# On Conducting Systematic Security & Privacy Analyses of TOTP 2FA Apps

## Case-Study: Authy 2FA

Conor Gilsenan
U.C. Berkeley

Noura Alomar
U.C. Berkeley

Serge Egelman
U.C. Berkeley / ICSI

# 2FA improves account security

# 2FA Methods

- SMS
- Time-based One-time Passwords (TOTP)
  - e.g. Google Authenticator
- Push notifications
  - e.g. Duo Push
- WebAuthn
  - e.g. USB security keys

# Research Questions

1. What security and privacy issues exist in the backup & recovery functionality of prevalent TOTP 2FA apps?
2. How can they be fixed?

# Research Questions

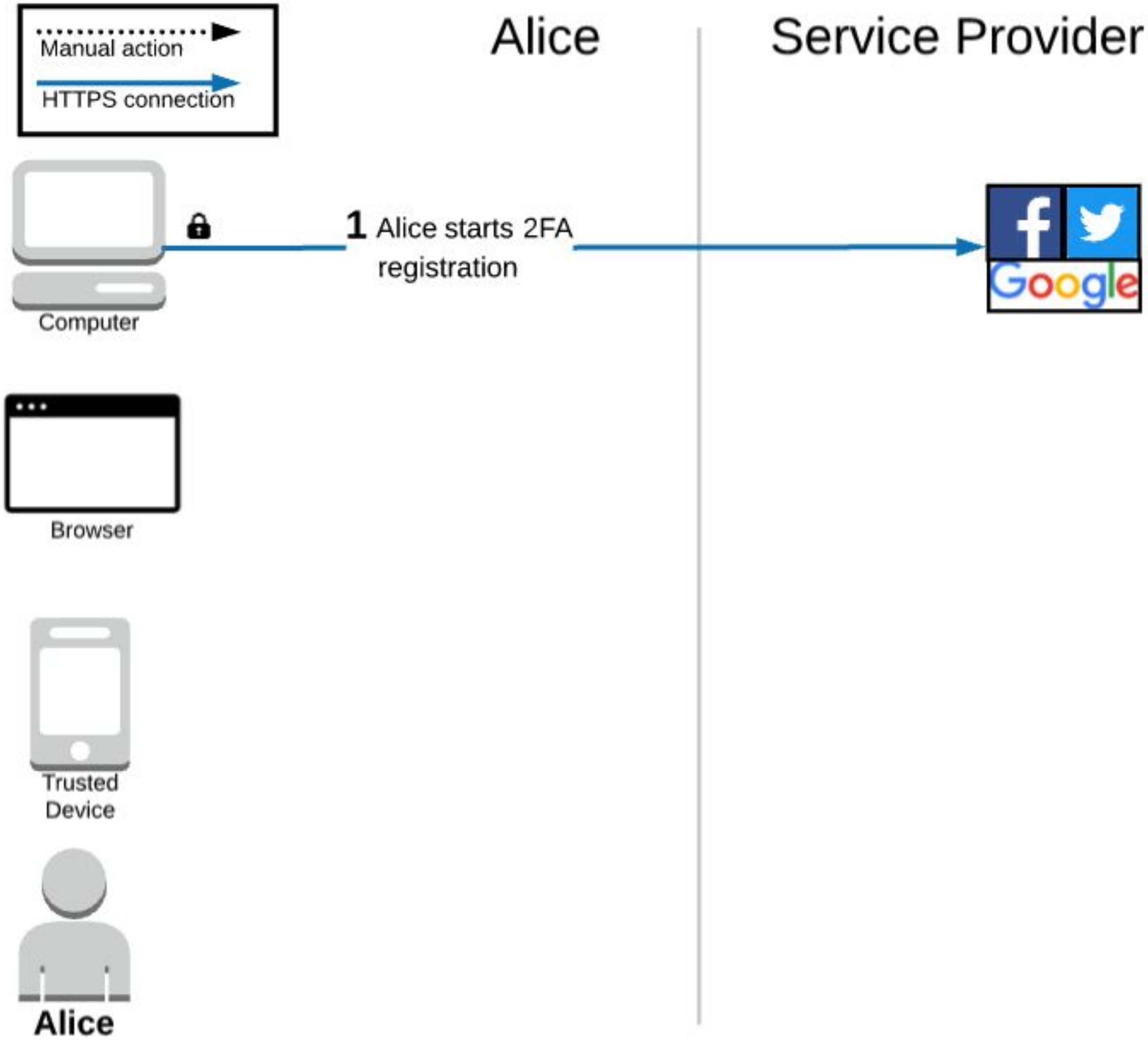
1. What security and privacy issues exist in the backup & recovery functionality of prevalent TOTP 2FA apps?
2. How can they be fixed?

# Research Questions

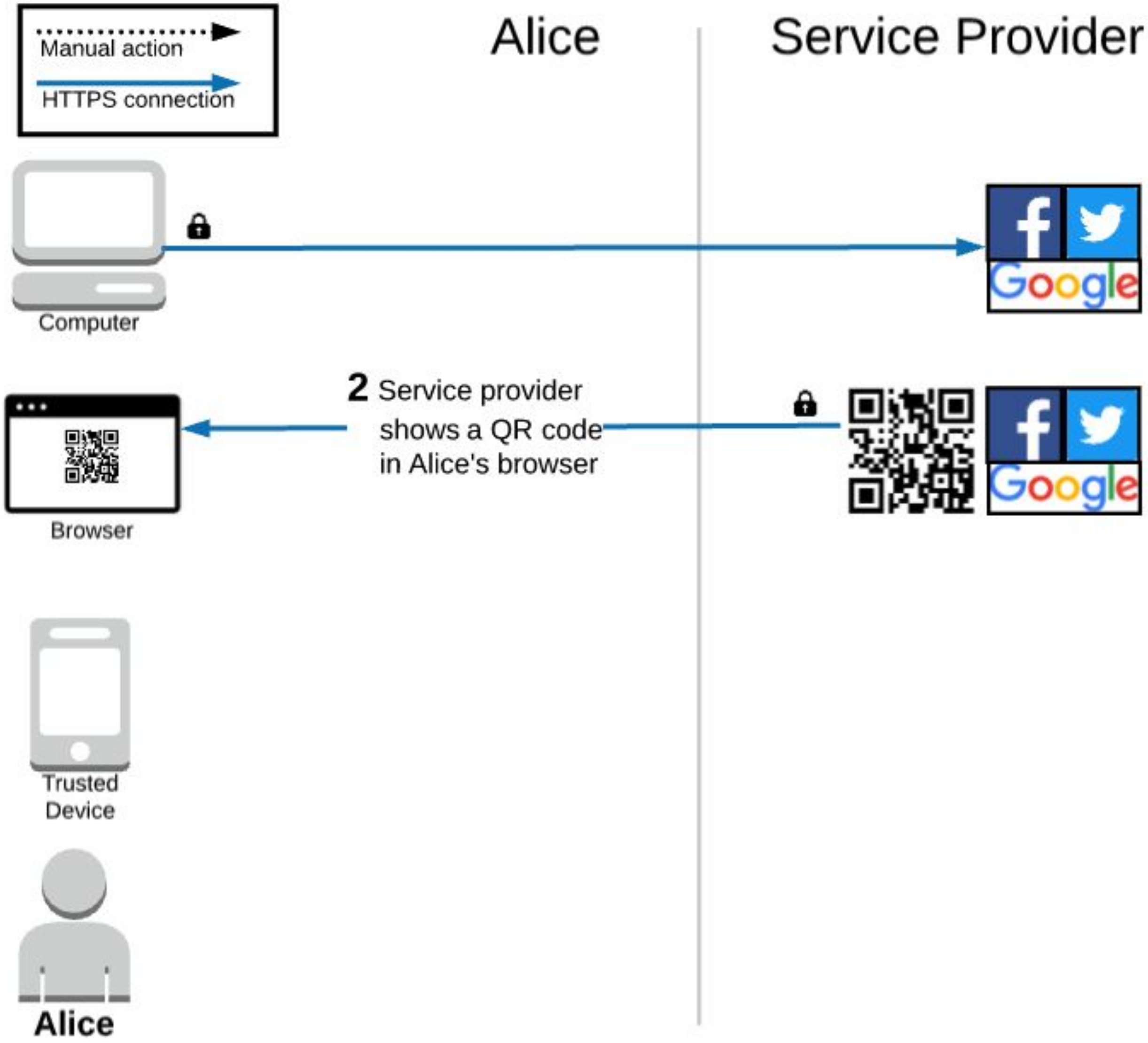
1. What security and privacy issues exist in the backup & recovery functionality of prevalent TOTP 2FA apps?
2. How can they be fixed?

# Background & Motivation

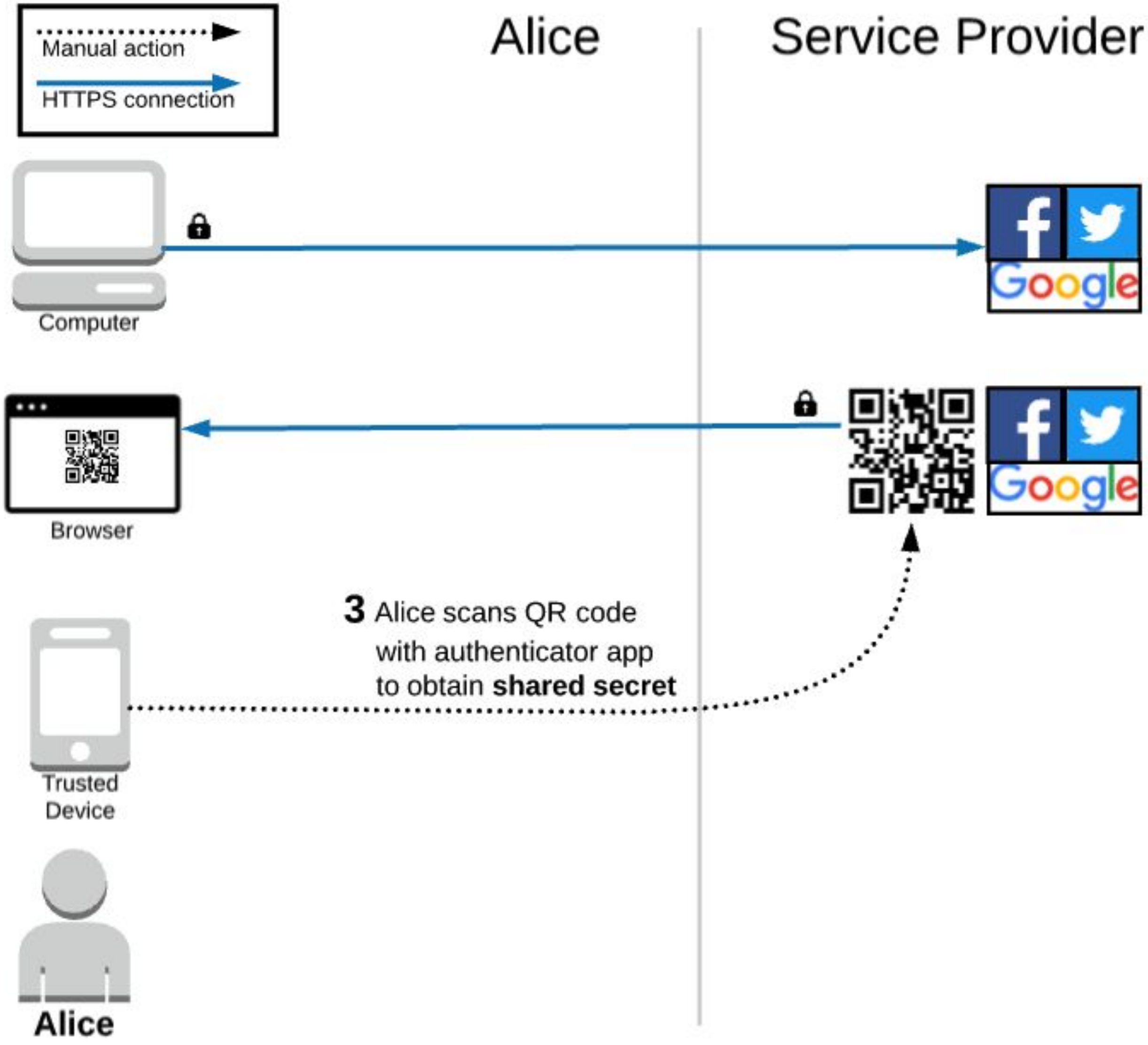
# TOTP


Manual action
HTTPS connection
Alice
Service Provider
Computer
1 Alice starts 2FA registration
Google
Browser
Trusted Device
Alice

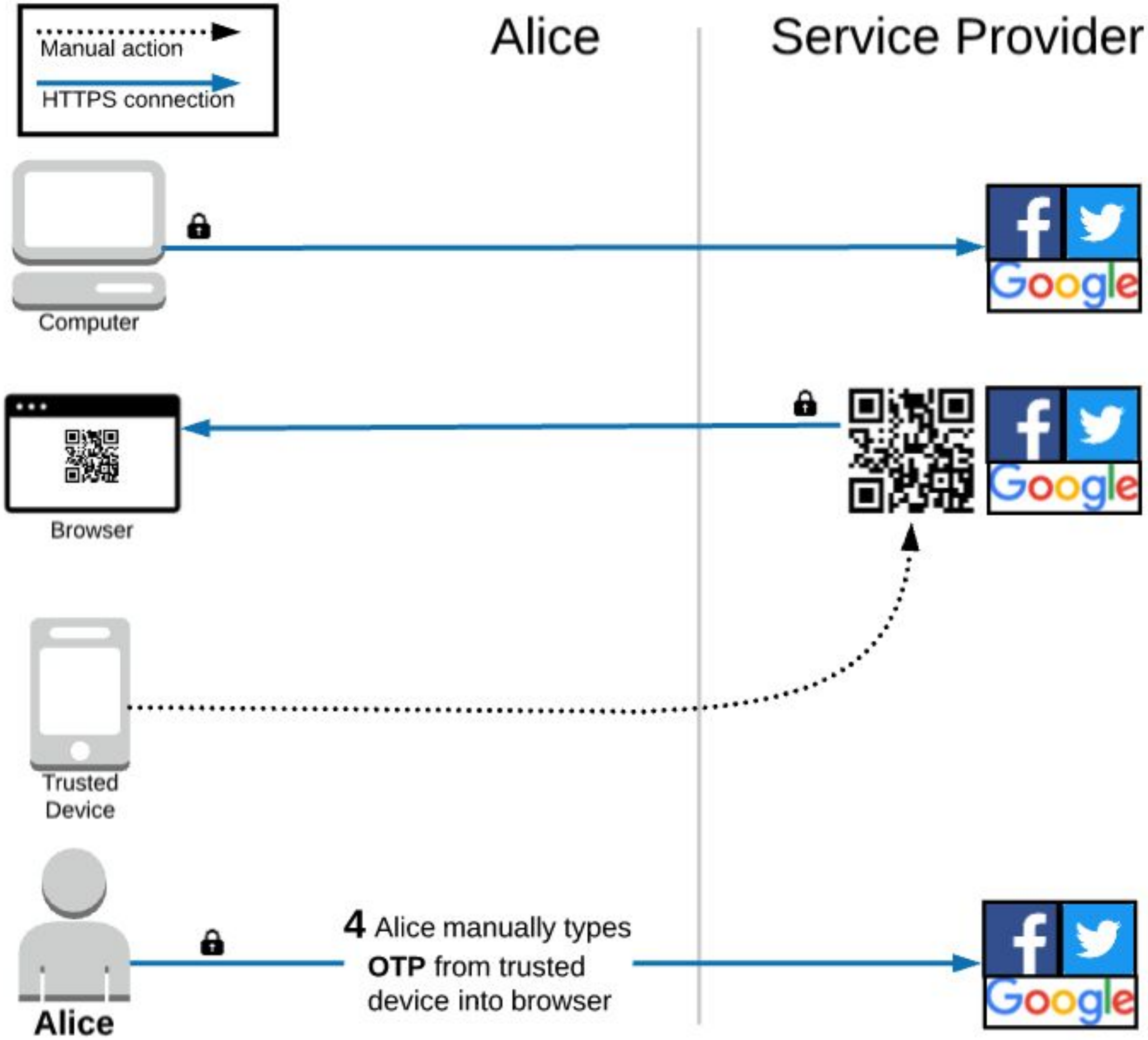
# TOTP


Manual action
HTTPS connection
Alice
Service Provider
Computer
Google
2 Service provider shows a QR code in Alice's browser
Browser
Google
Trusted Device
Alice

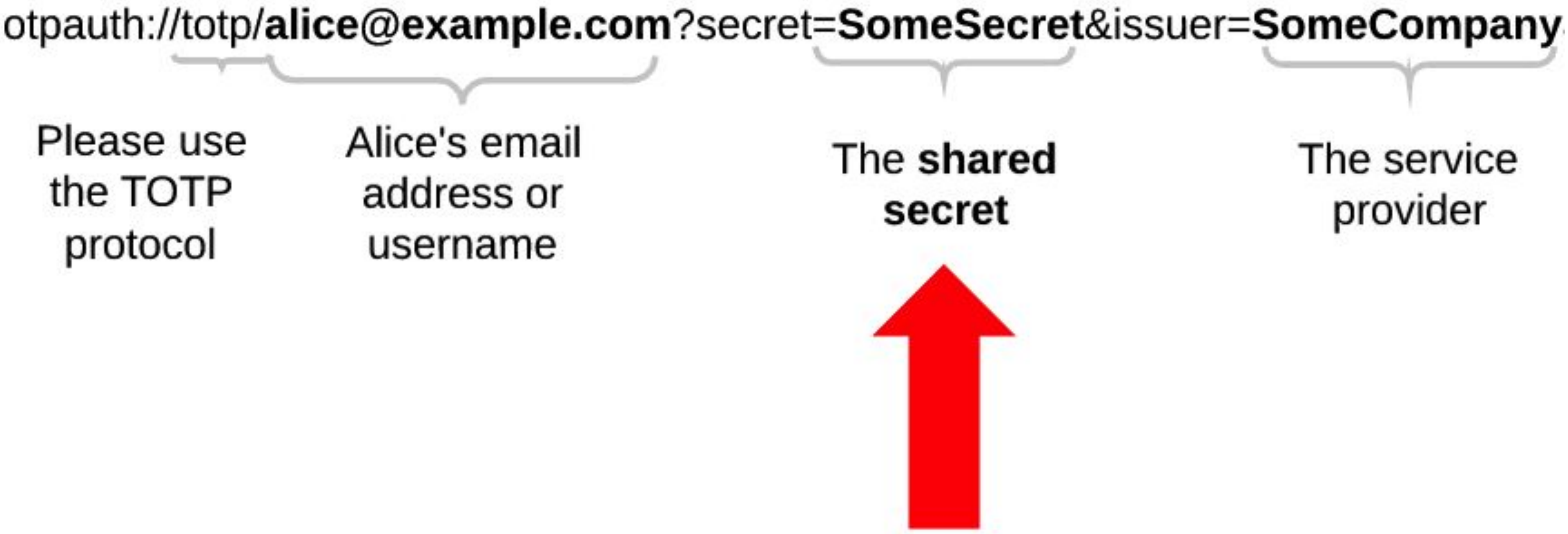
# TOTP


Manual action
HTTPS connection
Alice
Service Provider
Computer
Google
Browser
Google
3 Alice scans QR code with authenticator app to obtain **shared secret**
Trusted Device
Alice

# TOTP


Manual action
HTTPS connection
Alice
Service Provider
Computer
Google
Browser
Google
Trusted Device
4 Alice manually types OTP from trusted device into browser
Alice
Google

# TOTP: QR Code



otpauth://totp/**alice@example.com**?secret=**SomeSecret**&issuer=**SomeCompany**

Please use the TOTP protocol

Alice's email address or username

The **shared secret**

The service provider

👩🏾‍💻 👨🏼‍💻 👩🏽‍💻 👨🏿‍💻 👩🏼‍💻 👨🏾‍💻

# Anyone can build a TOTP 2FA app!

# Dozens of TOTP Apps

Blizzard Authenticator
Blizzard Entertainment, Inc.

2FA Authenticator (2FAS)
2FAS

LastPass Authenticator
LogMeIn, Inc.

FreeOTP Authenticator
Red Hat

Duo Mobile
Duo Security, Inc.

andOTP - Android OTP Authenticator
Jakob Nixdorf

SAASPASS Authenticator 2FA App & Password Manager
SAASPASS

Microsoft Authenticator
Microsoft Corporation

Salesforce Authenticator
Salesforce.com, inc.

Authy 2-Factor Authentication
Authy

TOTP Authenticator – 2FA with Backup & Restore
BinaryBoot

Google Authenticator
Google LLC

👩🏾‍💻 👨🏼‍💻 👩🏽‍💻 👨🏿‍💻 👩🏼‍💻 👨🏾‍💻

# How should our app generate the OTP?

# TOTP: Generate & Verify OTP

## RFC says:

OTP ≈ HMAC-SHA-1 (**shared secret** + **time**)

RFC6238 - https://tools.ietf.org/html/rfc6238

👩🏿‍💻 👨🏼‍💻 👩🏽‍💻 👨🏿‍💻 👩🏼‍💻 👨🏾‍💻

# How should our app backup the secret?

# TOTP: Backup the secret

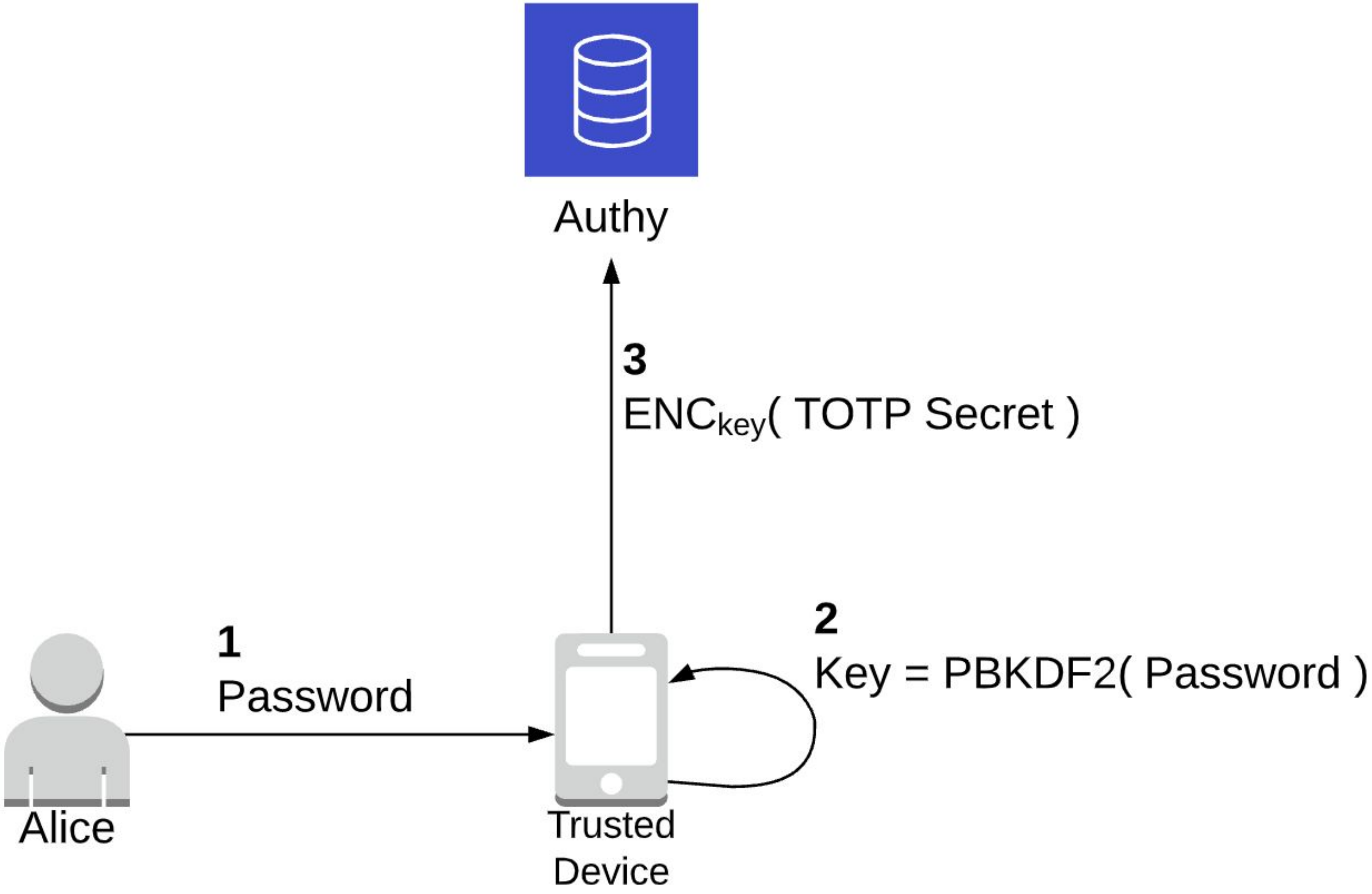
## RFC says:

🤔 🤨 🧐 😕 😴

RFC6238 - [https://tools.ietf.org/html/rfc6238](https://tools.ietf.org/html/rfc6238)

# Authy 2-Factor Authentication

Authy



https://authy.com/blog/how-the-authy-two-factor-backups-work/

# Related Work

# Quantifying password guessability

- People pick **mostly weak** passwords
  - easy for attackers to crack

[1] Bonneau, Joseph. "The science of guessing: analyzing an anonymized corpus of 70 million passwords." *2012 IEEE Symposium on Security and Privacy*.

[2] Bonneau, Joseph, Sören Preibusch, and Ross Anderson. "A birthday present every eleven wallets? The security of customer-chosen banking PINs." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2012.

[3] Ur, Blase, et al. "Measuring real-world accuracies and biases in modeling password guessability." *(USENIX Security 15)*.

# Password Managers

# Password Managers

- Bhargavan and Delignat-Lavaud (2012)
  - ideal: all data is encrypted on the clients
  - reality: flaws in client side implementations

Bhargavan, Karthikeyan, and Antoine Delignat-Lavaud. "Web-based Attacks on Host-Proof Encrypted Storage." *WOOT*. 2012.

Belenko, Andrey, and Dmitry Sklyarov. "“Secure Password Managers” and “Military-Grade Encryption” on Smartphones: Oh, Really?." *Blackhat Europe* (2012): 56.

Li, Zhiwei, et al. "The emperor’s new password manager: Security analysis of web-based password managers."  *(USENIX Security 14)*.

# Password Managers

- Bhargavan and Delignat-Lavaud (2012)
  - ideal: all data is encrypted on the clients
  - reality: flaws in client side implementations
- Belenko and Sklyarov (2012)
  - one day to brute force master passwords up to 10-15 characters in length

Bhargavan, Karthikeyan, and Antoine Delignat-Lavaud. "Web-based Attacks on Host-Proof Encrypted Storage." *WOOT*. 2012.

Belenko, Andrey, and Dmitry Sklyarov. "“Secure Password Managers” and “Military-Grade Encryption” on Smartphones: Oh, Really?." *Blackhat Europe* (2012): 56.

Li, Zhiwei, et al. "The emperor’s new password manager: Security analysis of web-based password managers." *(USENIX Security 14)*.

# Password Managers

- Bhargavan and Delignat-Lavaud (2012)
  - ideal: all data is encrypted on the clients
  - reality: flaws in client side implementations
- Belenko and Sklyarov (2012)
  - one day to brute force master passwords up to 10-15 characters in length
- Li et. al. (2014)
  - Analyzed 5 web-based password managers
  - Not enough detail to replicate

Bhargavan, Karthikeyan, and Antoine Delignat-Lavaud. "Web-based Attacks on Host-Proof Encrypted Storage." *WOOT*. 2012.

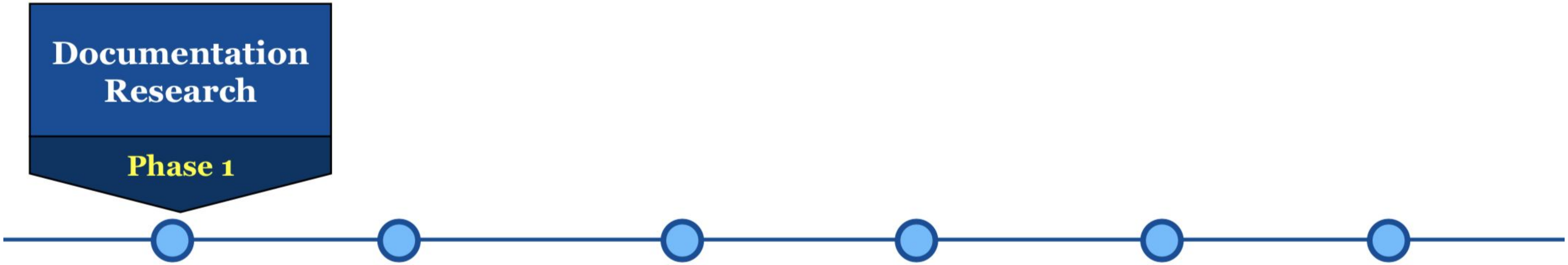
Belenko, Andrey, and Dmitry Sklyarov. "“Secure Password Managers” and “Military-Grade Encryption” on Smartphones: Oh, Really?." *Blackhat Europe* (2012): 56.

Li, Zhiwei, et al. "The emperor’s new password manager: Security analysis of web-based password managers." *(USENIX Security 14)*.

# Analysis Workflow

## Case-Study: Authy 2FA

# Documentation Research

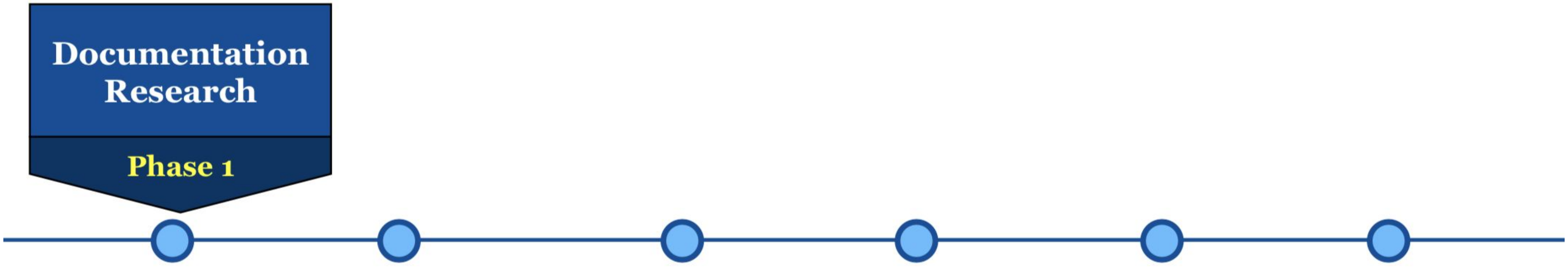

Documentation Research

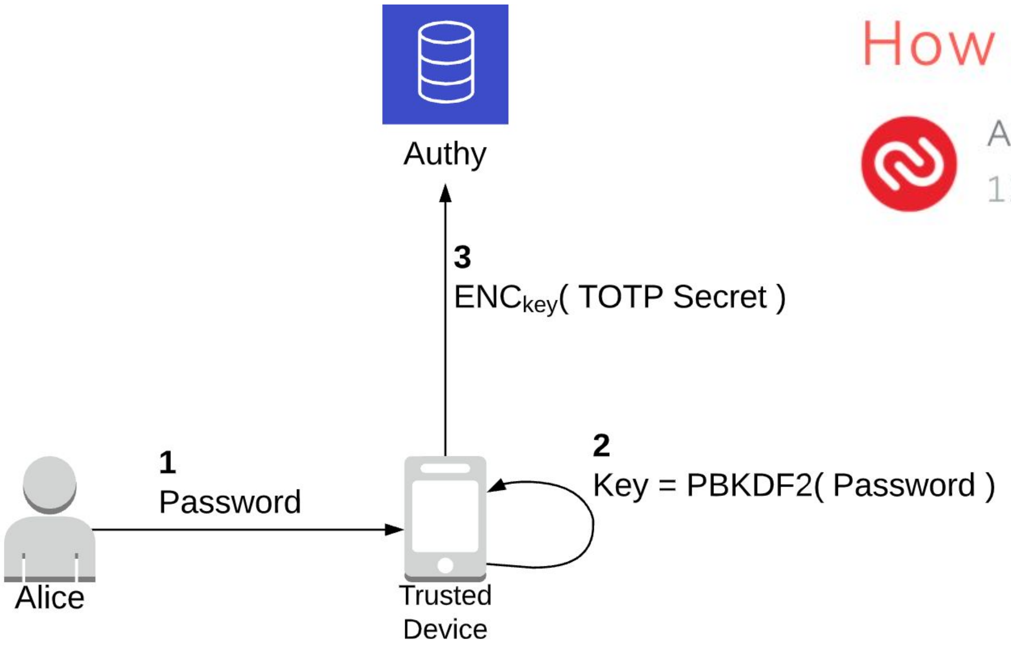
Phase 1

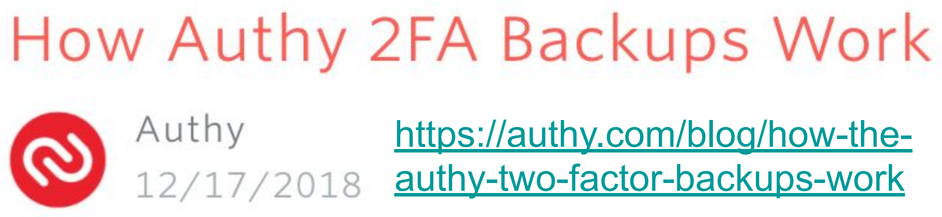
## Goals

1. Gather published technical details
   a. Do not start analysis blind

# Documentation Research







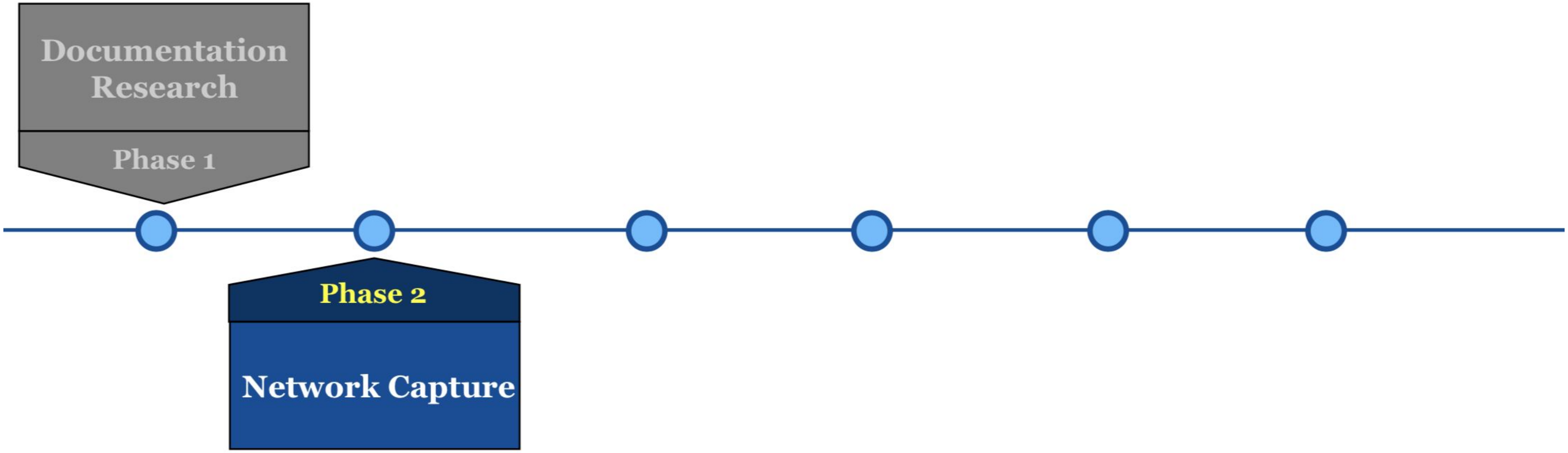
How Authy 2FA Backups Work

Authy

12/17/2018

https://authy.com/blog/how-the-authy-two-factor-backups-work

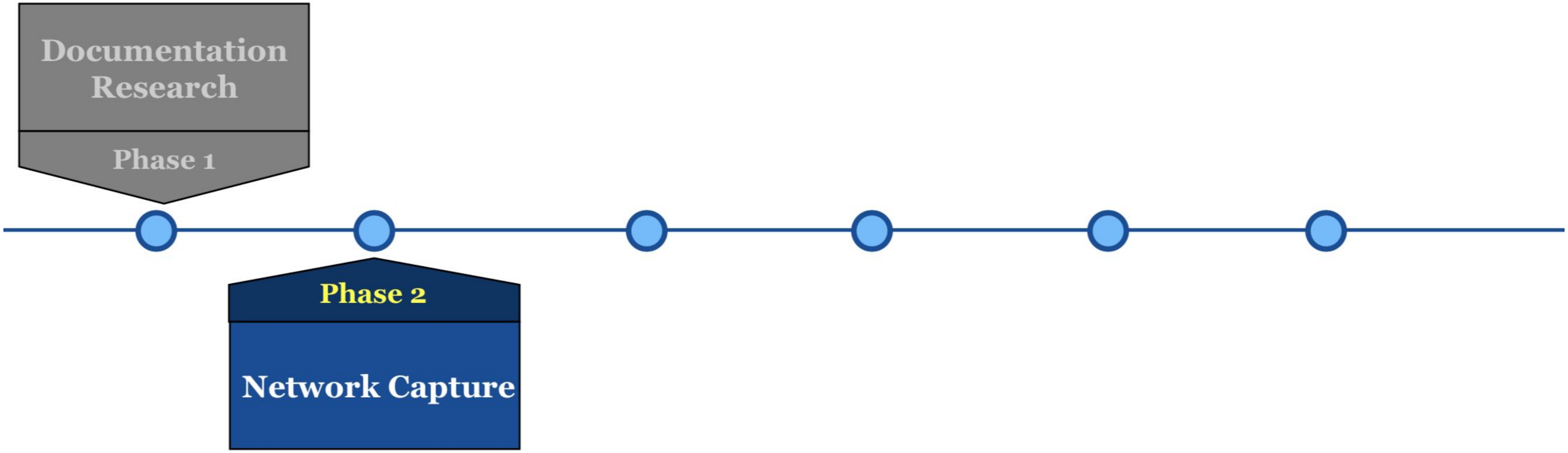
# Network Capture



**Goals**

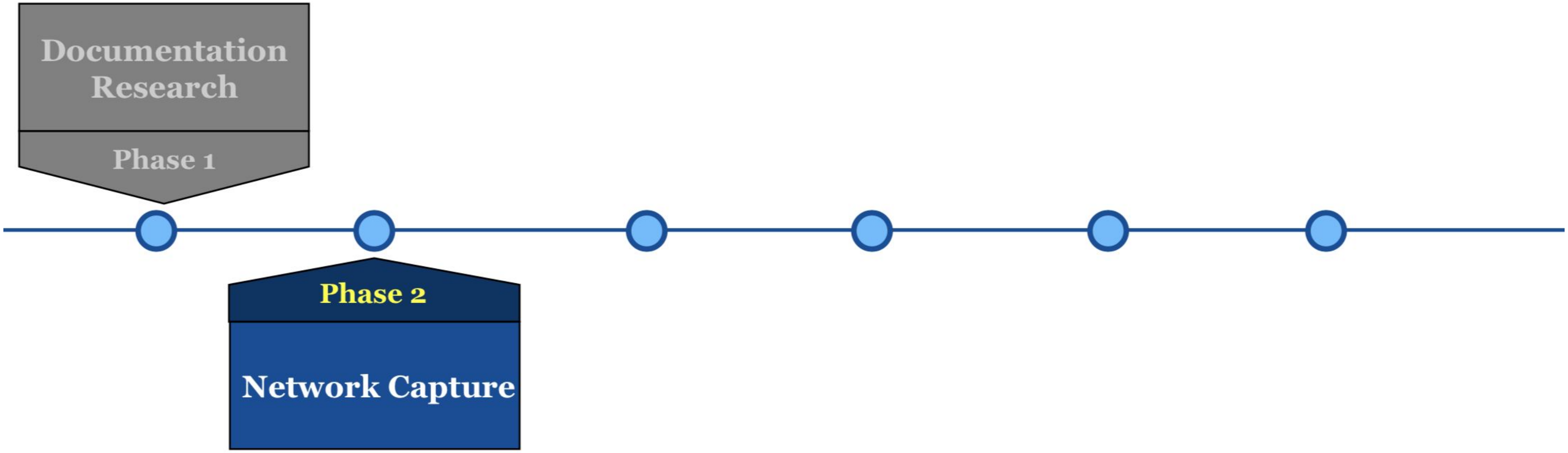
1. Obtain ciphertext.
2. Which fields are not encrypted?
3. Personal information required?

# Network Capture



- Take specific actions using the app
  - Add 1$^{st}$ TOTP secret
  - Enable backup
  - Add 2$^{nd}$ TOTP secret

# Network Capture

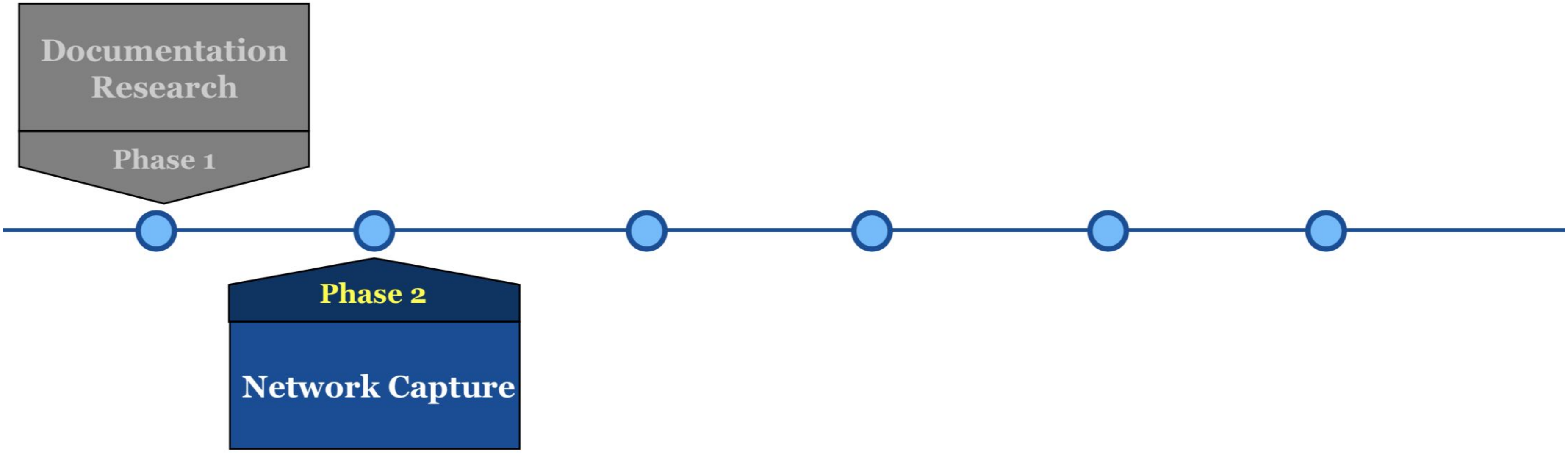


- We captured traffic on-device before TLS
  - closed source tools from Reardon et al

Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. In *Proceedings of the 28th USENIX Security Symposium*, pages 603–620, 2019.

# Network Capture

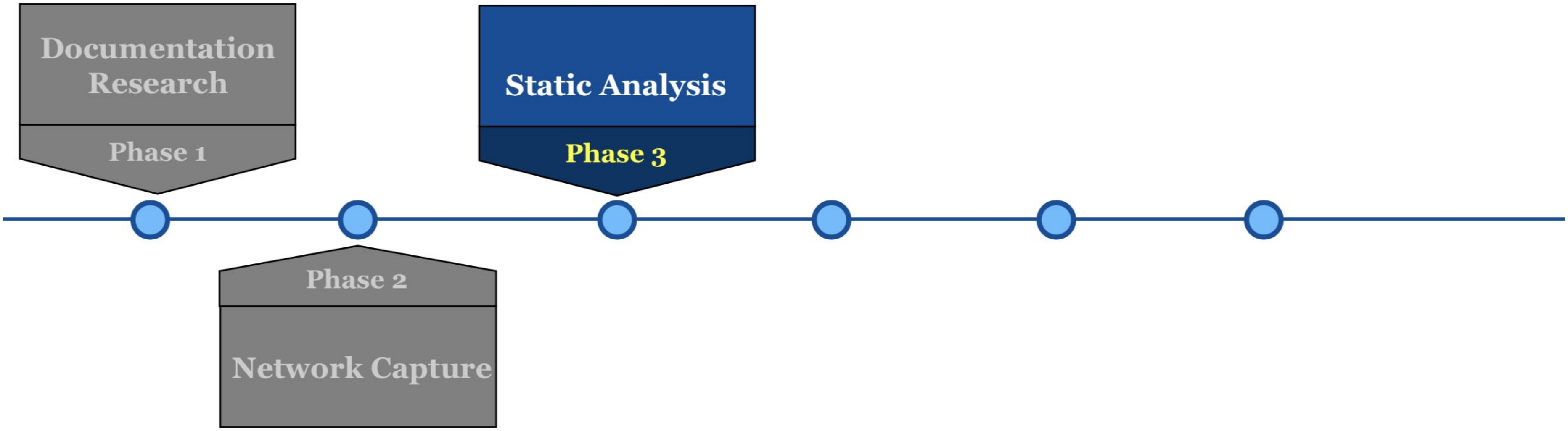
AUTHY
One App for All your Accounts



- We captured traffic on-device before TLS
  - closed source tools from Reardon et al
- Name and issuer fields are **not** encrypted

Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. In *Proceedings of the 28th USENIX Security Symposium*, pages 603–620, 2019.

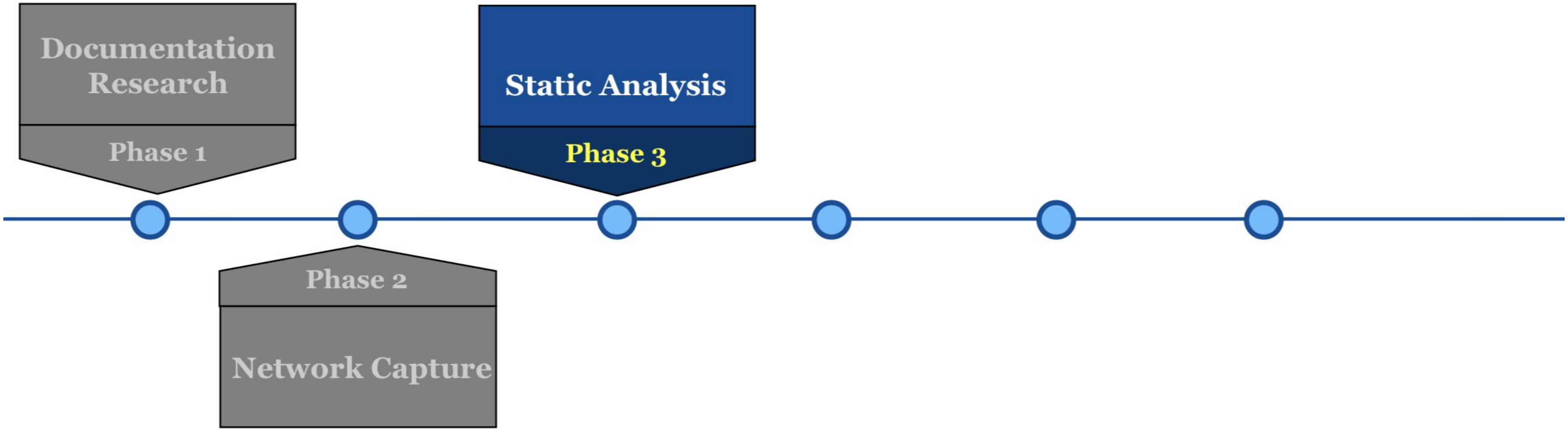
# Static Analysis



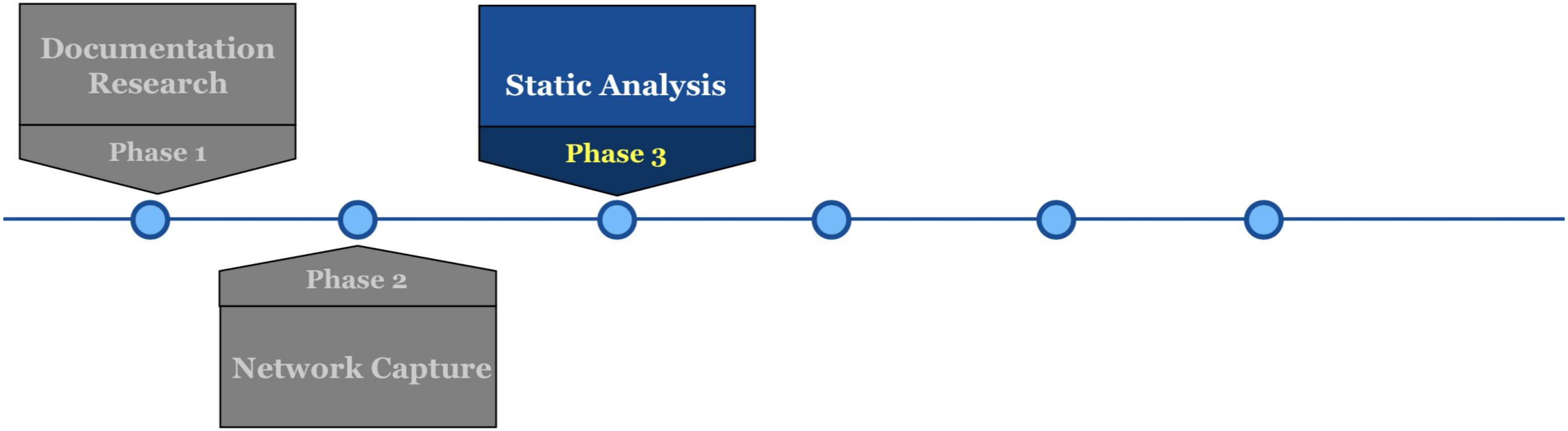
## **Goals**

1. Which crypto is used?
   a. cipher, mode, etc
2. How is <u>decryption</u> verified?
   a. “Sorry, wrong recovery password!”

# Static Analysis



# Static Analysis



Documentation Research

Phase 1

Phase 2

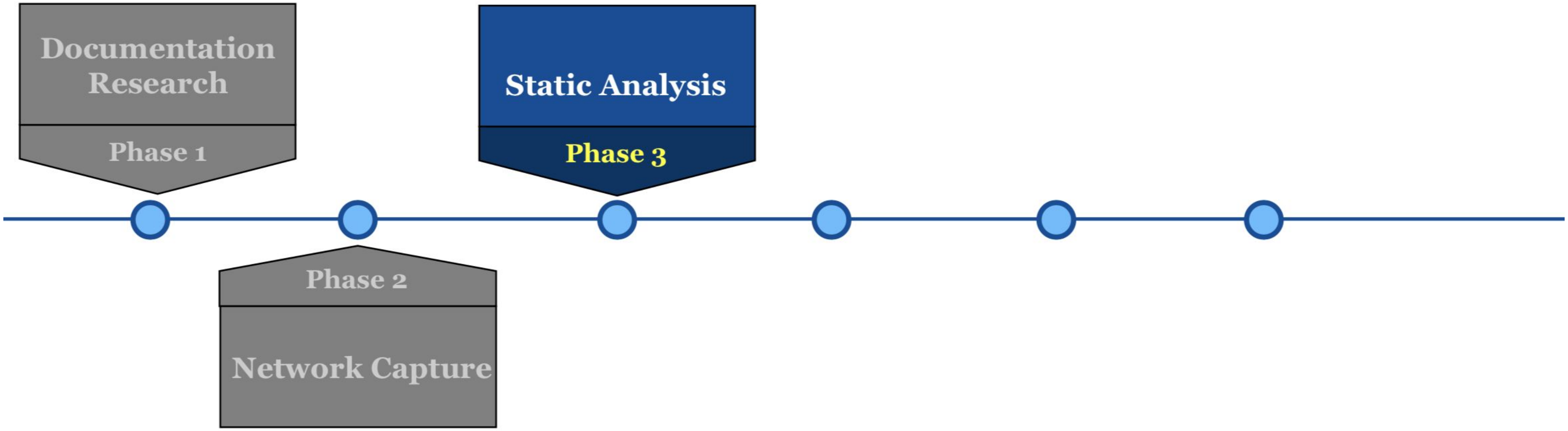
Network Capture

Static Analysis

Phase 3

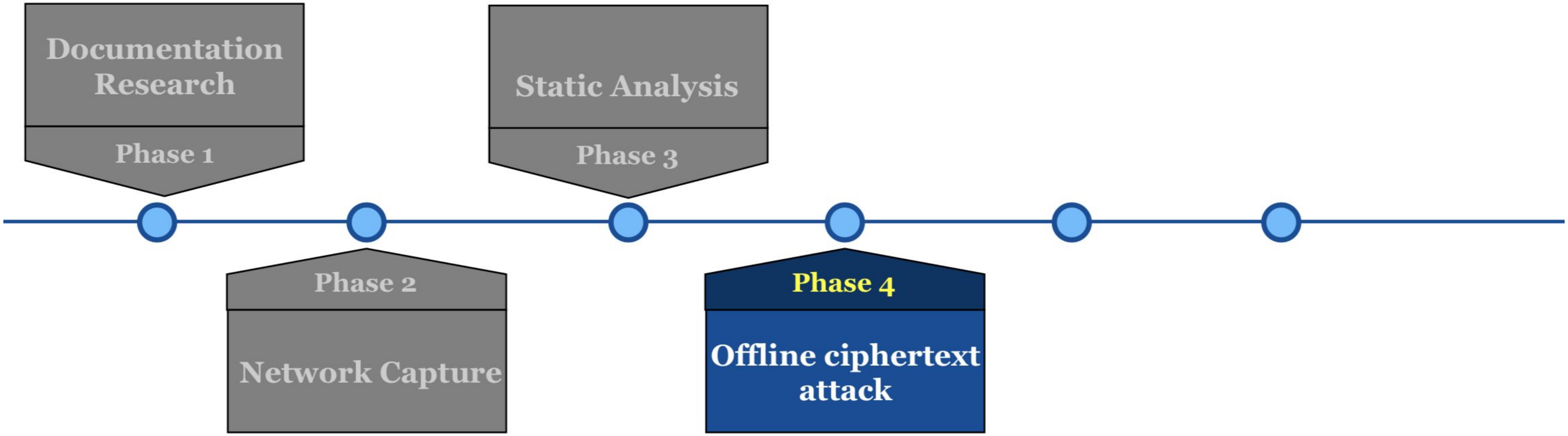
| Encrypted? | | | Key derivation | Cipher & mode | Decryption verification? |
|---|---|---|---|---|---|
| secret | name | issuer | | | |
| Yes | No | No | - PBKDF2<br>- 1k rounds | AES-CBC | Heuristic:<br>Valid Base32? |

# Static Analysis



| Encrypted? | | | Key derivation | Cipher & mode | Decryption verification? |
|---|---|---|---|---|---|
| secret | name | issuer | | | |
| Yes | No | No | - PBKDF2<br>- 1k rounds | AES-CBC | Heuristic:<br>Valid Base32? |

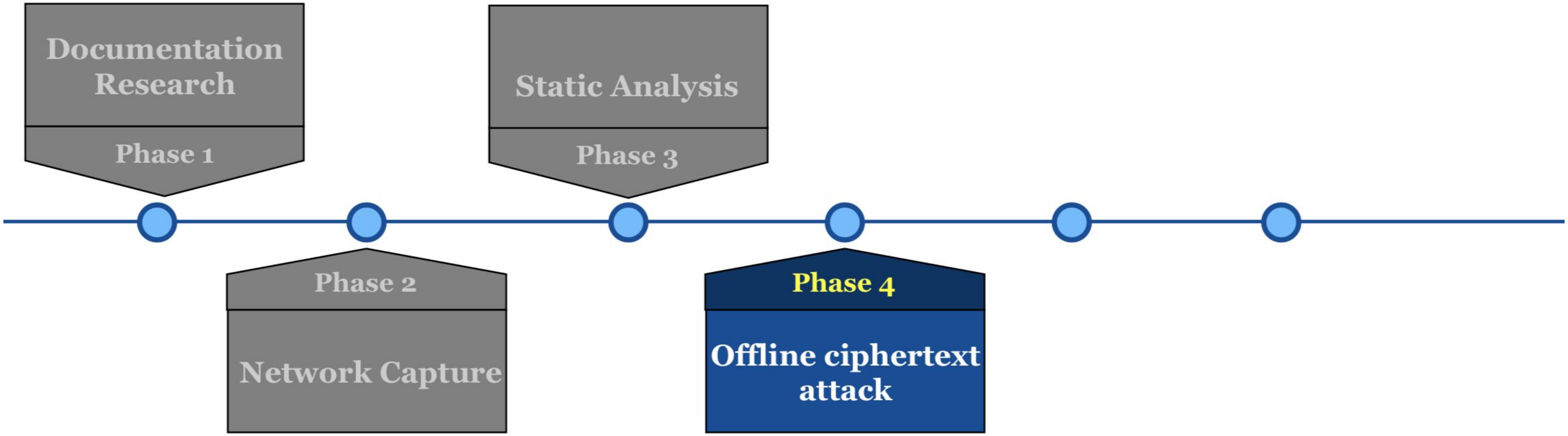
# Attack Ciphertext Offline



**Goals**

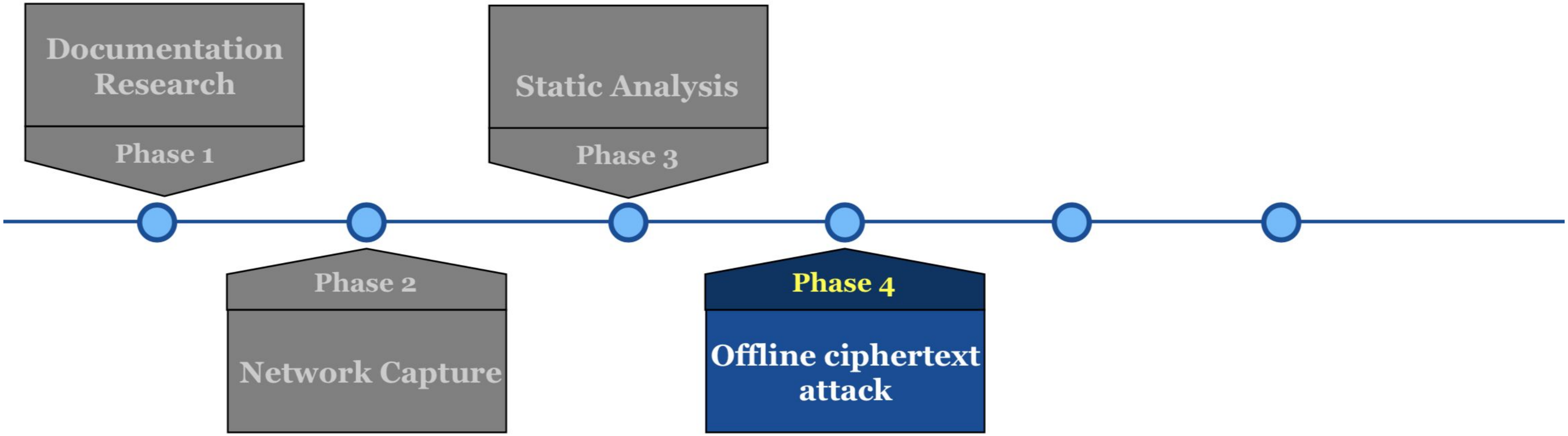
1. Difficulty of ciphertext => plaintext?

# Attack Ciphertext Offline



- Adapt password cracking tools to “crack” ciphertexts
  - e.g. Hashcat module framework

# Attack Ciphertext Offline

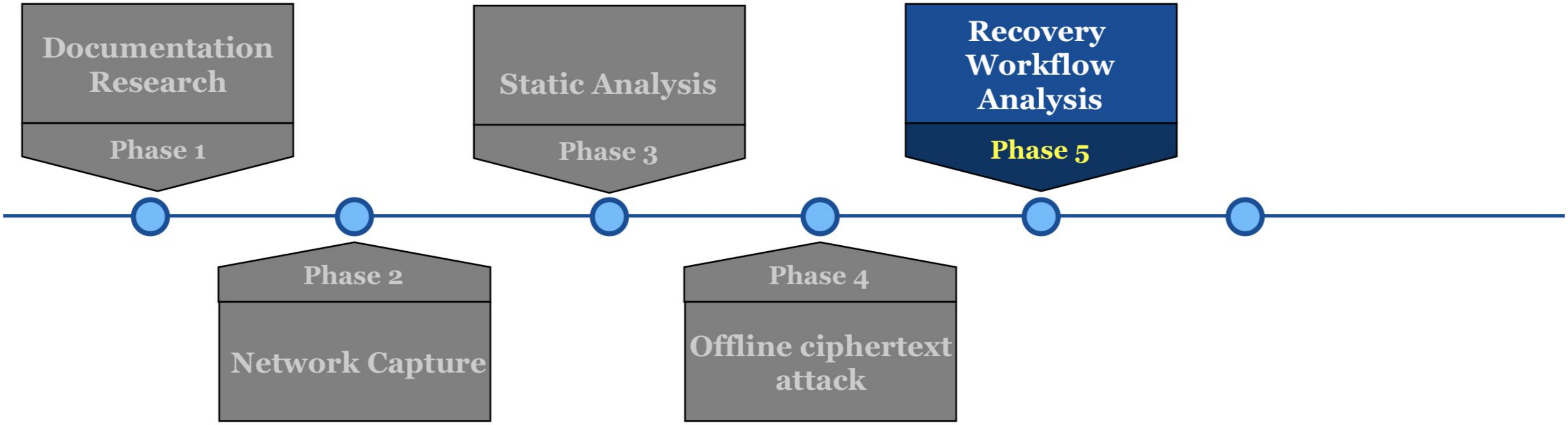


- Base32 heuristic enables offline attacks
  - Effective with **high probability** for weak backup pwds

P(plaintext from single guess is Base32) ≈ $\mathbf{10^{-29}}$

assuming 32 byte / 256 bit secret

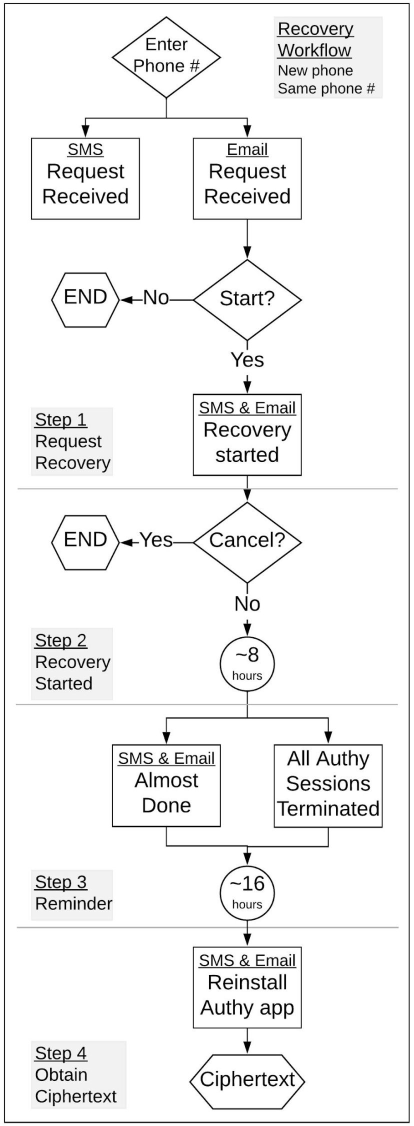
# Recovery Workflow Analysis



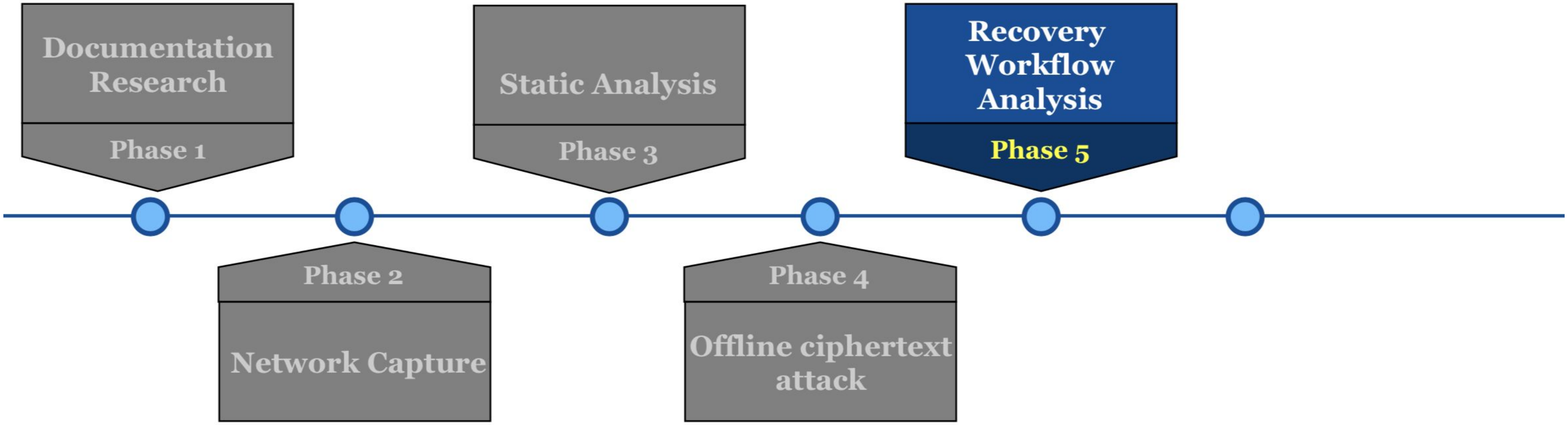
**Goals**

1. Diagram the recovery workflow
   a. How could an attacker access the ciphertext?
   b. Opportunities for user to identify/stop the attack?

# Recovery Workflow Analysis



# Recovery Workflow Analysis



Documentation Research

Phase 1

Phase 2

Network Capture

Static Analysis

Phase 3

Phase 4

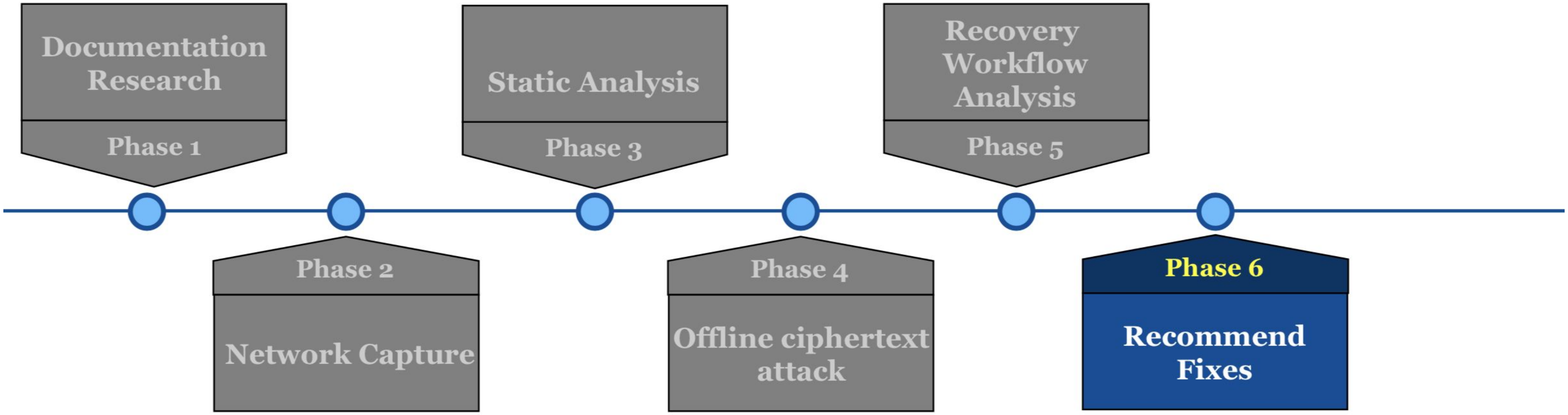
Offline ciphertext attack

Recovery Workflow Analysis

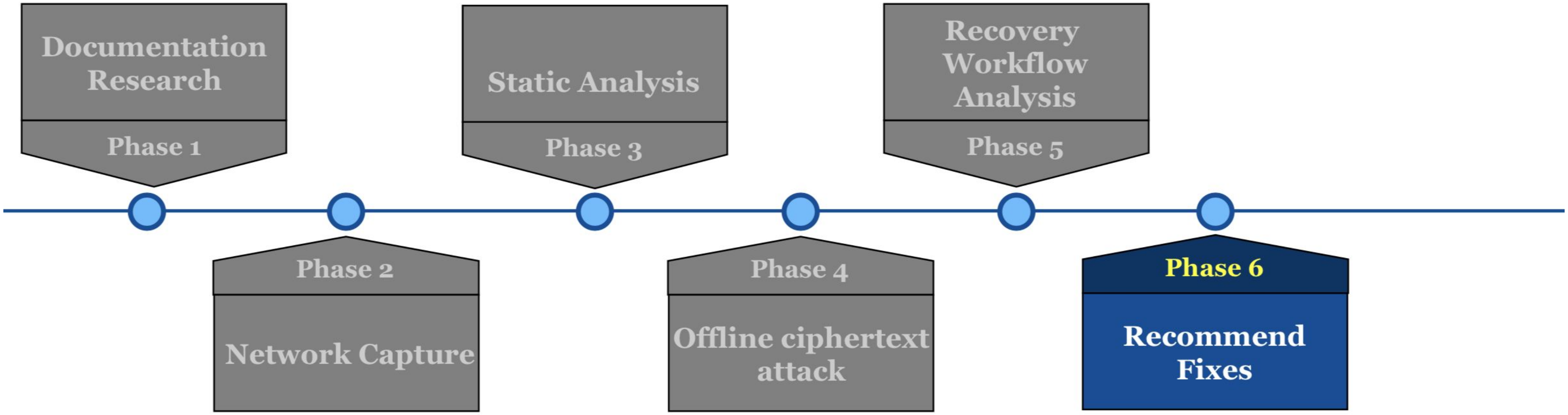
Phase 5

- **Very difficult** to obtain TOTP backups without compromising victim’s email
  - victim must approve recovery request via email
  - 24 hour delay
  - multiple notifications include cancel link

# Recommend Fixes

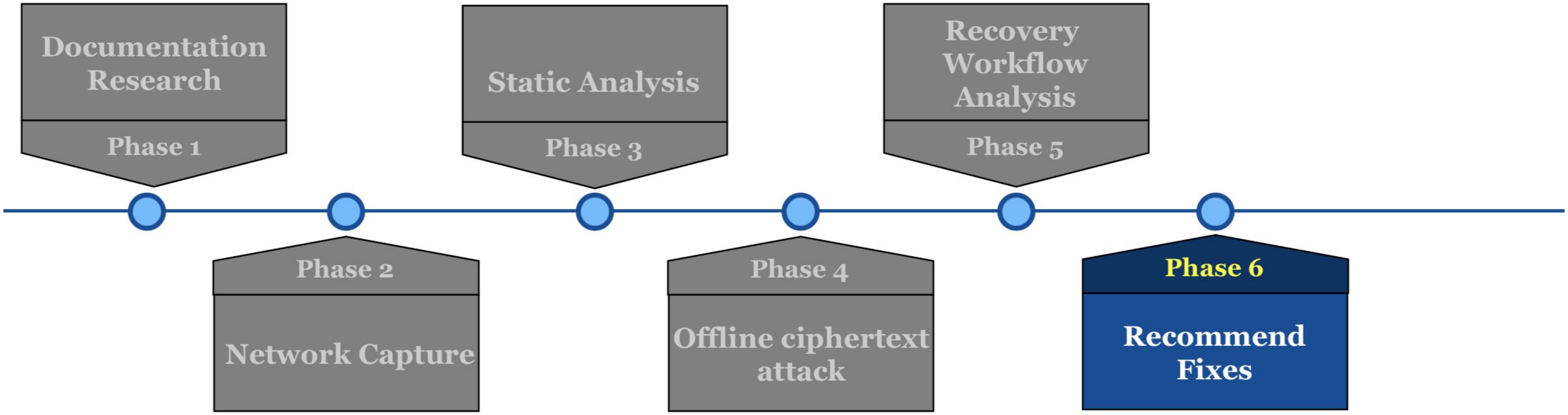


# Recommend Fixes



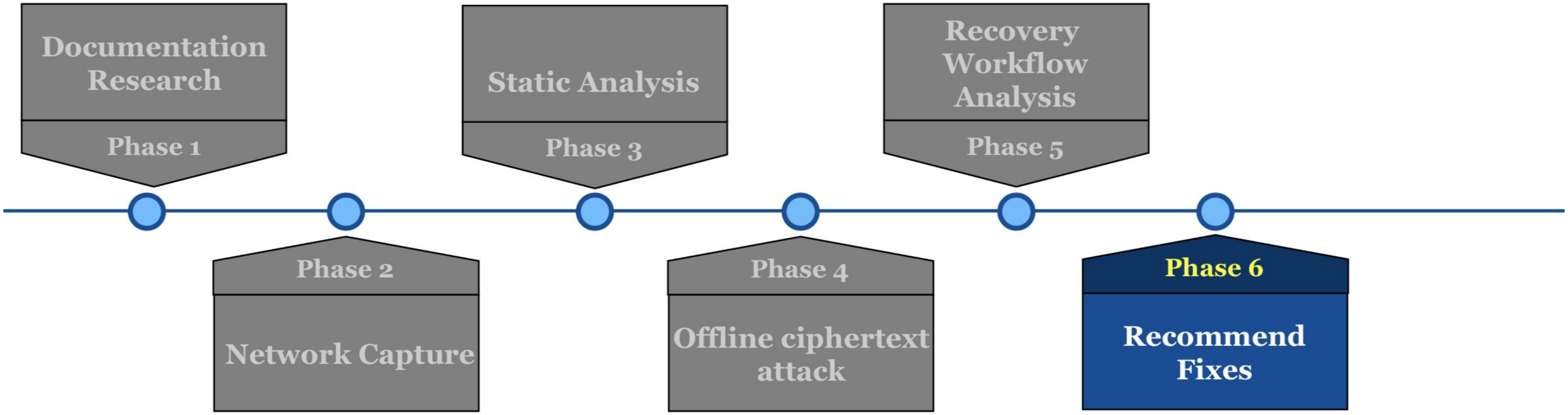
1. Encrypt name and issuer fields

# Recommend Fixes



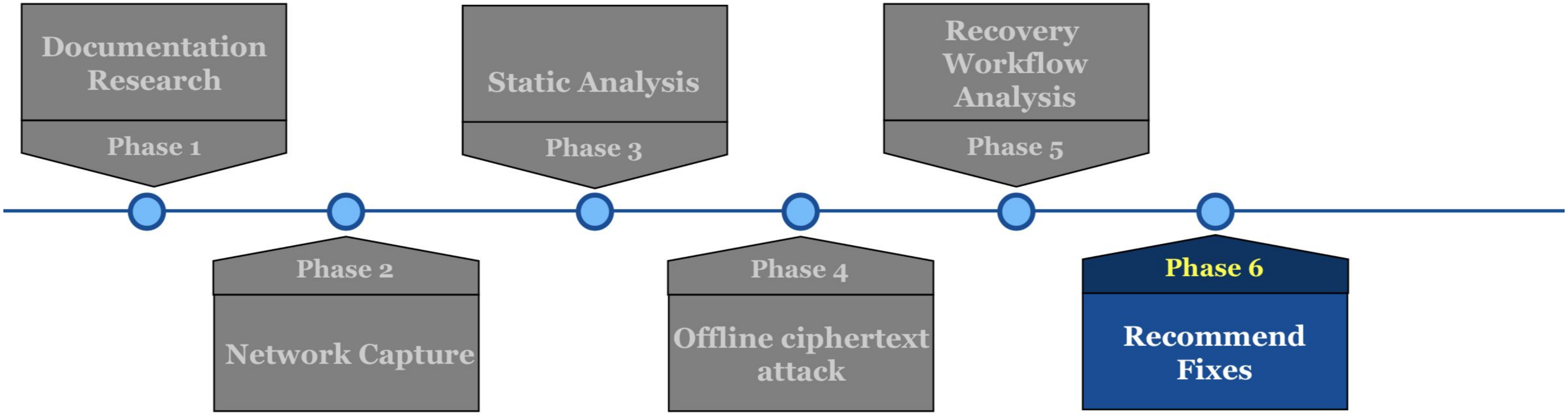
2. Strengthen key derivation
   - use <u>at least</u> 10k rounds for PBKDF2
   - calculate workfactor based on available resources
     - Argon2, bcrypt, or scrypt

# Recommend Fixes



3. Decode Base32 before encryption
   - improves security, but hurts usability

# Responsible Disclosure



# Future Work

Blizzard Authenticator
Blizzard Entertainment, Inc.

2FA Authenticator (2FAS)
2FAS

LastPass Authenticator
LogMeIn, Inc.

FreeOTP Authenticator
Red Hat

Duo Mobile
Duo Security, Inc.

andOTP - Android OTP Authenticator
Jakob Nixdorf

SAASPASS Authenticator 2FA App & Password Manager
SAASPASS

Microsoft Authenticator
Microsoft Corporation

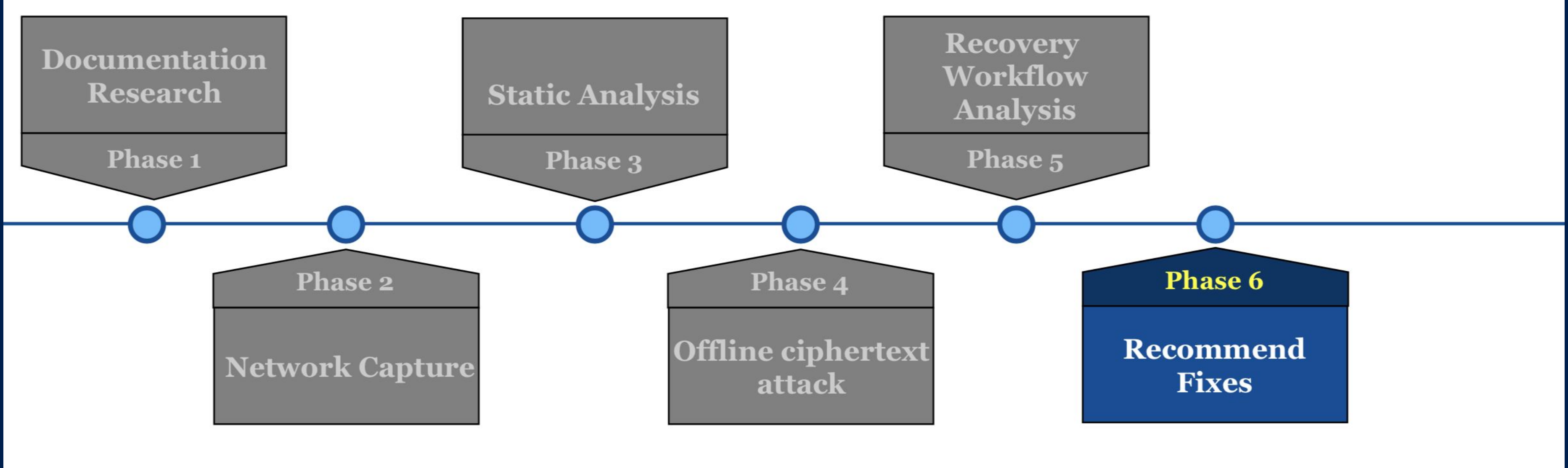
Salesforce Authenticator
Salesforce.com, inc.

Authy 2-Factor Authentication
Authy

TOTP Authenticator – 2FA with Backup & Restore
BinaryBoot

Google Authenticator
Google LLC

# Thank you! Questions?



**Email: conorgilsenan@berkeley.edu**

**Twitter: @conorgil**

Conor Gilsenan
U.C. Berkeley

Noura Alomar
U.C. Berkeley

Serge Egelman
U.C. Berkeley / ICSI