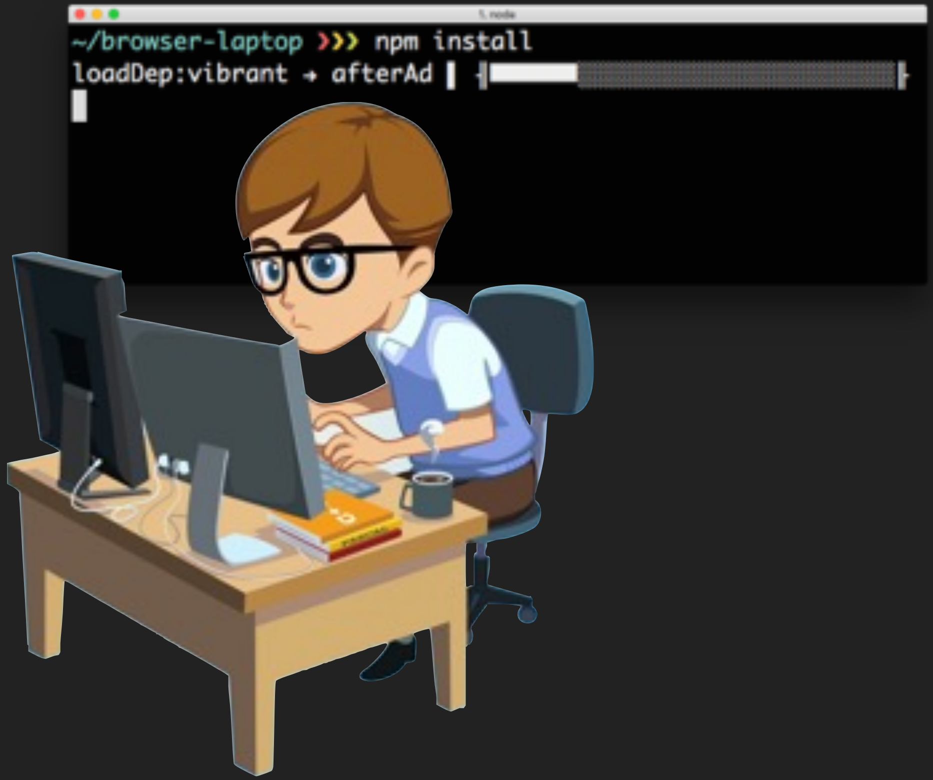
@FREDERICJACOBS

(OPEN SOURCE) SOFTWARE SUPPLY

Tom builds an app

››› NEW PROJECT

❯❯❯ DEPENDENCIES

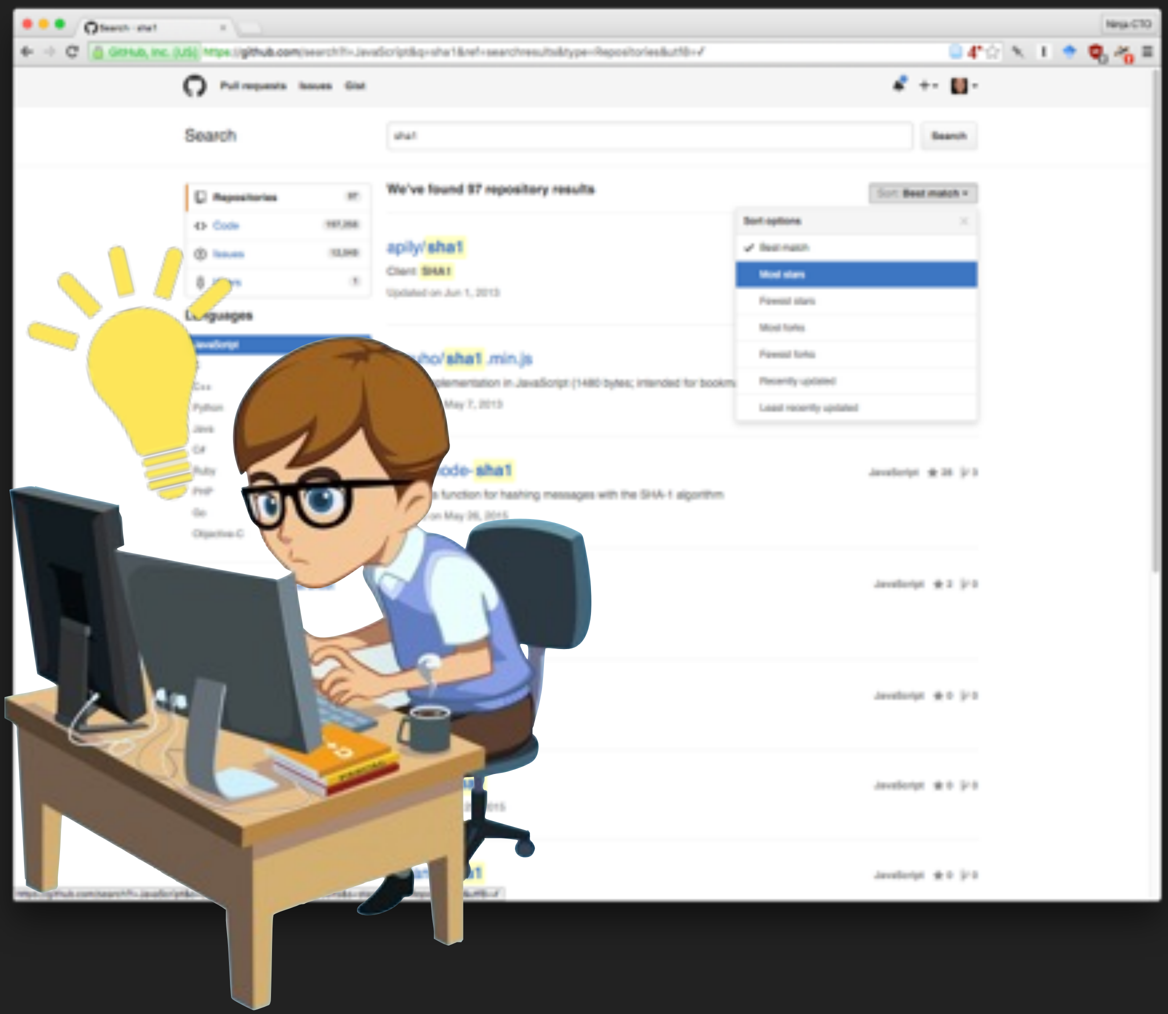


```
~/browser-laptop ❯❯❯ npm install
loadDep:vibrant → afterAd ▌ ╢████░░░░░░░░░░░░░░░░╟
█
```

⚠️ AVOID UNNECESSARY DEPENDENCIES

Less dependencies, smaller attack surface.

FINDING DEPENDENCIES



We've found 97 repository results

apily/sha1
Client SHA1
Updated on Jun 1, 2013

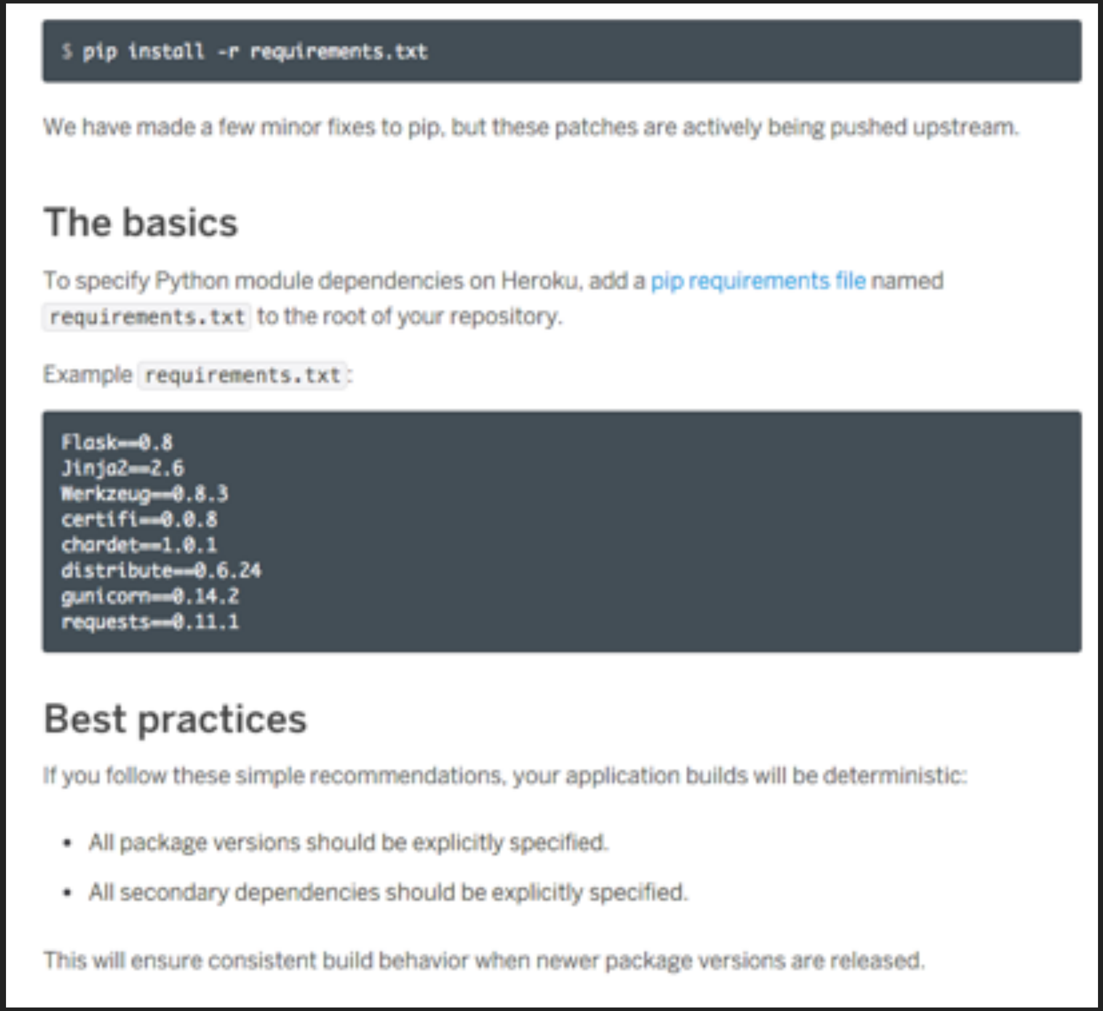
sha1.min.js
implementation in JavaScript (1480 bytes; intended for bookm…
May 7, 2013

node-sha1
function for hashing messages with the SHA-1 algorithm
on May 26, 2015

- Most apps are performing the same tasks.
- Great, there are dozens of libraries on GitHub that perform the task that Tom needs to be done.
- Are licenses compatible?
- But which one can be trusted?
  - GitHub stars as a reputation factor?
  - Tom doesn't have the skills to audit the quality of a cryptographic implementations, who can he trust?

EXAMPLE: PIP

Also known as YOLO package managing.



```
$ pip install -r requirements.txt
```

We have made a few minor fixes to pip, but these patches are actively being pushed upstream.

The basics

To specify Python module dependencies on Heroku, add a pip requirements file named `requirements.txt` to the root of your repository.

Example `requirements.txt`:

```
Flask==0.8
Jinja2==2.6
Werkzeug==0.8.3
certifi==0.0.8
chardet==1.0.1
distribute==0.6.24
gunicorn==0.14.2
requests==0.11.1
```

Best practices

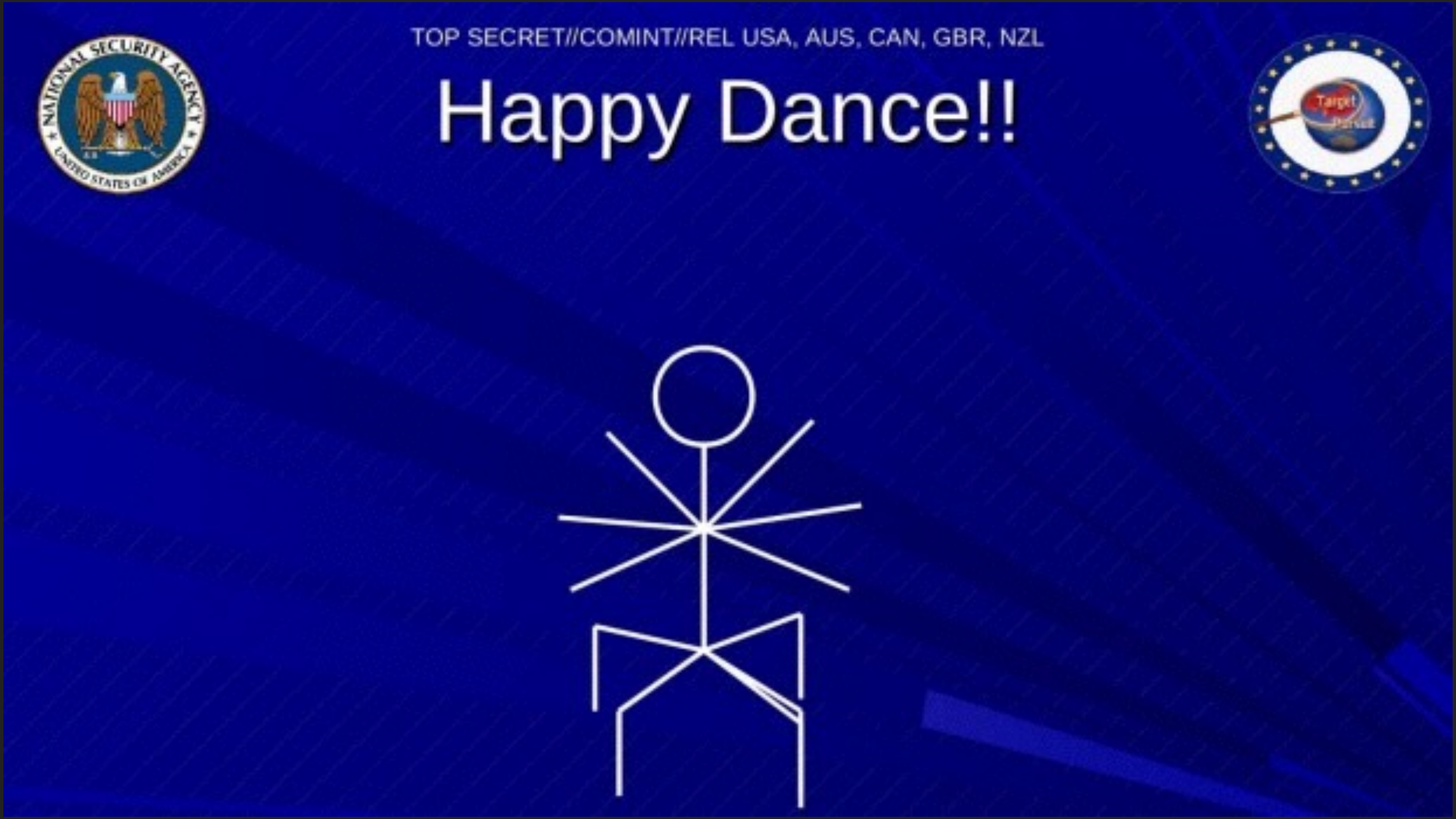
If you follow these simple recommendations, your application builds will be deterministic:

- All package versions should be explicitly specified.
- All secondary dependencies should be explicitly specified.

This will ensure consistent build behavior when newer package versions are released.

- Authority-based
- Previously distributed all packages over HTTP.
- No integrity checking whatsoever

BACKDOOR ALL THE PYTHON APPS!

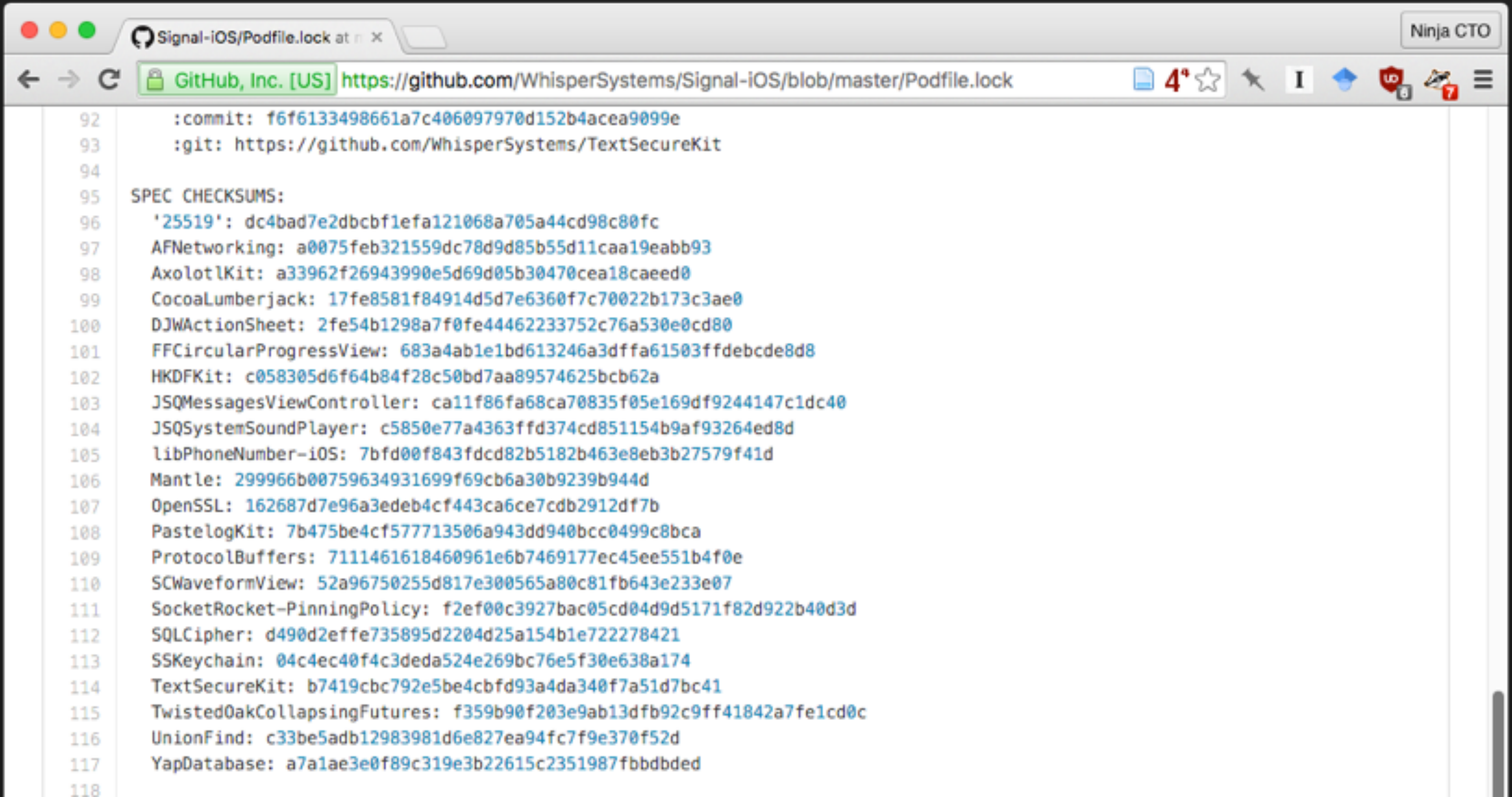


TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL

Happy Dance!!

BETTER DEPENDENCY MANAGEMENT

- Code-sign Git tags and verify signatures on checkout.
- Include a “lock” file that contains a cryptographically secure hash of the state of the fetched repository. Deployment security.



Signal-iOS/Podfile.lock at m
Ninja CTO
GitHub, Inc. [US]
https://github.com/WhisperSystems/Signal-iOS/blob/master/Podfile.lock

```
    :commit: f6f6133498661a7c406097970d152b4acea9099e
    :git: https://github.com/WhisperSystems/TextSecureKit

SPEC CHECKSUMS:
  '25519': dc4bad7e2dbcbf1efa121068a705a44cd98c80fc
  AFNetworking: a0075feb321559dc78d9d85b55d11caa19eabb93
  AxolotlKit: a33962f26943990e5d69d05b30470cea18caeed0
  CocoaLumberjack: 17fe8581f84914d5d7e6360f7c70022b173c3ae0
  DJWActionSheet: 2fe54b1298a7f0fe44462233752c76a530e0cd80
  FFCircularProgressView: 683a4ab1e1bd613246a3dffa61503ffdebcde8d8
  HKDFKit: c058305d6f64b84f28c50bd7aa89574625bcb62a
  JSQMessagesViewController: ca11f86fa68ca70835f05e169df9244147c1dc40
  JSQSystemSoundPlayer: c5850e77a4363ffd374cd851154b9af93264ed8d
  libPhoneNumber-iOS: 7bfd00f843fdcd82b5182b463e8eb3b27579f41d
  Mantle: 299966b007596349316 99f69cb6a30b9239b944d
  OpenSSL: 162687d7e96a3edeb4cf443ca6ce7cdb2912df7b
  PastelogKit: 7b475be4cf577713506a943dd940bcc0499c8bca
  ProtocolBuffers: 7111461618460961e6b7469177ec45ee551b4f0e
  SCWaveformView: 52a96750255d817e300565a80c81fb643e233e07
  SocketRocket-PinningPolicy: f2ef00c3927bac05cd04d9d5171f82d922b40d3d
  SQLCipher: d490d2effe735895d2204d25a154b1e722278421
  SSKeychain: 04c4ec40f4c3deda524e269bc76e5f30e638a174
  TextSecureKit: b7419cbc792e5be4cbfd93a4da340f7a51d7bc41
  TwistedOakCollapsingFutures: f359b90f203e9ab13dfb92c9ff41842a7fe1cd0c
  UnionFind: c33be5adb12983981d6e827ea94fc7f9e370f52d
  YapDatabase: a7a1ae3e0f89c319e3b22615c2351987fbbdbded

```

⚠️ KEEP YOUR DEPENDENCIES UP TO DATE

Adding dependencies are a liability that you should avoid in the first place

If no choice, be aware of what they are and keep an eye out on their ML / Issues.

❯❯❯ GIT PUSH

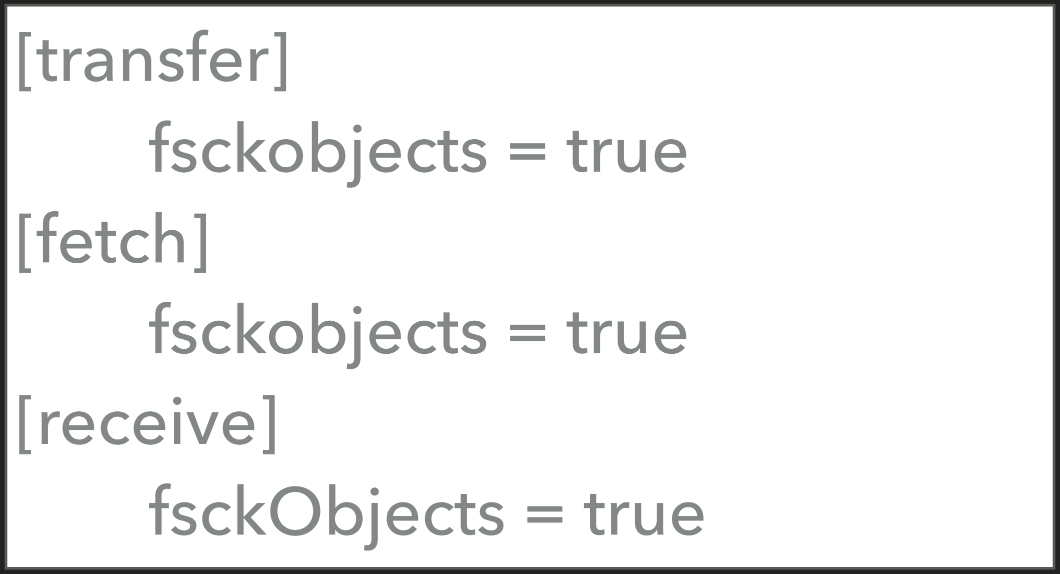
GIT: BEST PRACTICES

- Clone over SSH.
  - TOFU model > PKI
  - OpenSSH public key authentication (eg. ed25519) is widely superior than password auth
- Protect branches overwrite.
- I can't emphasize this enough: CLEAN DIFFS

GIT & INTEGRITY

- Unlike common belief, Git doesn’t guarantee integrity by default.

- Adding the following to your ~/.gitconfig



```
[transfer]
	fsckobjects = true
[fetch]
	fsckobjects = true
[receive]
	fsckObjects = true
```

- Source: https://groups.google.com/forum/#!topic/binary-transparency/f-BI4o8HZW0

GIT & SIGNING

- Sign Git tags
- Why not code sign commits? Much safer!
  - No rebasing
  - Unpractical for large OSS

SHA1 COLLISIONS & GIT

Cryptology ePrint Archive: Report 2015/967

Freestart collision on full SHA-1

Marc Stevens and Pierre Karpman and Thomas Peyrin

Abstract: We present in this article a freestart col [illegible] HA-1, i.e., a collision for its internal compression function. This is the first practica [illegible] eaching all 80 out of 80 steps, while only 10 days of computation on a 64 G [illegible] perform the attack. This work builds on a continuous series of cryptanalyti [illegible] e the theoretical collision attack breakthrough in 2005. In particular, we exte [illegible] work on reduced-round SHA-1 from CRYPTO 2015 that leverages the comp [illegible] ds and adapt it to allow the use of boomerang speed-up techniques. We also lev [illegible] iques by Stevens from EUROCRY [illegible] obtain optimal attack [illegible] further refinements for this work.

Freestart col [illegible] one presented here, [illegible] owever, this work is an in [illegible] towards an actual [illegible] phics cards can be used [illegible] k on SHA-1 by Stevens fr [illegible] present ne [illegible] al/financial cost required [illegible] projection [illegible] eviously

- “I read that SHA-1 is broken!”
- Generating a SHA-1 collision in Git would likely imply adding a large binary blob to the repo, no?

List: git
Subject: Re: Starting to think about sha-256?
From: Linus Torvalds <torvalds () osdl ! org>
Date: 2006-08-28 17:56:01
On Mon, 28 Aug 2006, David Lang wrote:

>
> just to double check.
>
> if you already have a file A in git with hash X is there any condition where a
> remote file with hash X (but different contents) would overwrite the local
> version?

Nope. **If it has the same SHA1, it means that when we receive the object from the other end, we will _not_ overwrite the object we already have.**

Source: Git Mailing List

Tom published his code

it’s all vulnerability proof now, no?

(IN MOST CASES)NOBODY CARES ABOUT YOUR CODE

- In most cases, nobody will look at your code until it creates a problem in their own project.
- Open Source software developed by one burned out dev isn’t going to be safer than something from MSR or DoD funded software who can afford more eyes on their code.
- OSS? Get the community to care.
- Closed or open: Get your code audited

❯❯❯ DEPLOY

TRUSTING TRUST

“the Boeing 777 uses compiler-based and also hardware-based N-version diversity: there is a single version of the Ada avionics software that is compiled by three different compilers and then it runs on three different processors: a 486, a 68040, and an AMD 29050”

http://blog.regehr.org/archives/1282

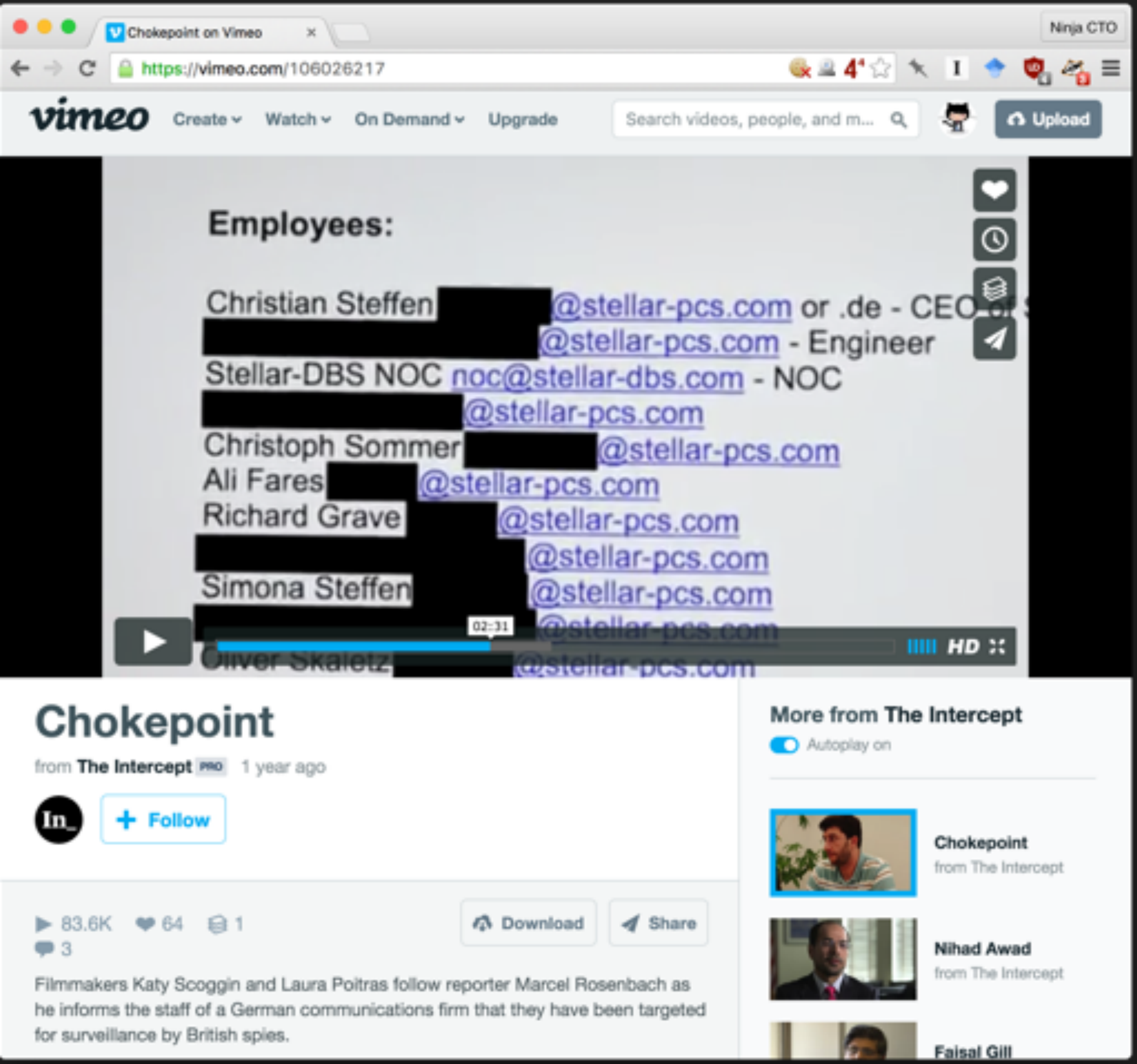
TRUSTING BUILD ENV

Watering Hole Attacks

- Nation States detect which websites are predominantly used by the targeted community. Uploads malware to target website or
- Recent examples:
    - Targeting of iOS developers using watering hole attack on popular developer forum with a Java 0-Day. Successfully compromised engineers at Apple and Facebook
    - “XcodeGhost” is compiler backdooring all apps it builds. It was uploaded to popular mirrors where Chinese iOS devs get their IDE from resulting in backdooring of most popular Chinese apps.

TRUSTING BUILD ENV

Targeted Attacks



Employees:

Christian Steffen [redacted]@stellar-pcs.com or .de - CEO of
[redacted]@stellar-pcs.com - Engineer
Stellar-DBS NOC noc@stellar-dbs.com - NOC
[redacted]@stellar-pcs.com
Christoph Sommer [redacted]@stellar-pcs.com
Ali Fares [redacted]@stellar-pcs.com
Richard Grave [redacted]@stellar-pcs.com
[redacted]@stellar-pcs.com
Simona Steffen [redacted]@stellar-pcs.com
[redacted]@stellar-pcs.com
Oliver Skaletz [redacted]@stellar-pcs.com

Chokepoint

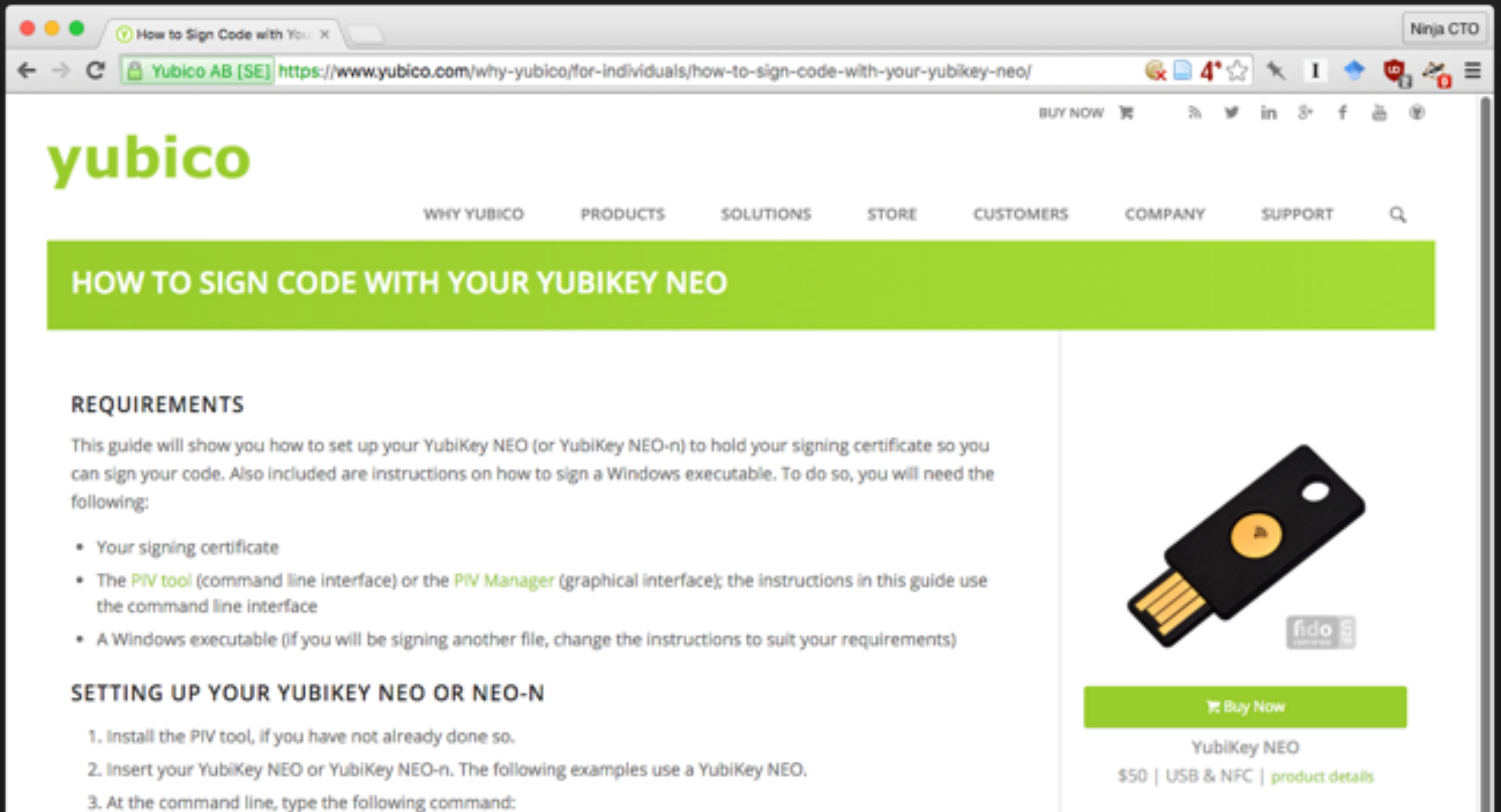
from The Intercept PRO 1 year ago

Filmmakers Katy Scoggin and Laura Poitras follow reporter Marcel Rosenbach as he informs the staff of a German communications firm that they have been targeted for surveillance by British spies.

- If your software is used by high-value targets, they might target you personally. Even if you're a law-abiding citizen.
- Eg:
  - Belgacom engineers
  - Chokepoint

TRUSTING YOUR BUILD ENV

- If you can afford it, dedicated “mostly offline” build environment.
- If you can’t, compartmentalize using VMs.
- Use YubiKeys or similar to protect signing keys.



How to Sign Code with You
Ninja CTO
Yubico AB [SE] https://www.yubico.com/why-yubico/for-individuals/how-to-sign-code-with-your-yubikey-neo/
BUY NOW
yubico
WHY YUBICO
PRODUCTS
SOLUTIONS
STORE
CUSTOMERS
COMPANY
SUPPORT

HOW TO SIGN CODE WITH YOUR YUBIKEY NEO

REQUIREMENTS

This guide will show you how to set up your YubiKey NEO (or YubiKey NEO-n) to hold your signing certificate so you can sign your code. Also included are instructions on how to sign a Windows executable. To do so, you will need the following:

- Your signing certificate
- The PIV tool (command line interface) or the PIV Manager (graphical interface); the instructions in this guide use the command line interface
- A Windows executable (if you will be signing another file, change the instructions to suit your requirements)

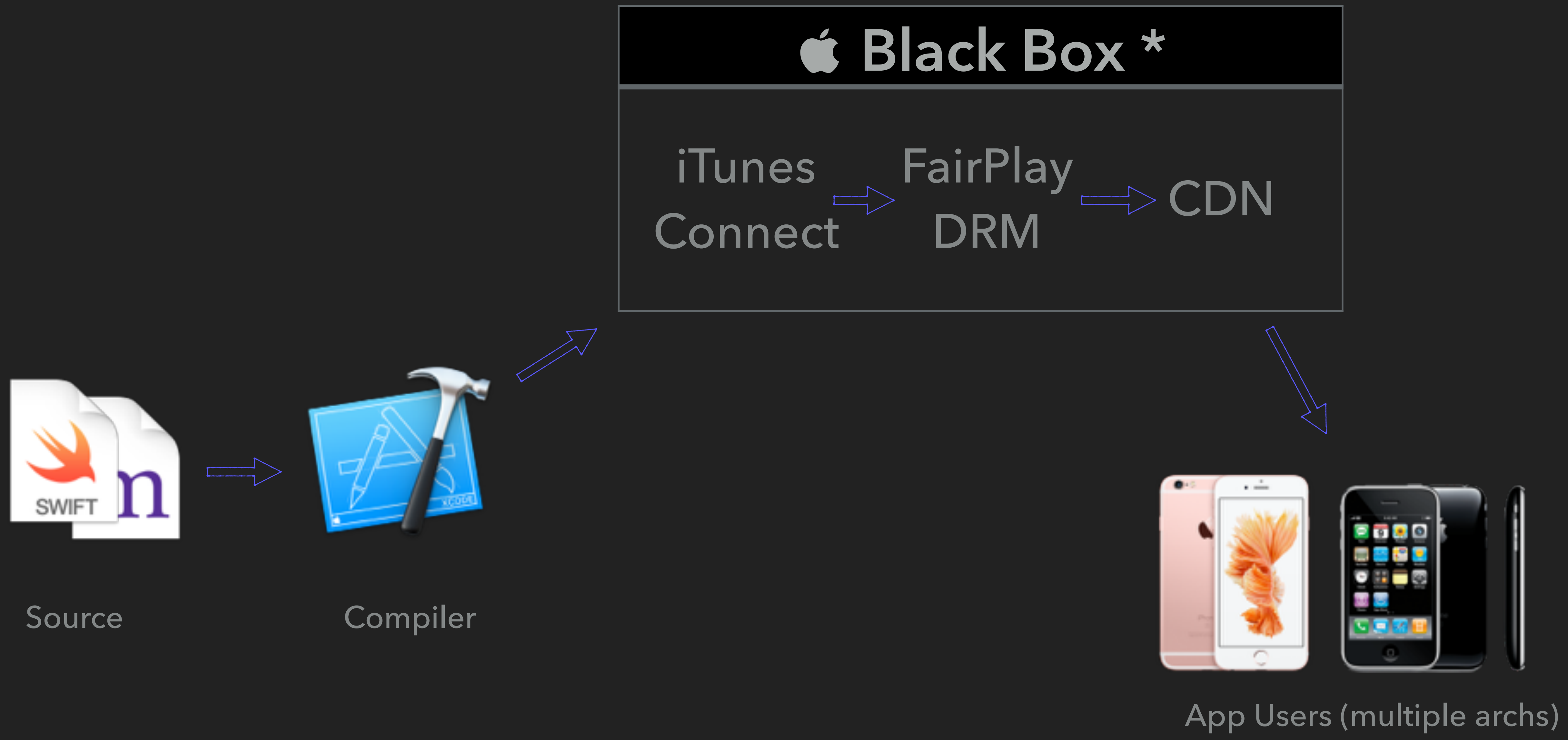
SETTING UP YOUR YUBIKEY NEO OR NEO-N

1. Install the PIV tool, if you have not already done so.
2. Insert your YubiKey NEO or YubiKey NEO-n. The following examples use a YubiKey NEO.
3. At the command line, type the following command:

CONTAINERS

(Sadly, skipping this)

APP STORES



Black Box *

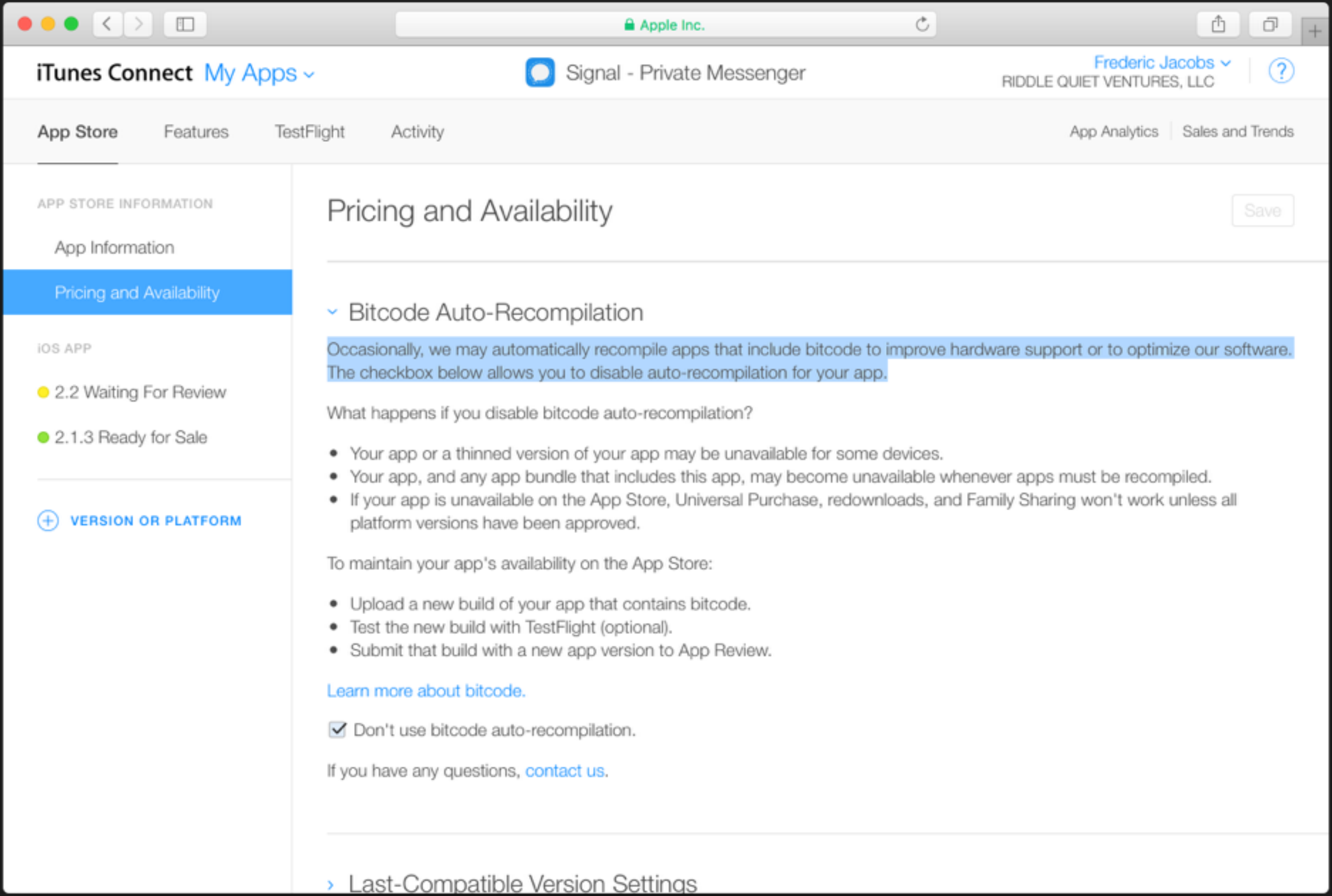
iTunes Connect → FairPlay DRM → CDN

Source

Compiler

App Users (multiple archs)

* Heh, it's a black box, I actually have no clue what's really in there but given functionality these components must be there.



Pricing and Availability

Bitcode Auto-Recompilation

Occasionally, we may automatically recompile apps that include bitcode to improve hardware support or to optimize our software. The checkbox below allows you to disable auto-recompilation for your app.

What happens if you disable bitcode auto-recompilation?

- Your app or a thinned version of your app may be unavailable for some devices.
- Your app, and any app bundle that includes this app, may become unavailable whenever apps must be recompiled.
- If your app is unavailable on the App Store, Universal Purchase, redownloads, and Family Sharing won't work unless all platform versions have been approved.

To maintain your app's availability on the App Store:

- Upload a new build of your app that contains bitcode.
- Test the new build with TestFlight (optional).
- Submit that build with a new app version to App Review.

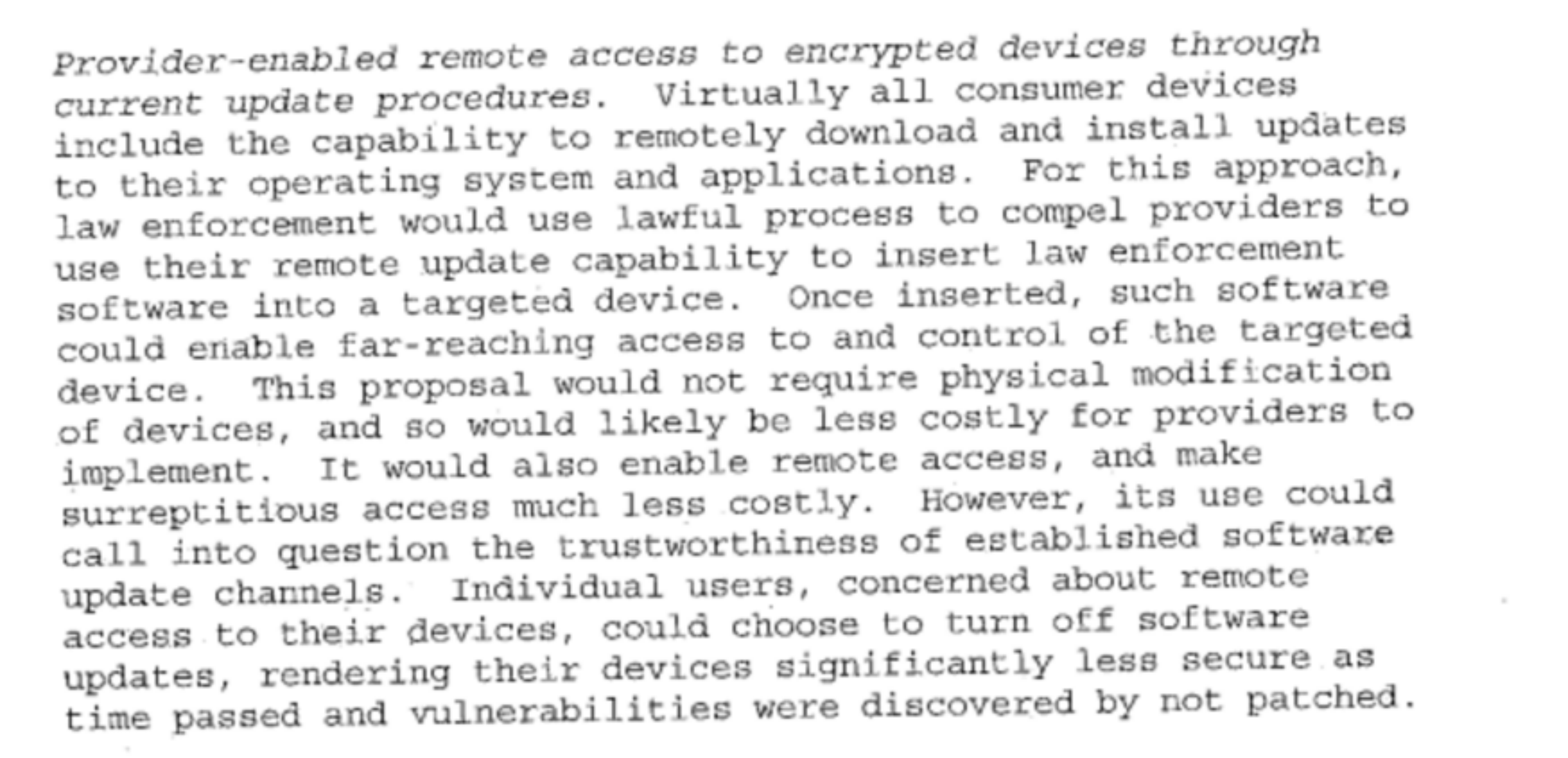
Learn more about bitcode.

☑ Don't use bitcode auto-recompilation.

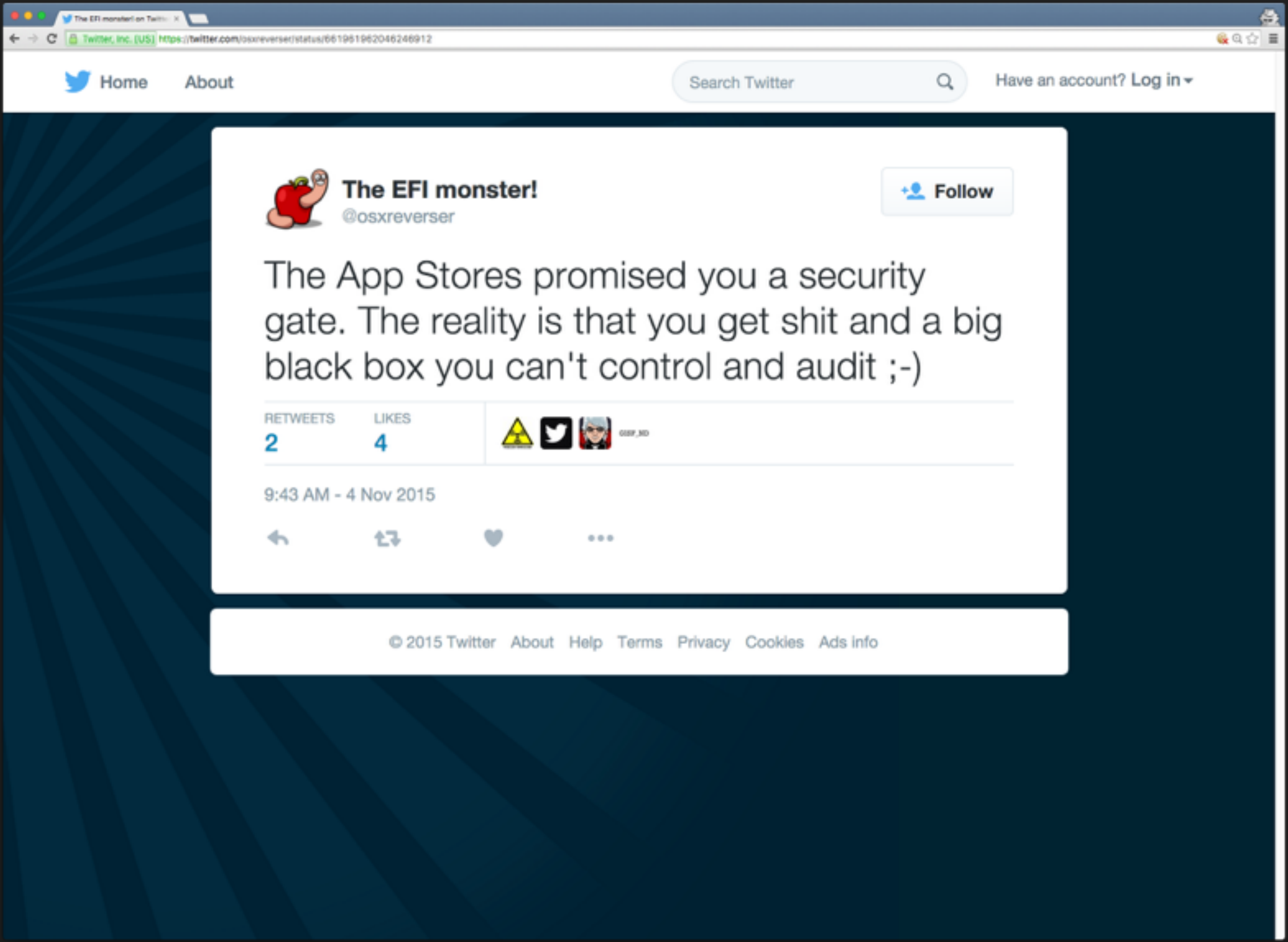
If you have any questions, contact us.

Last-Compatible Version Settings

Obama Administration Working Group discussing using automatic updates to insert backdoors



Provider-enabled remote access to encrypted devices through current update procedures. Virtually all consumer devices include the capability to remotely download and install updates to their operating system and applications. For this approach, law enforcement would use lawful process to compel providers to use their remote update capability to insert law enforcement software into a targeted device. Once inserted, such software could enable far-reaching access to and control of the targeted device. This proposal would not require physical modification of devices, and so would likely be less costly for providers to implement. It would also enable remote access, and make surreptitious access much less costly. However, its use could call into question the trustworthiness of established software update channels. Individual users, concerned about remote access to their devices, could choose to turn off software updates, rendering their devices significantly less secure as time passed and vulnerabilities were discovered by not patched.



The EFI monster! on Twitt
Twitter, Inc. [US] https://twitter.com/osxreverser/status/661951962046246912
Home
About
Search Twitter
Have an account? Log in
Follow

The EFI monster!
@osxreverser

The App Stores promised you a security gate. The reality is that you get shit and a big black box you can't control and audit ;-)

RETWEETS	LIKES
2	4

9:43 AM - 4 Nov 2015

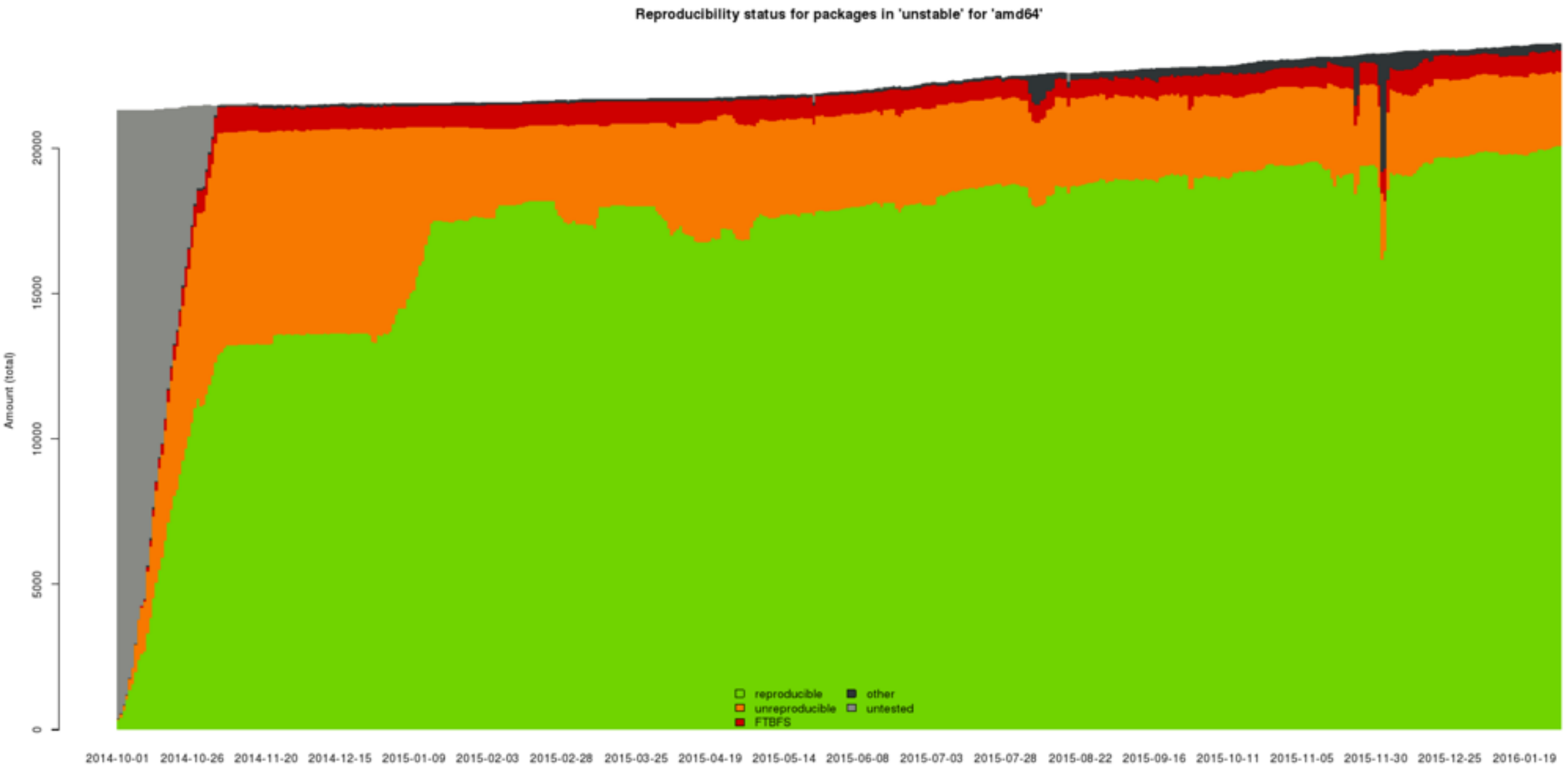
© 2015 Twitter About Help Terms Privacy Cookies Ads info

⚠️ HOW DO I KNOW THE BINARY IS THE RESULT OF THE COMPILATION OF THE PUBLICLY POSTED SOURCE?

Open Source code doesn’t have a major advantage over closed one if you can’t reproduce the binary.

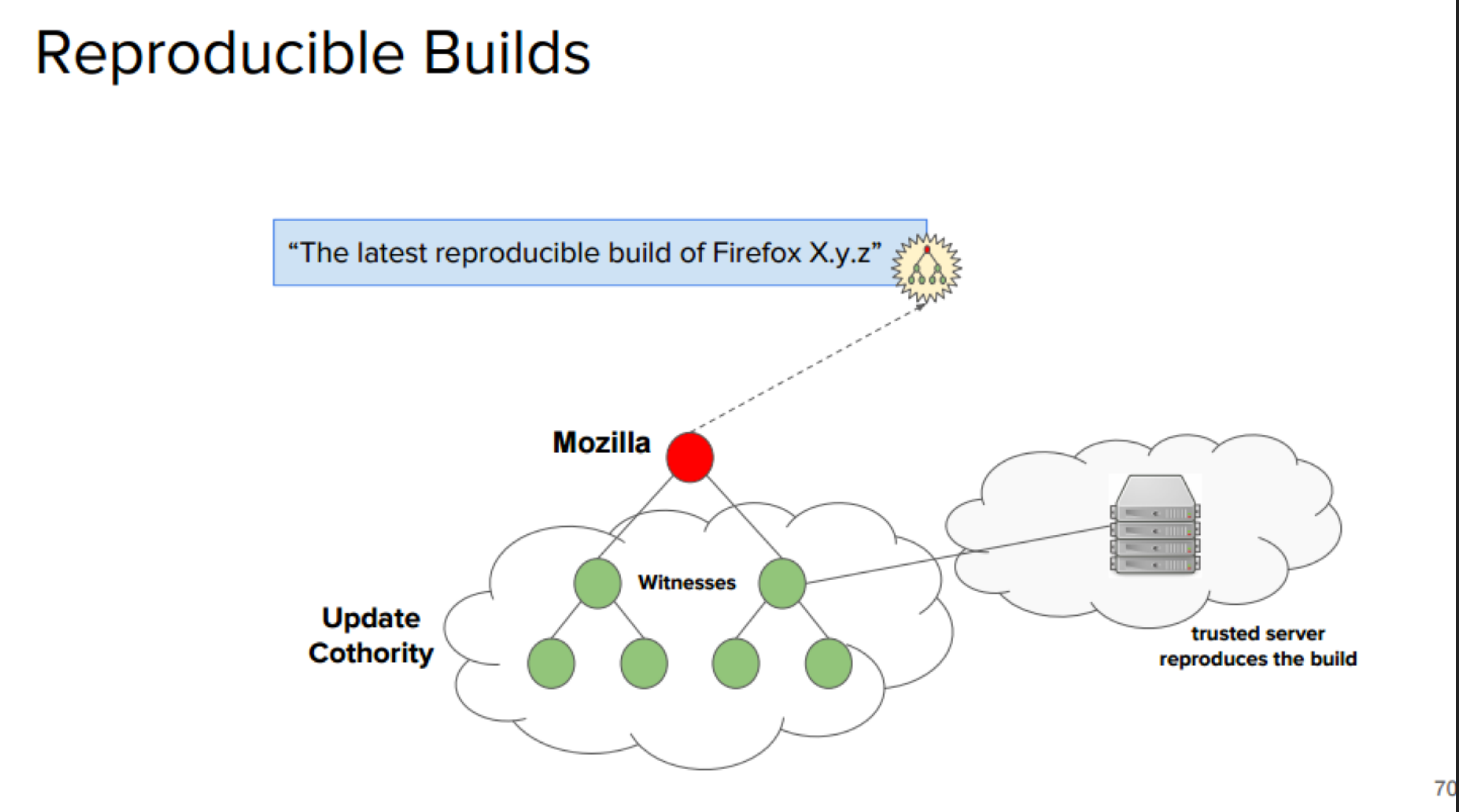
REPRODUCIBLE BUILDS

DEBIAN LEADING THE WAY



https://wiki.debian.org/ReproducibleBuilds

COTHORITY (EPFL)



Reproducible Builds

“The latest reproducible build of Firefox X.y.z”

Mozilla

Witnesses

Update Cothority

trusted server reproduces the build

https://github.com/dedis/cothority

QUESTIONS?