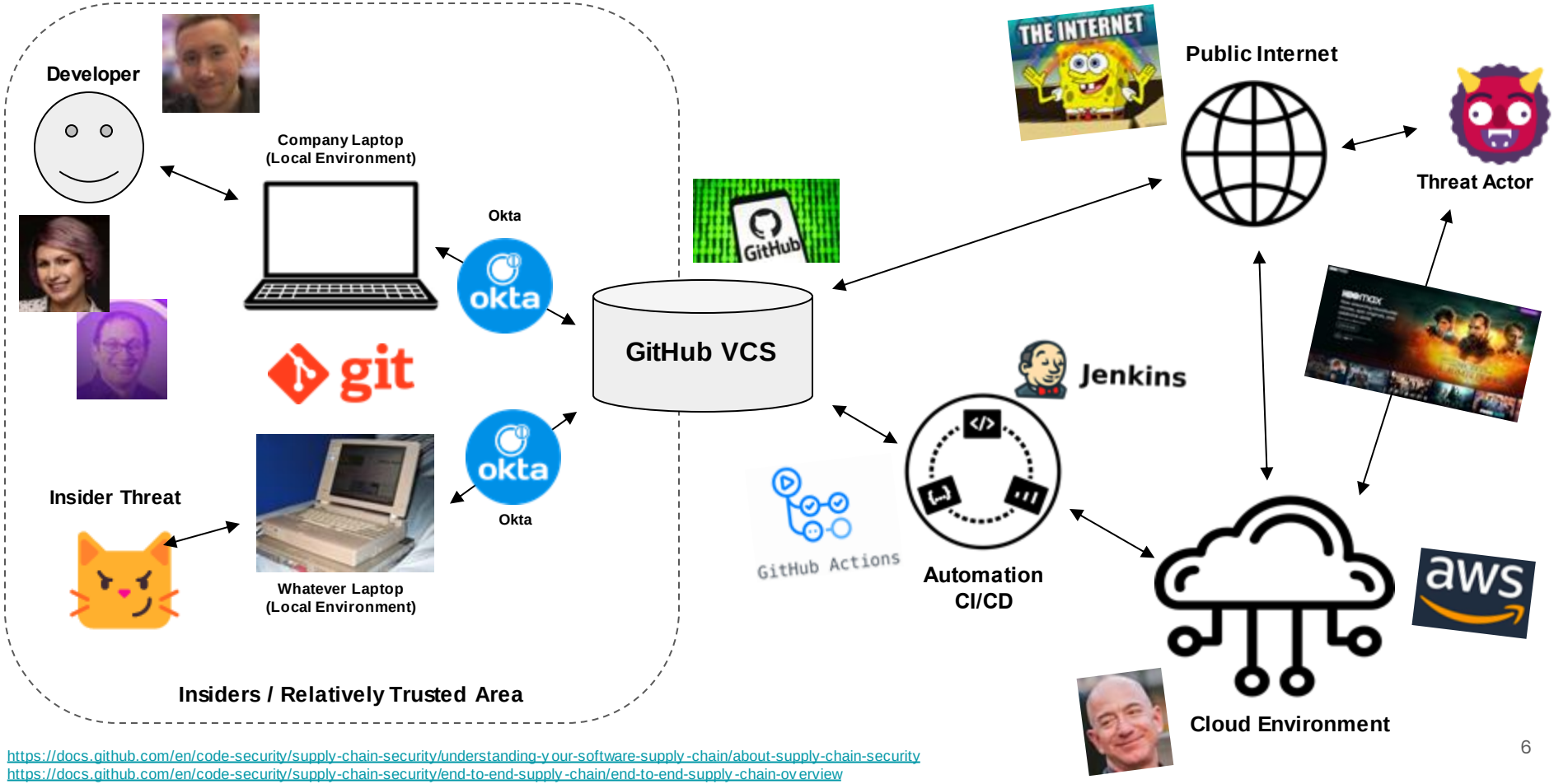
SOFTWARE / IT



GitHub in the supply chain

- **Hosts remote Git repositories for company-wide development**
  - "All of the code"
- **Maintains some sense of identity (developers, teams) and access controls**
  - Derives from Okta at least in part
- **Lots of processes that extend from it**
  - i.e. pull request process has some direct security impact
- **Essential to doing business**

GitHub in the supply chain



https://docs.github.com/en/code-security/supply-chain-security/understanding-your-software-supply-chain/about-supply-chain-security
https://docs.github.com/en/code-security/supply-chain-security/end-to-end-supply-chain/end-to-end-supply-chain-overview

GitHub security challenges

- **Securing accounts**
- **Securing code**
- **Securing builds**

From https://docs.github.com/en/code-security/supply-chain-security/end-to-end-supply-chain/end-to-end-supply-chain-overview

"Best practices for securing accounts"

"Best practices for securing code in your supply chain"

"Best practices for securing your build system"

GitHub security challenges

- **Third-party libraries** (What is in my software, SBOMs, vulnerabilities and risk!)
- **To personal account or not to personal account ?**
    - What should Okta do or not do ?

- **Device access – from where can you access GitHub ?**

- **Can you trust what you're seeing in GitHub ?** Demo
    - Default state is arguably insecure
        - Need to add "official" or "unofficial" guard rails

- **Much range in visibility and access** Demo
    - Either amongst your company *or* public Internet
        - Secrets and sensitive data → 💀

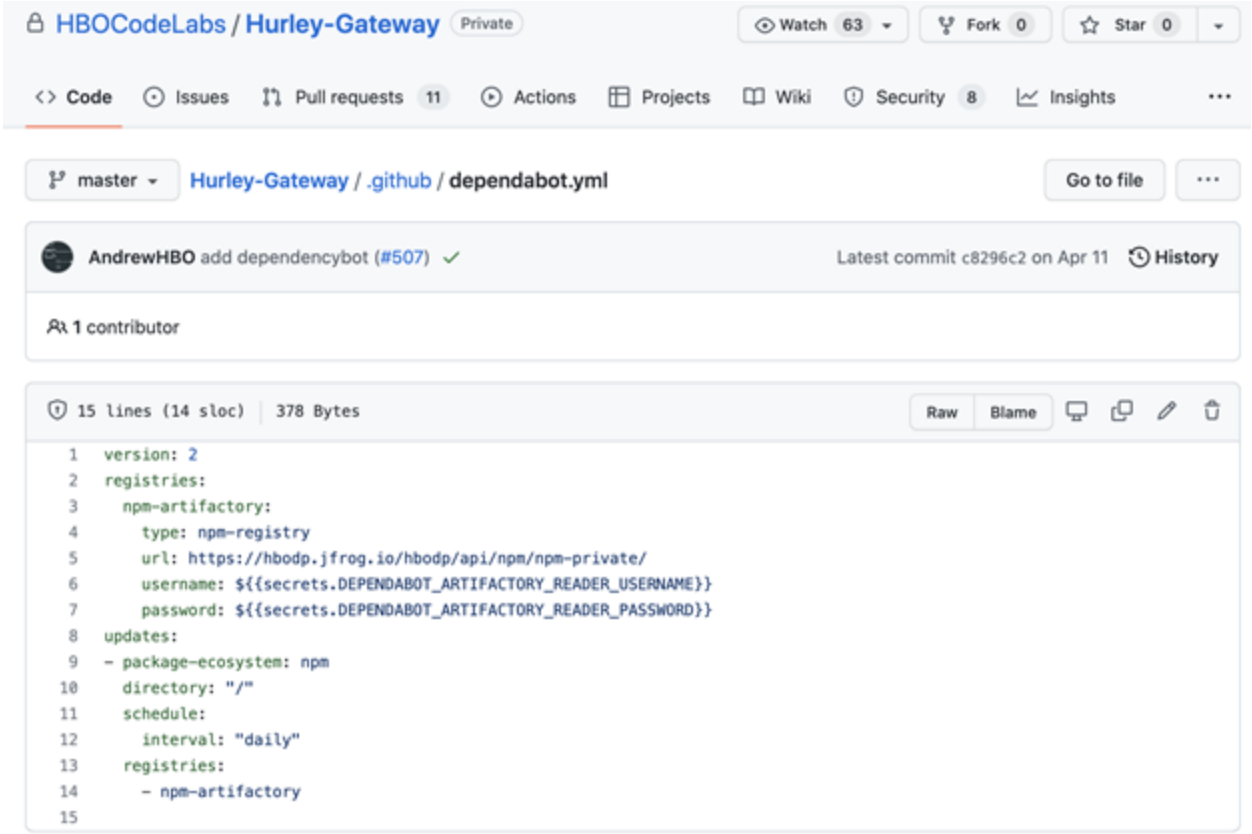
Github Dependabot Security Updates

Dependabot Security Updates - Enable Automated PR for patching

- **Why?** Can prevent security and compliance events such as the PartitionAwareS2SClient library bug
- **Current State:** Single PR for each update
- **Dream State:** Updates grouped by priority + Github Actions = Single PR for Bulk updates (Service Framework Dependency Management - John Felton)

Dependabot.yml Configuration

Example: ***https://github.com/HBOCodeLabs/Hurley-Gateway/blob/master/.github/dependabot.yml***



Github Secrets Detection

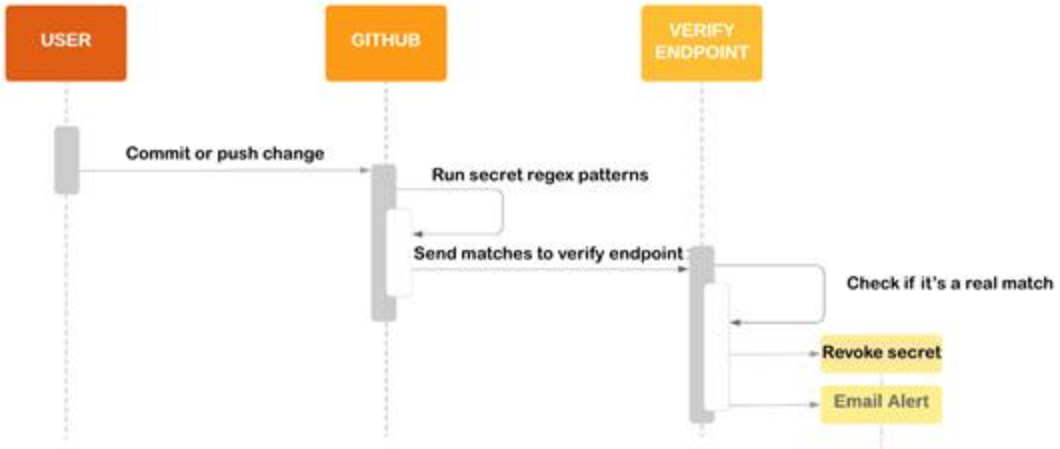
GitHub Security PR Watchdog

- https://security-pr-watchdog.hurley.hbo.com/

Native GitHub secrets detection?

Public Scanning (spurred by HackerOne submissions!)

- **GitGuardian**
- **BluBracket**
- **ShhGit** or **shhbt**



New initiatives

- **GPG key setup between local Git and your GitHub**
  - Eventual enforcement? TBD
- **Dependabot automatic update PRs for internal libraries**
  - https://wiki.hbo.com/display/DevP/Dev+Proposal+-+Service+Frameworks+Dependency+Management
    - https://github.com/HBOCodeLabs/Hurley-Gateway/blob/master/.github/dependabot.yml
- **Improved secrets detection**
  - Missing public scanning/coverage today
- **Okta "trusted devices"?**
- **Okta full control of the GitHub account lifecycle?**
  - GitHub Enterprise Managed Users
- **Your idea here?** 🥰 🙏

Code signing demo

https://github.com/HBOCodeLabs/code-signing-demo

Code signing figures

- **GPG key setup figures**, per **our audit script** at about 2022-05-31 ~12:30 ET

```
rgingele@Randys-MacBook-Pro code-signing-demo % python3 check_github_for_gpg.py --org HBOCodeLabs
[INFO] Defaulting mode to "all-users" since no span argument was given.
[INFO] Total unique users across GitHub orgs : 1264 (100.0%)
[INFO]      Ignored users, per exception list for GPG key setup : 0 (0.0%)
[INFO]      Users with GPG keys : 36 (2.848%)
...
[INFO]      Users without GPG keys : 1228 (97.152%)
...
```

```
rgingele@Randys-MacBook-Pro code-signing-demo % python3 check_github_for_gpg.py --org turnercode
[INFO] Defaulting mode to "all-users" since no span argument was given.
[INFO] Total unique users across GitHub orgs : 1244 (100.0%)
[INFO]                      Ignored users, per exception list for GPG key setup : 0 (0.0%)
[INFO]                      Users with GPG keys : 61 (4.904%)
...
[INFO]                      Users without GPG keys : 1183 (95.096%)
...
```

Secrets demo

https://github.com/eth0izzle/shhgit

Contact Us

- Contact DTC Security Team for general inquiries in #security-team slack channel:
  - @dtc-security-team to notify all security team members
  - @appsec application security (SigSci, Web, etc.)
  - @cloudsec cloud security (AWS, infra, etc.)