Security & Privacy Analysis Framework For TOTP 2FA apps

Case-Study: Authy 2FA

Conor Gilsenan, Noura Alomar

CS261N - Spring 2020

Agenda

- Research Questions
- Background & Motivation
  - Related work
- Analysis framework
  - Case-study: Authy 2FA

Research Questions

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?

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

Two-Factor Authentication (2FA)

- Knowledge (something you know)
- Possession (something you have)
- Inherence (something you are)

Two-Factor Authentication (2FA)

- Knowledge (something you know)
- Possession (something you have)
- Inherence (something you are)

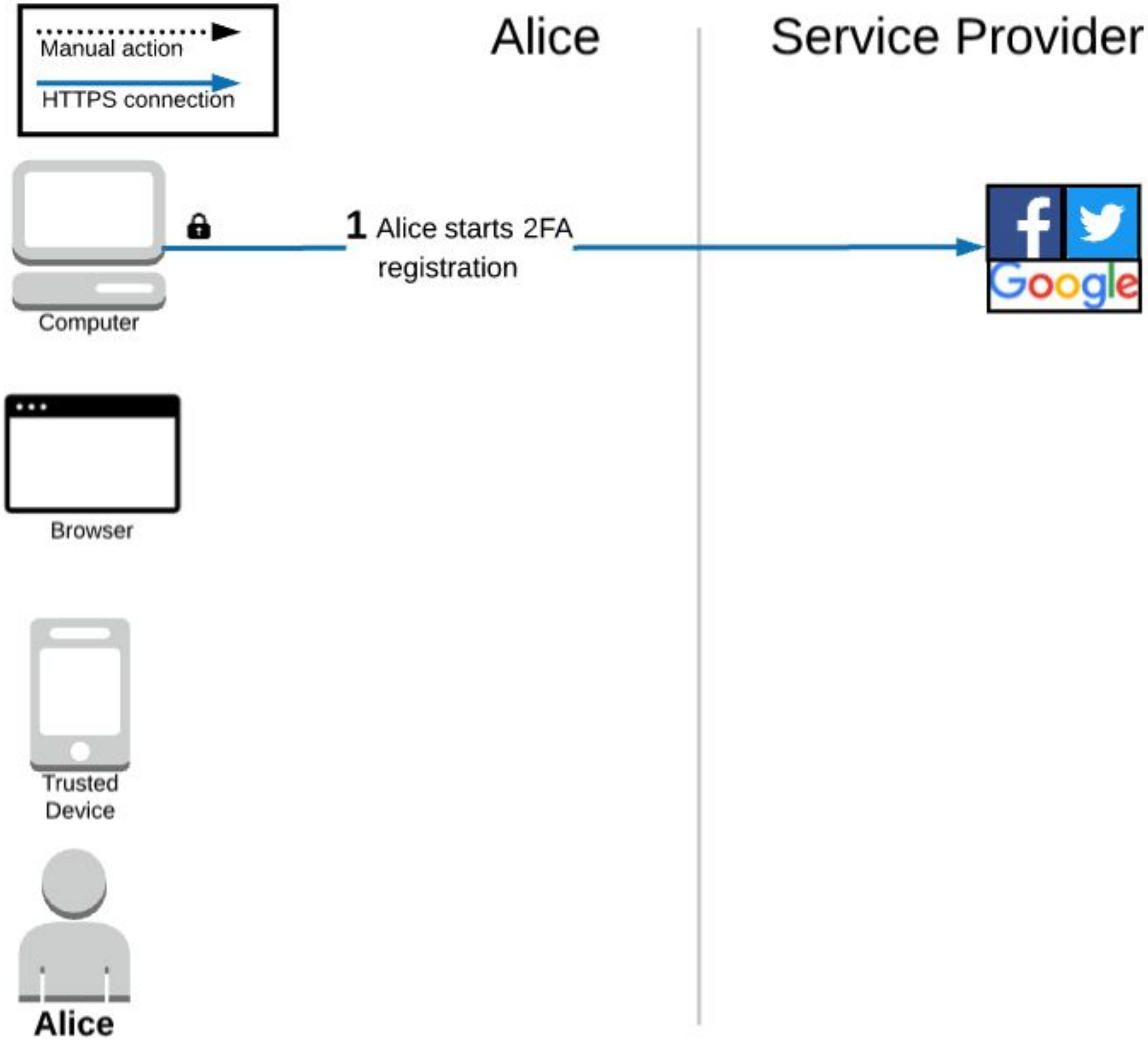
2FA Methods

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

2FA Methods

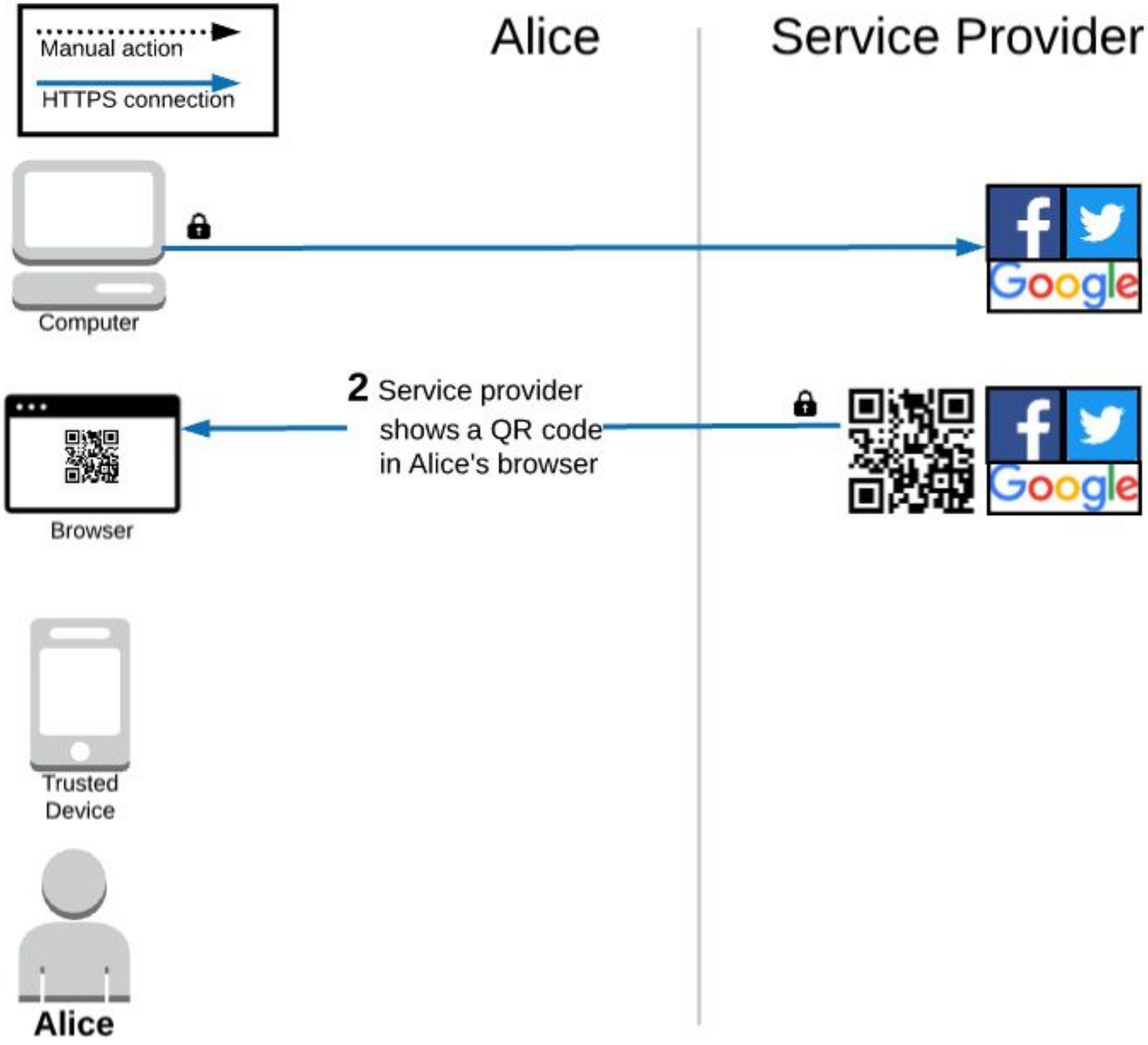
- SMS
- Time-based One-time Passwords (TOTP)
  - e.g. Google Authenticator
- Push notifications
  - e.g. Duo Push
- WebAuthn
  - e.g. USB security keys

TOTP

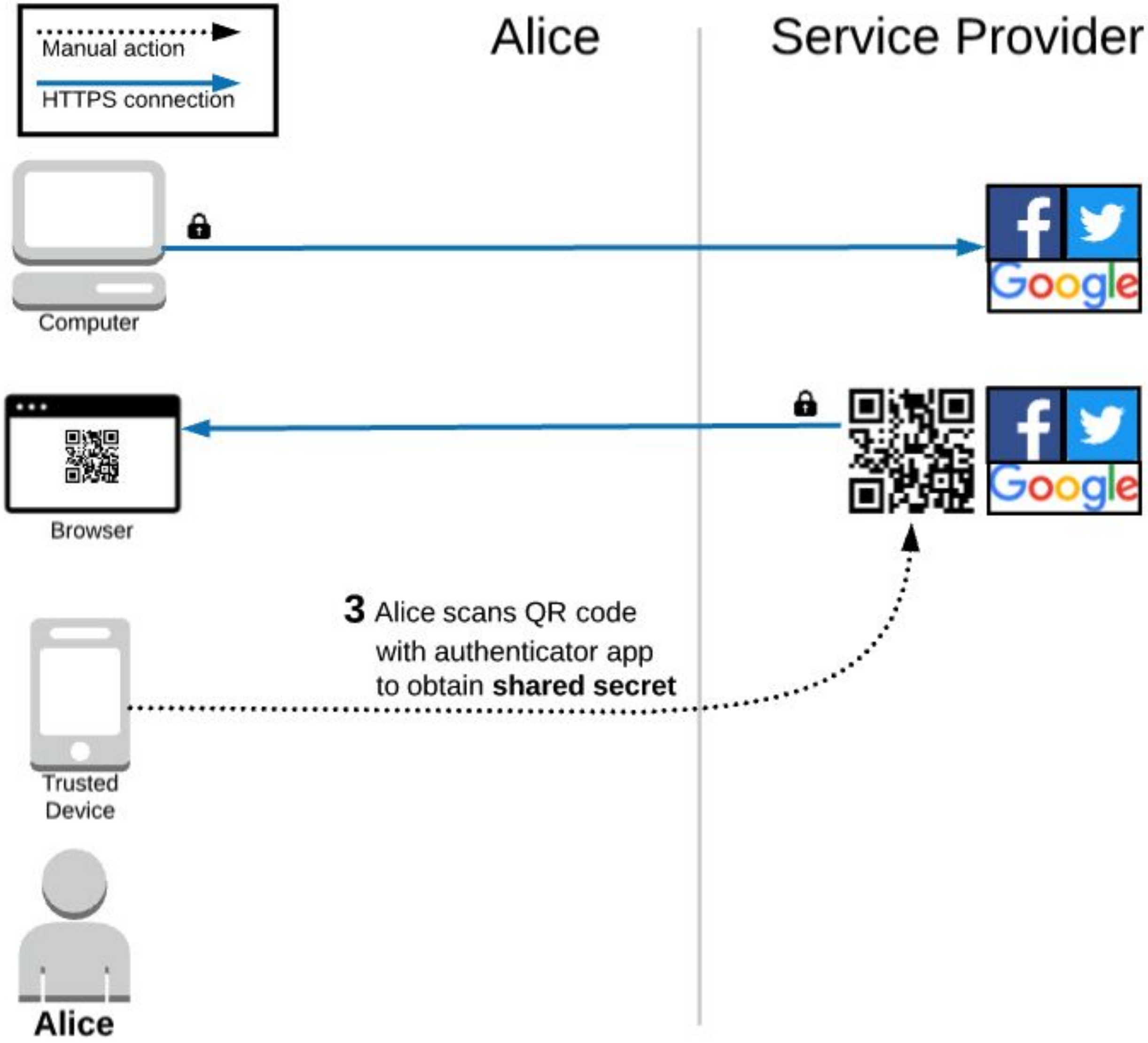


Manual action
HTTPS connection
Alice
Service Provider
Computer
1 Alice starts 2FA registration
Google
Browser
Trusted Device
Alice

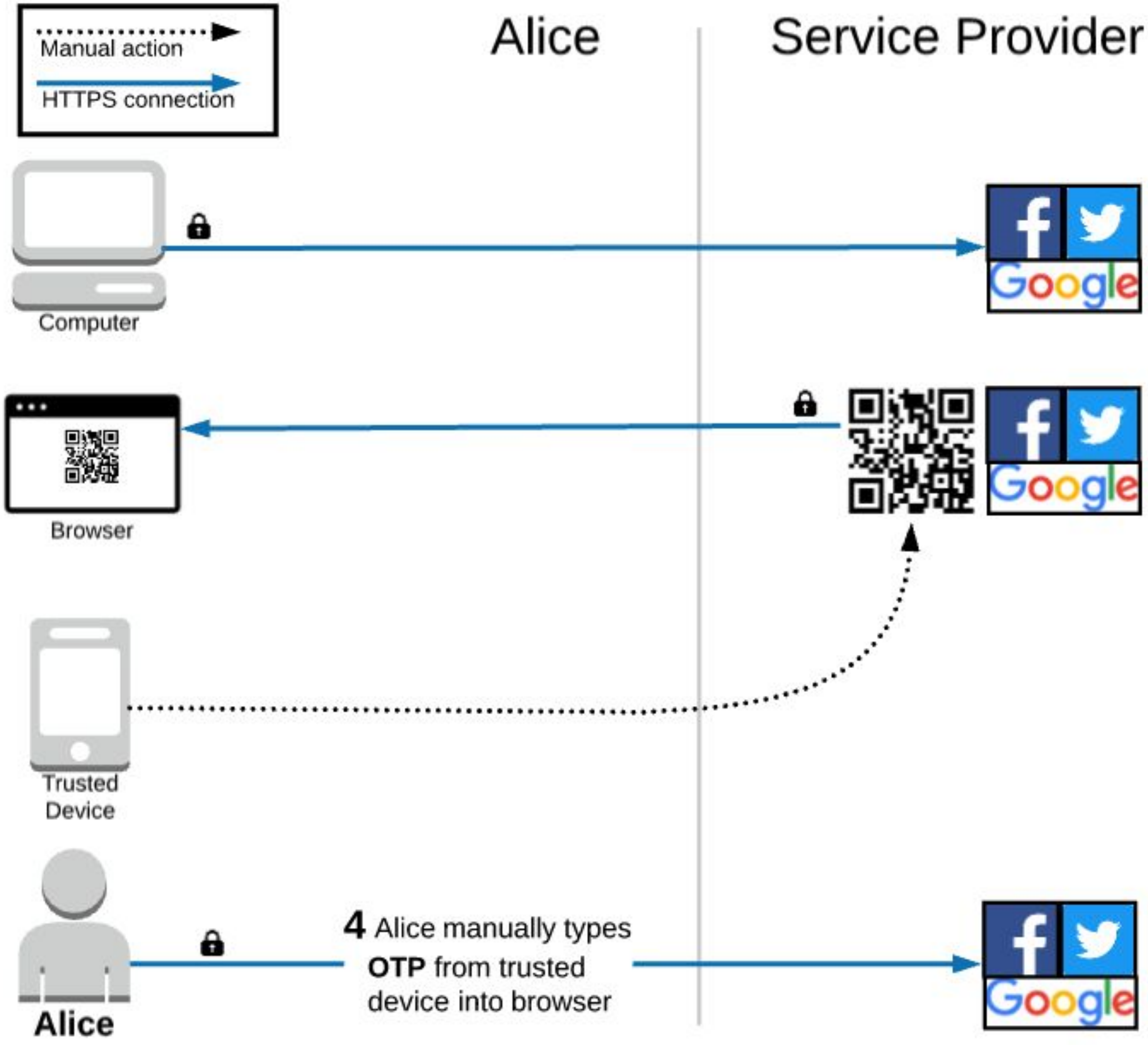
TOTP


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

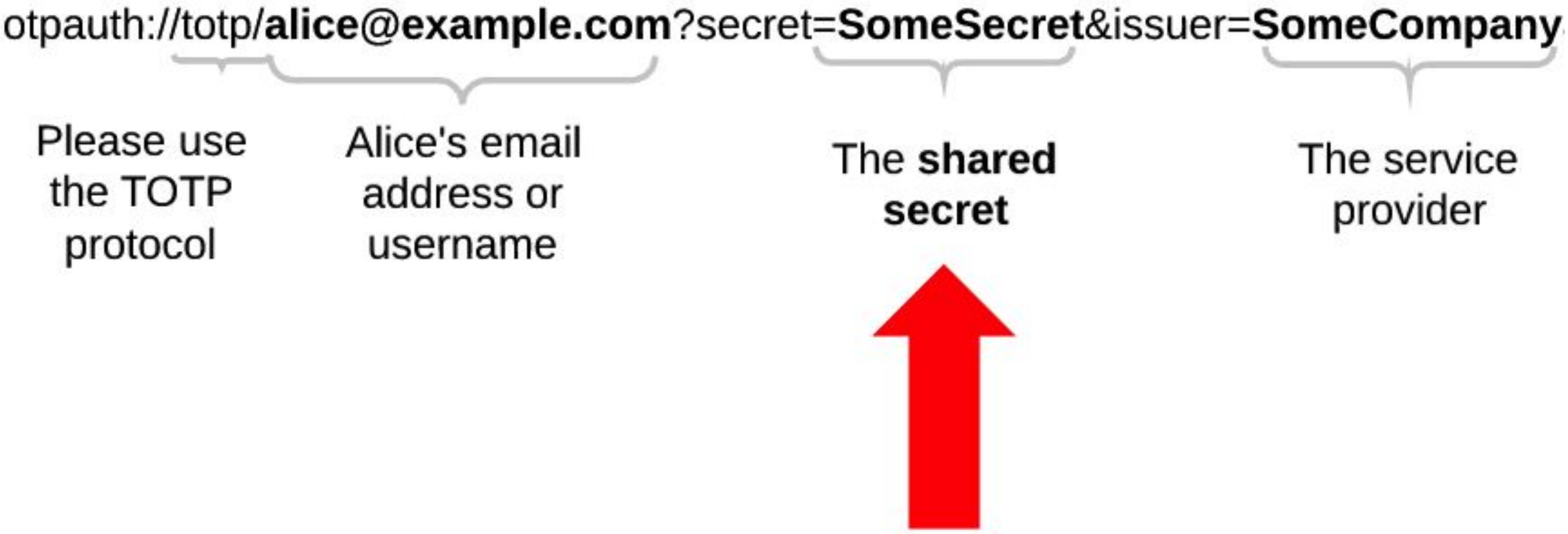
TOTP


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
Alice
4 Alice manually types **OTP** from trusted device into browser
Google

TOTP: QR Code



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

Please use the TOTP protocol

Alice's email address or username

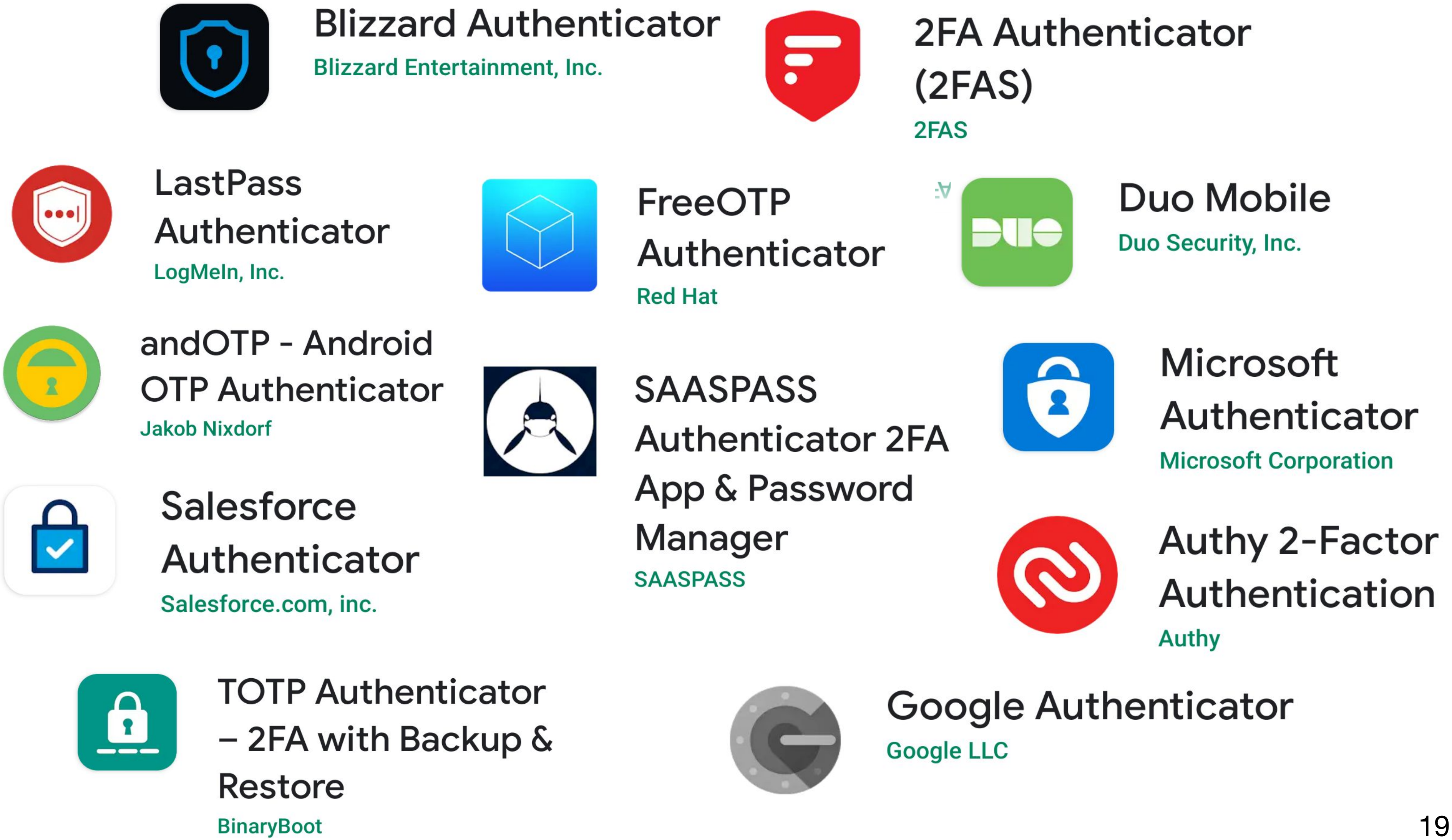
The **shared secret**

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: Generate & Verify OTP

RFC says:

🤔 🤨 🧐 😕 😪

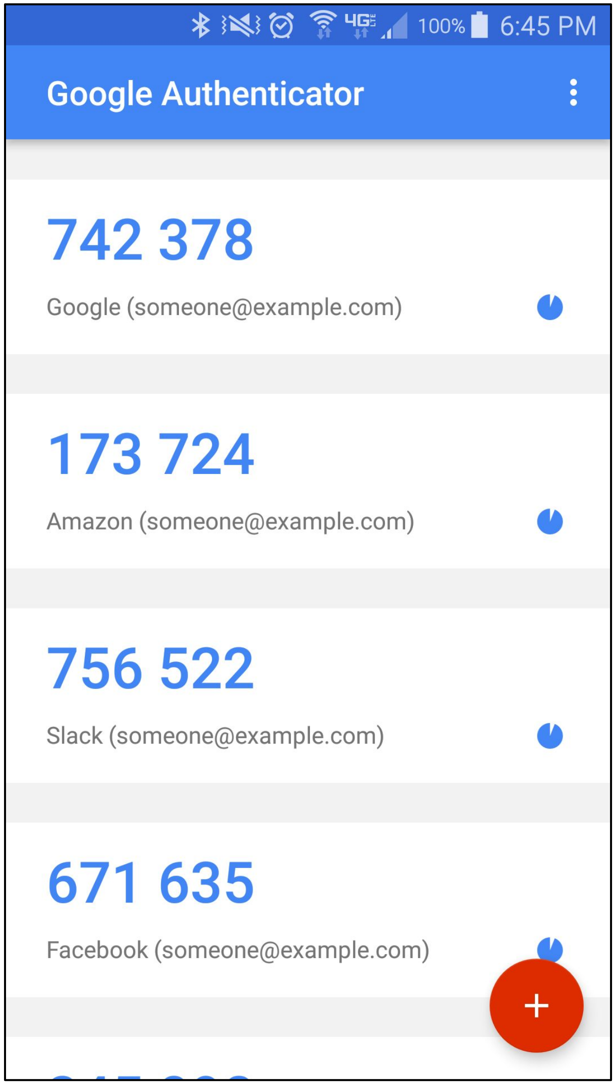
RFC6238 - https://tools.ietf.org/html/rfc6238

Google Authenticator

Google LLC

❌ No backup capability

by design!



100% 6:45 PM

Google Authenticator

742 378

Google (someone@example.com)

173 724

Amazon (someone@example.com)

756 522

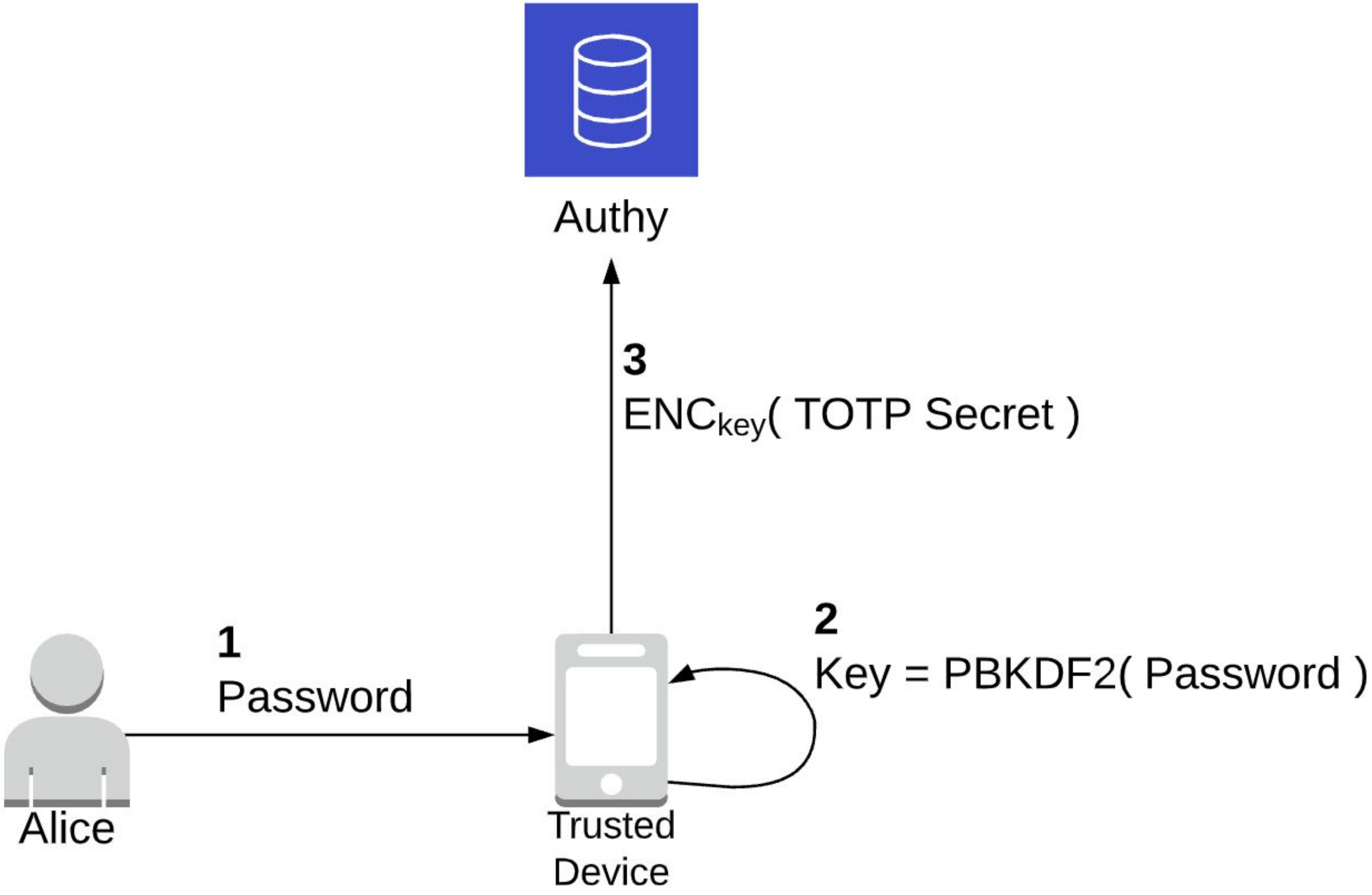
Slack (someone@example.com)

671 635

Facebook (someone@example.com)

Authy 2-Factor Authentication

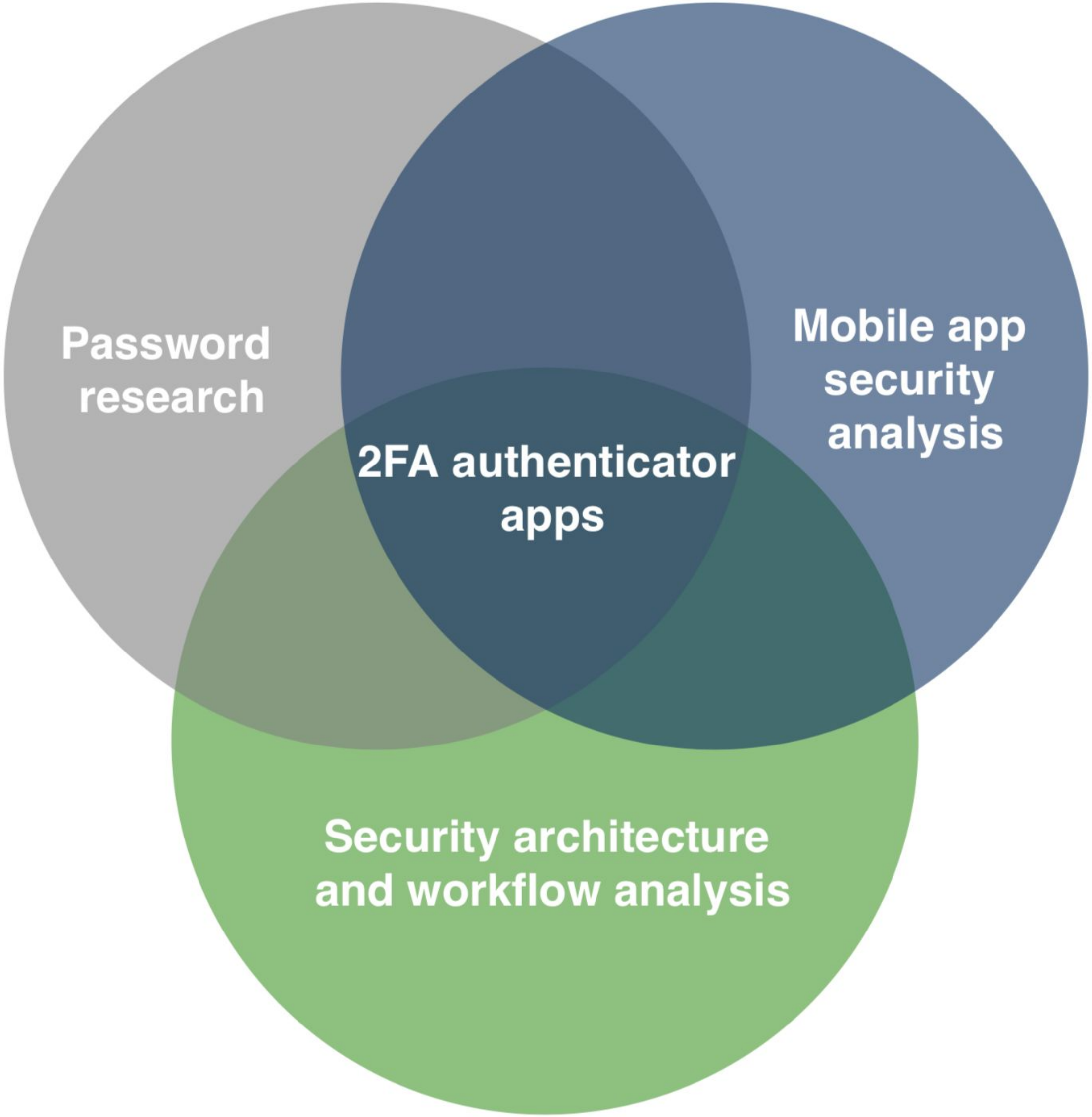
Authy



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

Related Work

Related Work



Password research

Mobile app security analysis

2FA authenticator apps

Security architecture and workflow analysis

Quantifying password guessability

- Password research shows
  - people pick **mostly weak** passwords
  - passwords are 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)

- Analyzed several "**host-proof**" systems
  - ideal: all data is encrypted on the clients
  - reality: flaws in client side crypto

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

Password Managers

Bhargavan and Delignat-Lavaud (2012)

- Analyzed several "**host-proof**" systems
  - ideal: all data is encrypted on the clients
  - reality: flaws in client side crypto
- Relationship to our work
  - considered offline brute force attacks out of scope
  - which data is encrypted?
  - how to circumvent client-side crypto?

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

Password Managers

Lie et al. (2014)

- Systematic security analysis
  - 5 web-based password managers

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

Password Managers

Lie et al. (2014)

- Security goals
  - Master account security
  - Credential db security
    - sharing features
  - Unlinkability

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

Password Managers

Lie et al. (2014)

- Security goals
  - Master account security
  - Credential db security
    - sharing features
  - Unlinkability

- Attack surface
  - Bookmarklet
  - Web
  - Authorization
  - User Interface

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

Password Managers

Lie et al. (2014)

- Relationship to our work
  - identified attacks to obtain password ciphertexts
    - CSRF

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

Password Managers

Lie et al. (2014)

- Relationship to our work
  - identified attacks to obtain password ciphertexts
    - CSRF
- “Systematic”

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

Password Managers

Lie et al. (2014)

- Relationship to our work
  - identified attacks to obtain password ciphertexts
    - CSRF
- “Systematic”
- Our goals
  - systematic analysis of TOTP 2FA apps
  - more technical detail to allow replication

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

Password Managers

Belenko and Sklyarov (2012)

- Analyzed 16 password managers
  - iOS & Blackberry
- **Goal**: brute force master passwords
  - attacker has password database

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

Password Managers

Belenko and Sklyarov (2012)

- **Findings**: takes only one day to brute force master passwords up to 10-15 characters

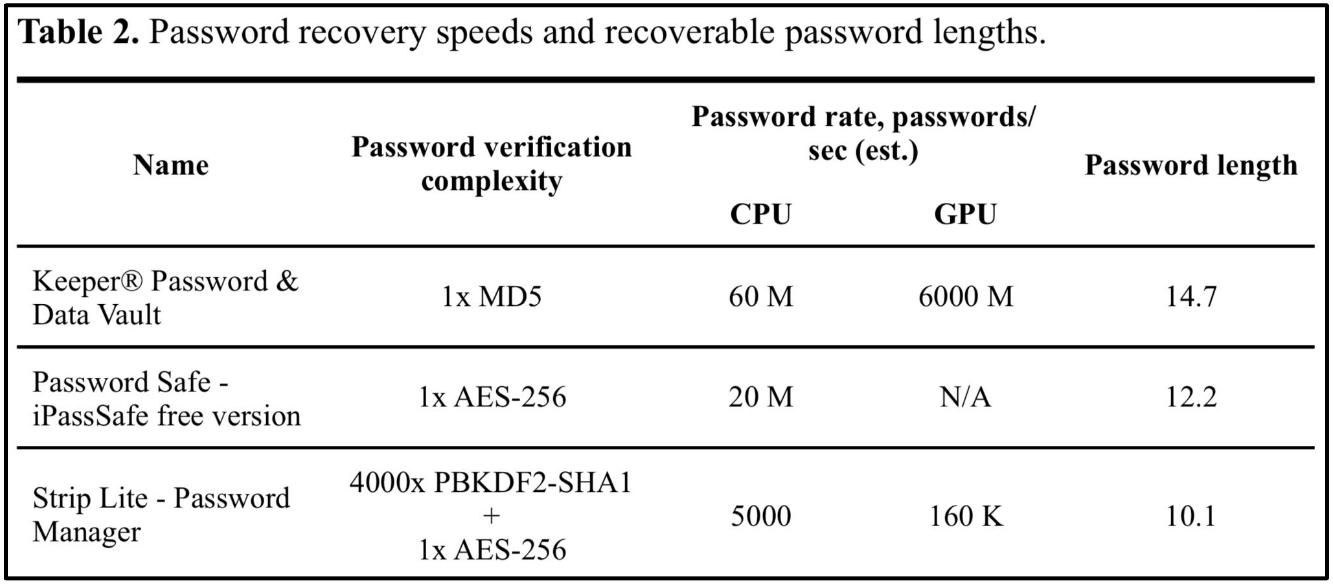


Table 2. Password recovery speeds and recoverable password lengths.

Name	Password verification complexity	Password rate, passwords/ sec (est.)		Password length
		CPU	GPU	
Keeper® Password & Data Vault	1x MD5	60 M	6000 M	14.7
Password Safe - iPassSafe free version	1x AES-256	20 M	N/A	12.2
Strip Lite - Password Manager	4000x PBKDF2-SHA1 + 1x AES-256	5000	160 K	10.1

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

Password Managers

Belenko and Sklyarov (2012)

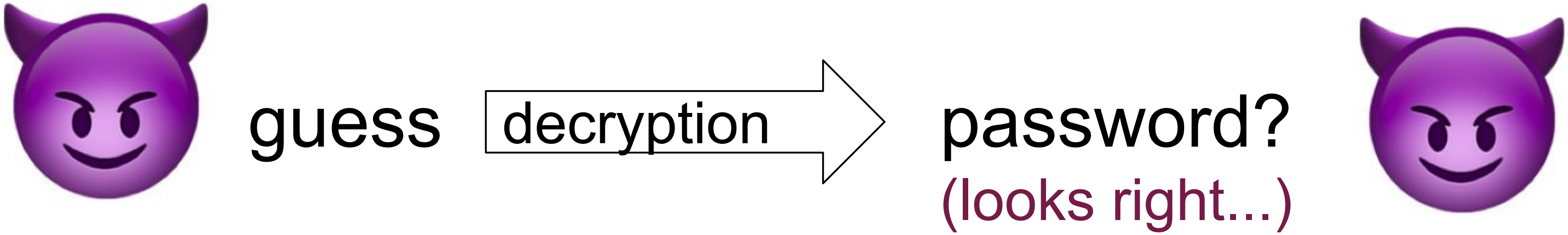
- Relationship to our work
  - offline brute force attacks
  - attacker has ciphertext

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

Offline Attacks on Passwords

Chatterjee et al. (2015)

- Proposed a novel defense scheme of "Plausible looking decoys"



guess

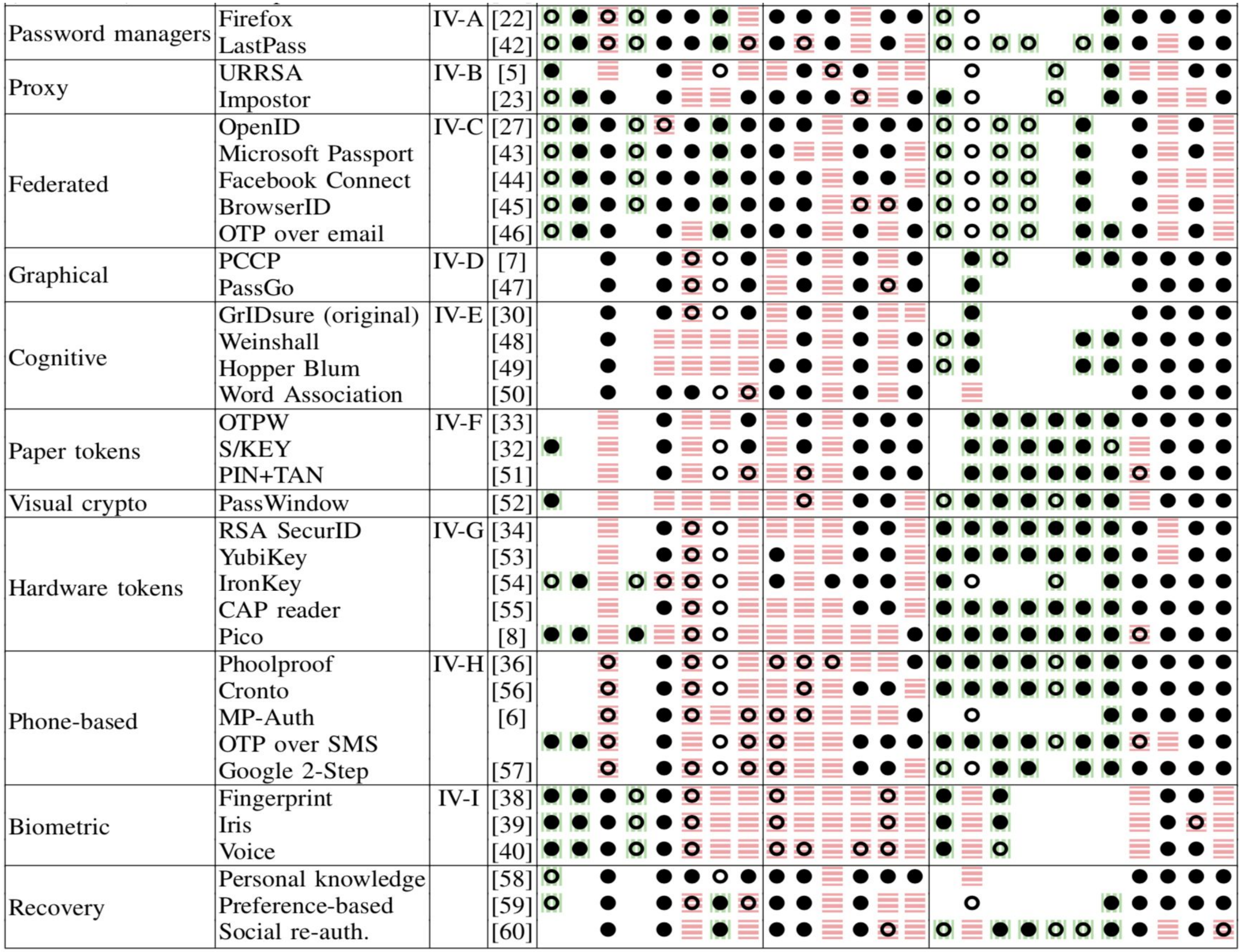
decryption

password?

(looks right...)

Chatterjee, Rahul, et al. "Cracking-resistant password vaults using natural language encoders." *2015 IEEE Symposium on Security and Privacy*.

Bonneau’s Authentication Framework



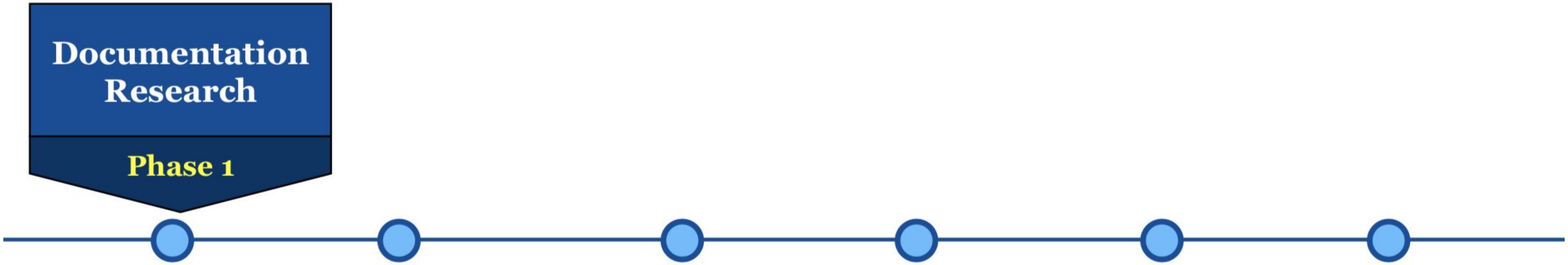
Password managers	Firefox	IV-A	[22]	🟩○	🟩●	🟥○	🟩○	●	●	🟩●	🟥	●	●	●	🟥	●	●	🟩○	○					🟩●	●	●	●	●
	LastPass		[42]	🟩○	🟩●	🟥○	🟩○	●	●	🟩●	🟥○	●	🟥○	●	🟥	●	🟥	🟩○	○	🟩○	🟩○		🟩○	🟩●	●	🟥	●	●
Proxy	URRSA	IV-B	[5]	🟩●		🟥		●	🟥	○	🟥	🟥	●	🟥○	●	🟥	🟥		○			🟩○		🟩●	🟥	🟥	●	●
	Impostor		[23]	🟩○	🟩●	●		●	🟥	🟥	●	●	●	●	🟥○	🟥	●	🟩●	○			🟩○		🟩●	●	🟥	🟥	●
Federated	OpenID	IV-C	[27]	🟩○	🟩●	●	🟩○	🟥○	●	🟩●	●	●	●	🟥	●	●	●	🟩○	○	🟩○	🟩○		🟩●		●	🟥	●	🟥
	Microsoft Passport		[43]	🟩○	🟩●	●	🟩○	●	●	🟩●	●	●	🟥	🟥	●	●	🟥	🟩○	○	🟩○	🟩○		🟩●		●	🟥	●	🟥
	Facebook Connect		[44]	🟩○	🟩●	●	🟩○	●	●	🟩●	●	●	●	🟥	●	●	🟥	🟩○	○	🟩○	🟩○		🟩●		●	🟥	🟥	🟥
	BrowserID		[45]	🟩○	🟩●	●	🟩○	●	●	🟩●	●	●	●	🟥	🟥○	🟥○	●	🟩○	○	🟩○	🟩○		🟩●		●	🟥	●	🟥
	OTP over email		[46]	🟩○	🟩●	●		●	🟥	🟩●	●	●	●	🟥	●	🟥	●	🟩○	○	🟩○	🟩○		🟩●	🟩●	●	🟥	●	🟥
Graphical	PCCP	IV-D	[7]			●		●	🟥○	○	●	🟥	●	🟥	●	🟥	●		🟩●	🟩○			🟩●	🟩●	●	●	●	●
	PassGo		[47]			●		●	🟥○	○	●	🟥	●	🟥	●	🟥○	●		🟩●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	🟥○	○	●	🟥	●	🟥	●	🟥	🟥		🟩●						●	●	●	●
	Weinshall		[48]			●		🟥	🟥	🟥	🟥	🟥	●	🟥	●	🟥	●	🟩○	🟩●				🟩●	🟩●	●	●	●	●
	Hopper Blum		[49]			●		🟥	🟥	🟥	🟥	●	●	🟥	●	🟥	●	🟩○	🟩●				🟩●	🟩●	●	●	●	●
	Word Association		[50]			●		●	●	○	🟥○	●	●	🟥	●	🟥	●		🟥						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			🟥		●	🟥	🟥	●	🟥	●	🟥	●	●	●		🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	●	●	●
	S/KEY		[32]	🟩●		🟥		●	🟥	○	●	🟥	●	🟥	●	●	●		🟩●	🟩●	🟩●	🟩●	🟩●	🟩○	🟥	●	●	●
	PIN+TAN		[51]			🟥		●	🟥	○	🟥○	🟥	🟥○	🟥	●	●	●		🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟥○	●	●	●
Visual crypto	PassWindow		[52]	🟩●		🟥		🟥	🟥	🟥	🟥	🟥	🟥○	🟥	●	●	🟥	🟩○	🟩●	🟩●	🟩●	🟩○	🟩●	🟩●	🟥	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			🟥		●	🟥○	○	🟥	🟥	🟥	🟥	●	●	🟥	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	🟥	●	●
	YubiKey		[53]			🟥		●	🟥○	○	🟥	●	🟥	🟥	●	●	🟥	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	🟥	●	●
	IronKey		[54]	🟩○	🟩●	🟥	🟩○	🟥○	🟥○	○	🟥	●	🟥	●	●	●	🟥	🟩●	○			🟩○		🟩●	●	●	●	●
	CAP reader		[55]			🟥		●	🟥○	○	🟥	🟥	🟥	🟥	●	●	🟥	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	●	●	●	●
	Pico		[8]	🟩●	🟩●	🟥	🟩●	🟥	🟥○	○	🟥	🟥	🟥	🟥	🟥	🟥	●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟩●	🟥○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			🟥○		●	🟥○	○	🟥	🟥○	🟥○	🟥○	🟥	🟥	●	🟩●	🟩●	🟩●	🟩●	🟩○	🟩●	🟩●	●	●	●	●
	Cronto		[56]			🟥○		●	🟥○	○	🟥	🟥	🟥○	🟥	●	●	🟥	🟩●	🟩●	🟩●	🟩●	🟩○	🟩●	🟩●	●	●	●	●
	MP-Auth		[6]			🟥○		●	🟥○	🟥	🟥○	🟥○	🟥○	🟥	🟥	🟥	●		○					🟩●	●	●	●	●
	OTP over SMS			🟩●	🟩●	🟥○		●	🟥	○	🟥○	🟥○	🟥	🟥	●	●	●	🟩●	🟩●	🟩●	🟩●	🟩○	🟩●	🟩●	🟥○	🟥	●	●
	Google 2-Step		[57]			🟥○		●	🟥○	○	🟥○	🟥○	🟥	🟥	●	●	🟥	🟩○	○	🟩●	🟩●		🟩●	🟩●	●	●	●	●
Biometric	Fingerprint	IV-I	[38]	🟩●	🟩●	●	🟩○	●	🟥○	🟥	🟥	🟥○	🟥	🟥	🟥	🟥○	🟥	🟩●	🟥	🟩●					🟥	●	●	🟥
	Iris		[39]	🟩●	🟩●	●	🟩○	●	🟥○	🟥	🟥	🟥○	🟥	🟥	🟥	🟥○	🟥	🟩●	🟥	🟩●					🟥	●	🟥○	🟥
	Voice		[40]	🟩●	🟩●	●	🟩○	●	🟥○	🟥	🟥	🟥○	🟥○	🟥	🟥○	🟥○	🟥	🟩●	🟥	🟩○					🟥	●	●	🟥
Recovery	Personal knowledge		[58]	🟩○		●		●	●	○	●	●	●	🟥	●	●	●		🟥						●	●	●	●
	Preference-based		[59]	🟩○		●		●	🟥○	🟩●	🟥○	●	●	🟥	●	🟥	🟥		○					🟩●	●	●	●	●
	Social re-auth.		[60]			●		●	🟥	🟩●	🟥	●	●	🟥	●	🟥○	🟥	🟩○	🟥	🟩●	🟩●	🟩○	🟩○	🟩●	●	🟥	●	🟥○

Bonneau, Joseph, et al. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." *2012 IEEE Symposium on Security and Privacy*.

Analysis Workflow

Case-Study: Authy 2FA

Documentation Research



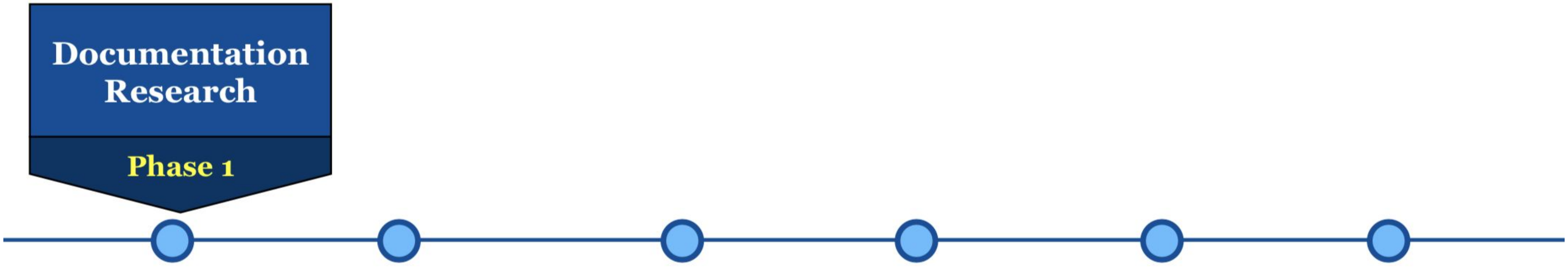
Documentation Research

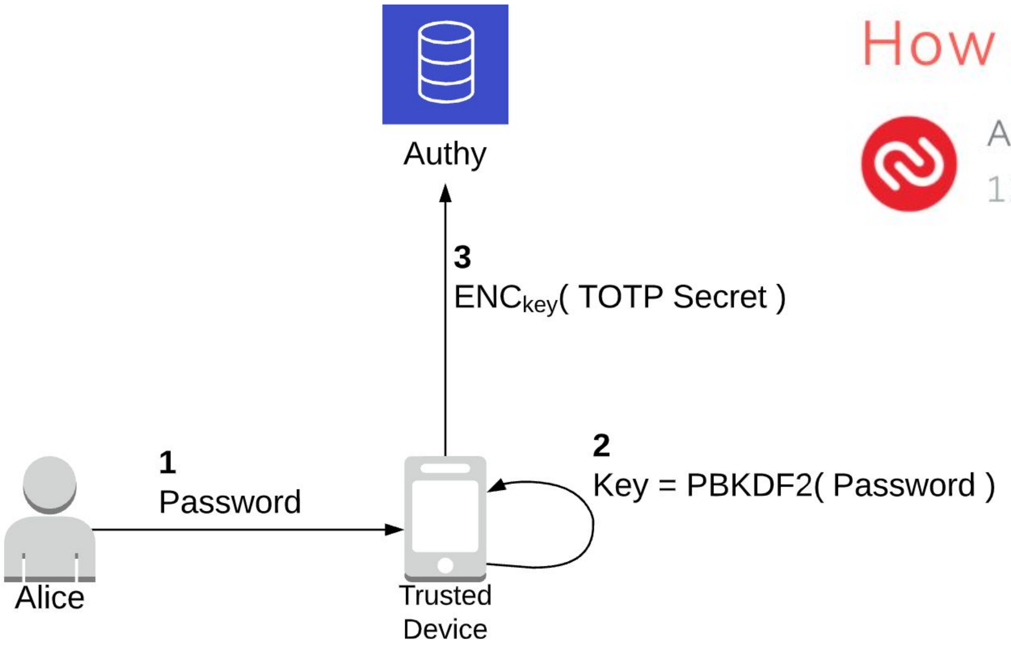
Phase 1

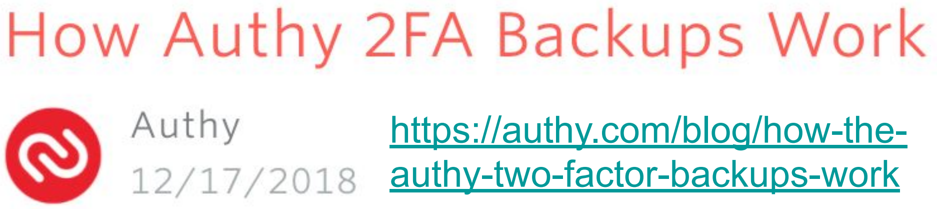
Goals

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

Documentation Research







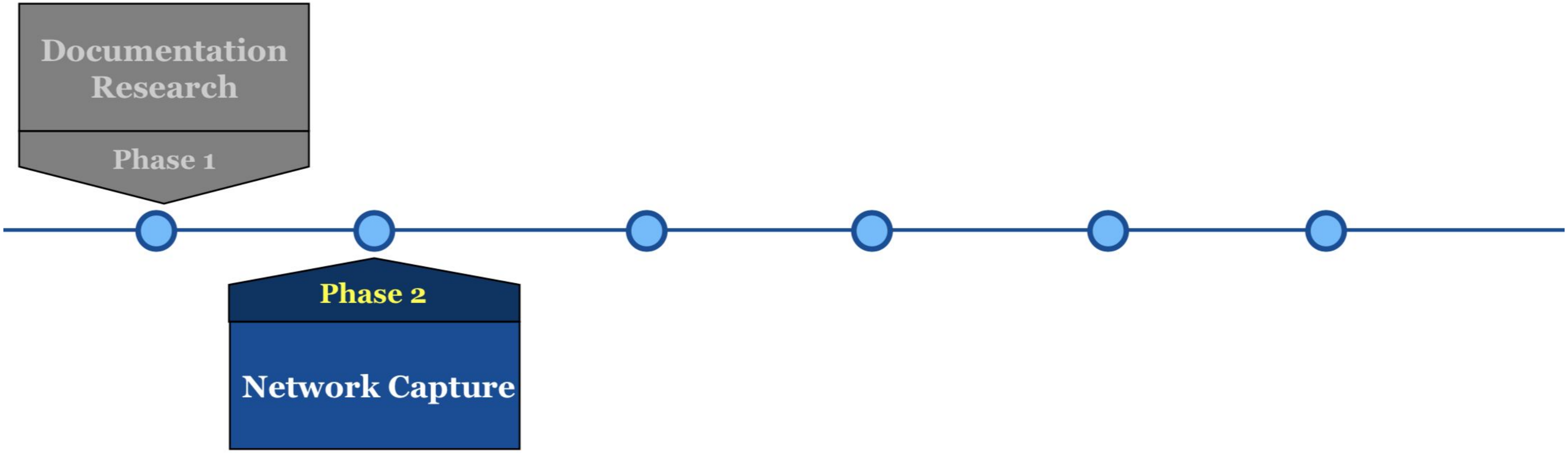
How Authy 2FA Backups Work

Authy

12/17/2018

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

Network Capture



Documentation Research

Phase 1

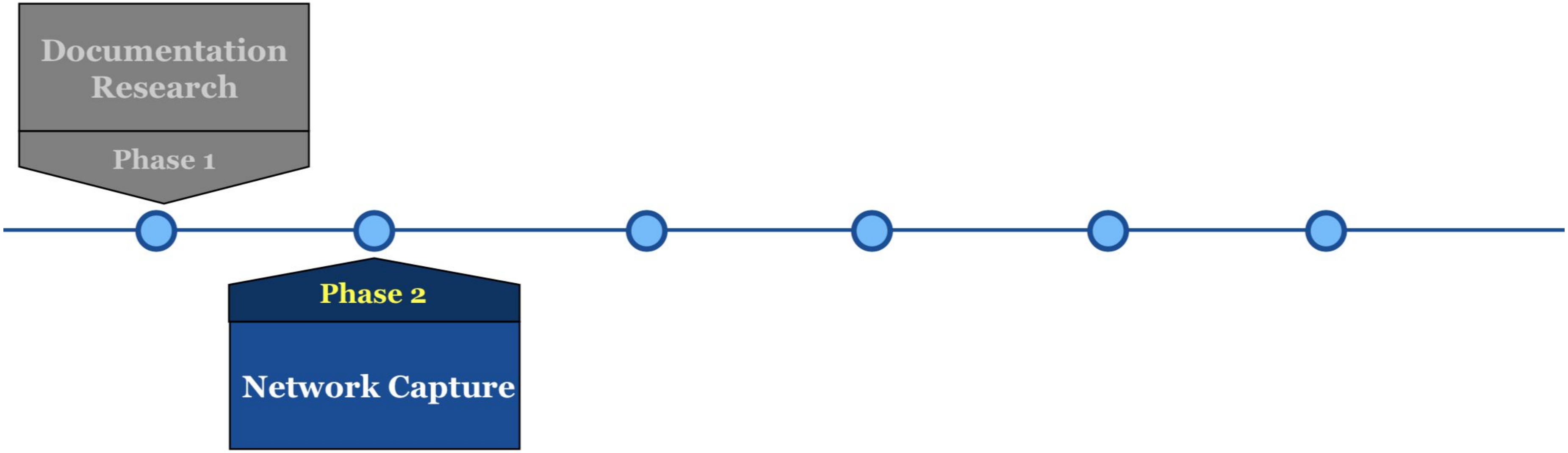
Phase 2

Network Capture

Goals

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

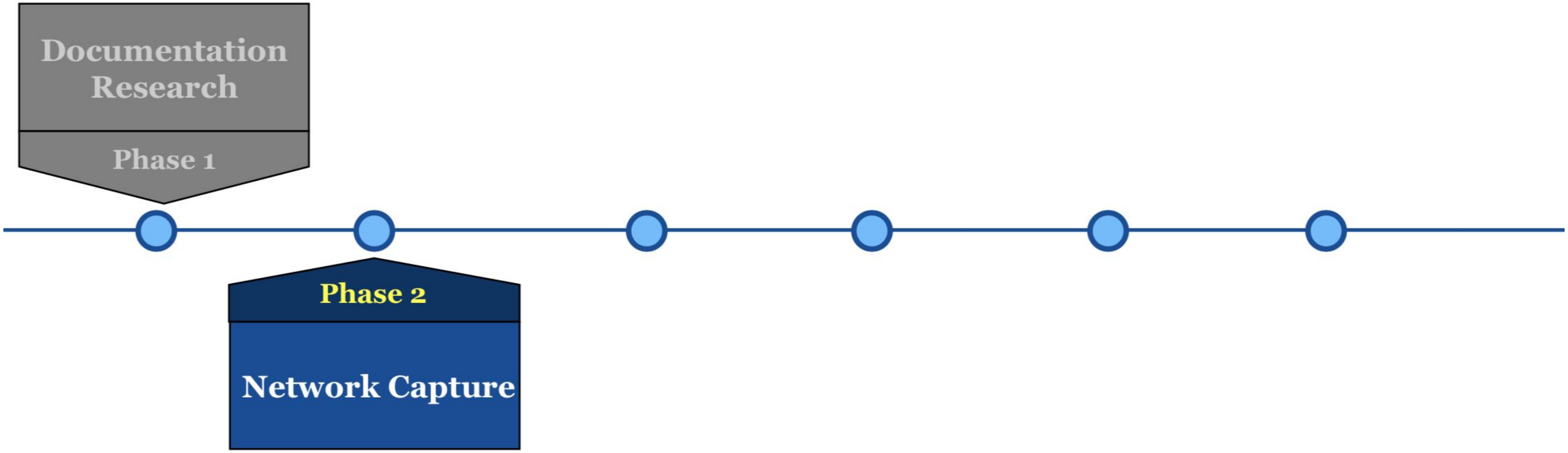
Network Capture



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

In Progress

Network Capture



Documentation Research

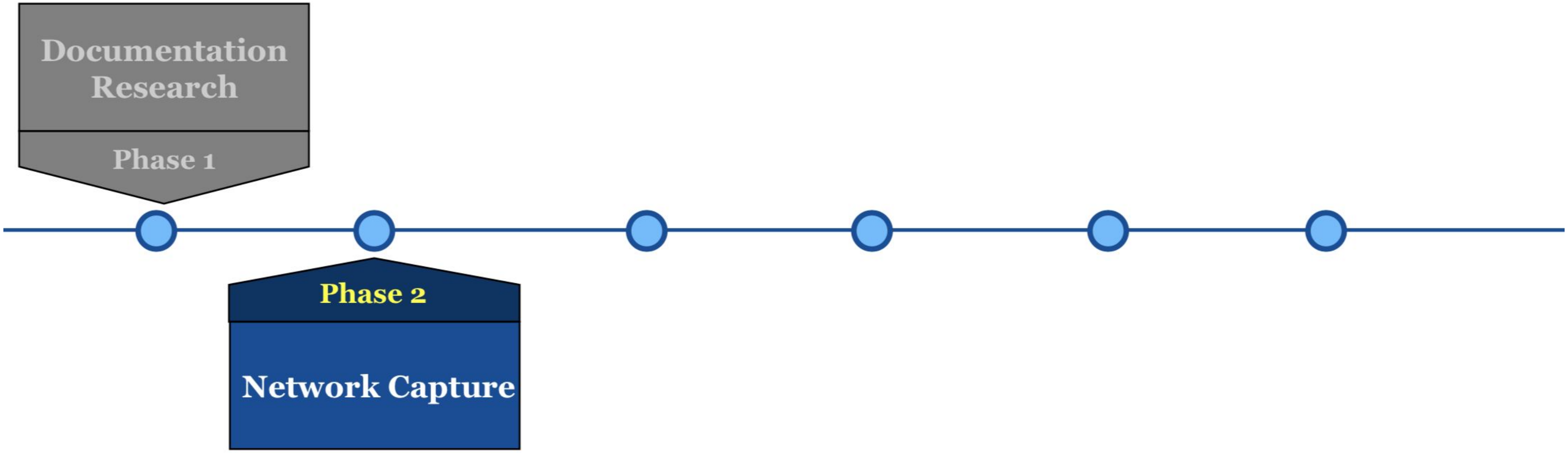
Phase 1

Phase 2

Network Capture

- Authy requires phone & email
  - Even if backup is not enabled

Network Capture



Documentation Research

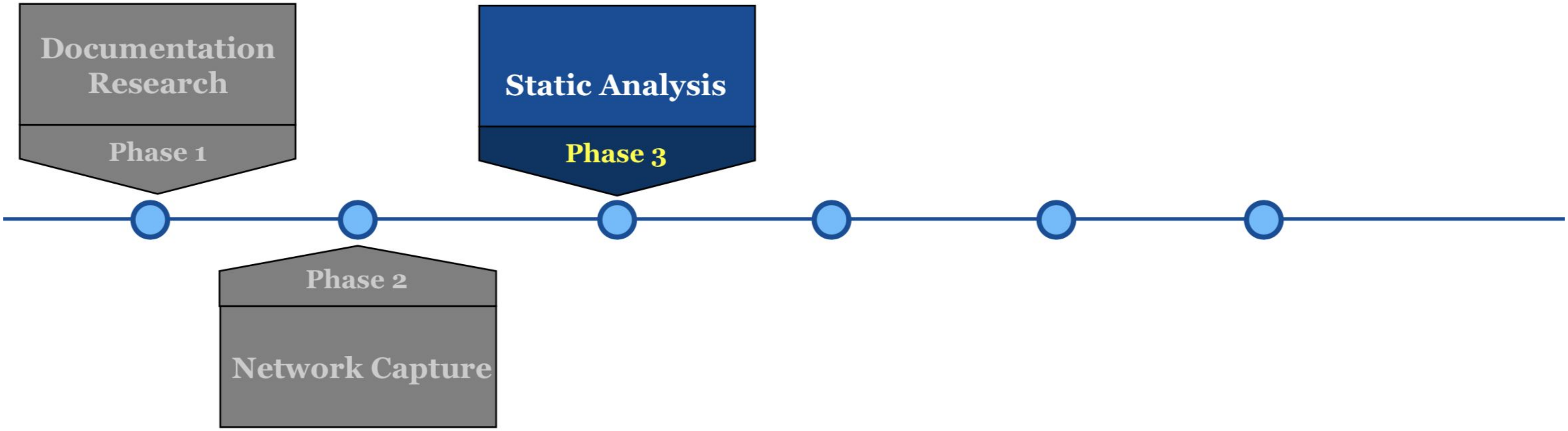
Phase 1

Phase 2

Network Capture

- mitmproxy + cert pinning = 😥
- Used lab-built Android image
  - Lesson learned: communicate early and clearly!

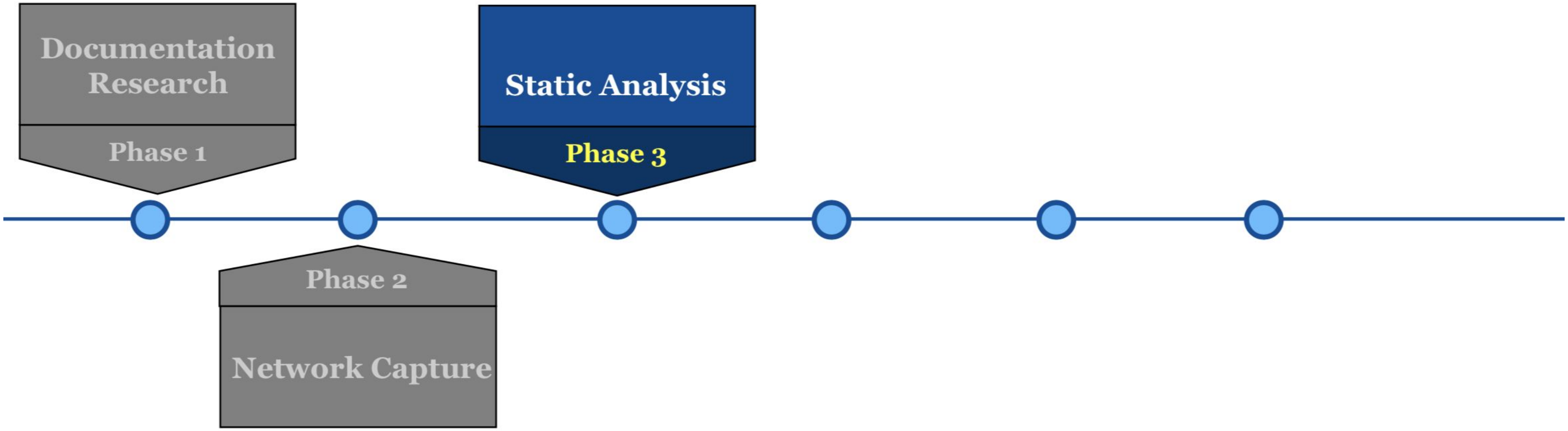
Static Analysis



Goals

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

Static Analysis



Documentation Research

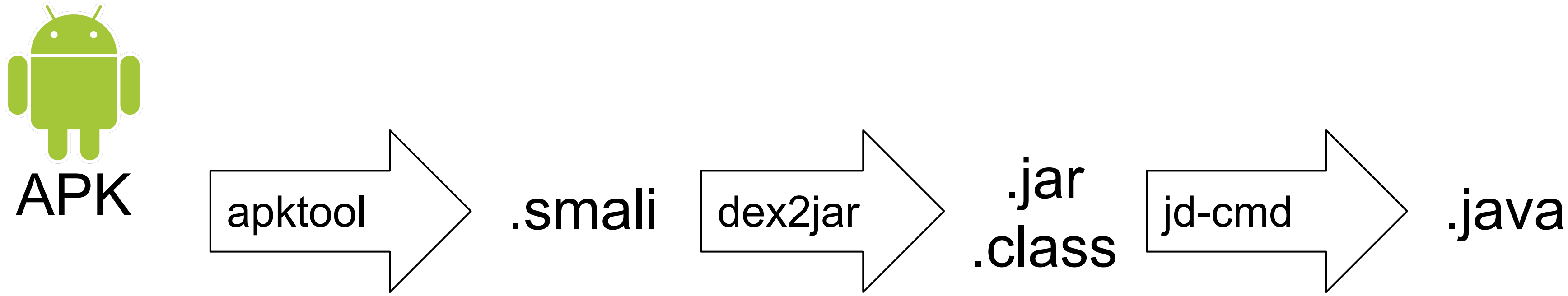
Phase 1

Static Analysis

Phase 3

Phase 2

Network Capture



APK

apktool

.smali

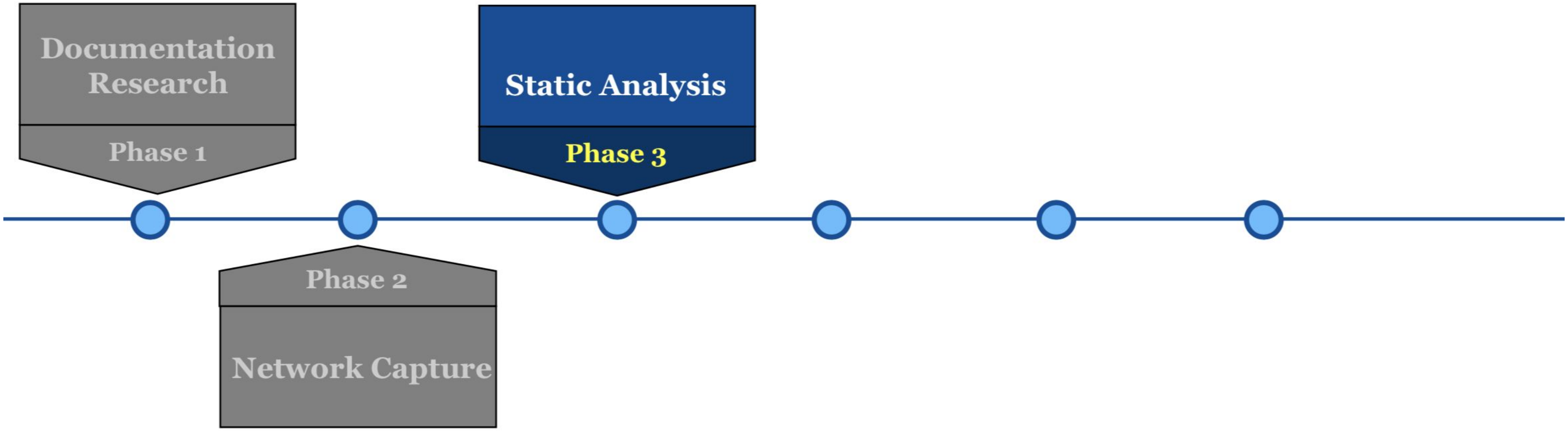
dex2jar

.jar
.class

jd-cmd

.java

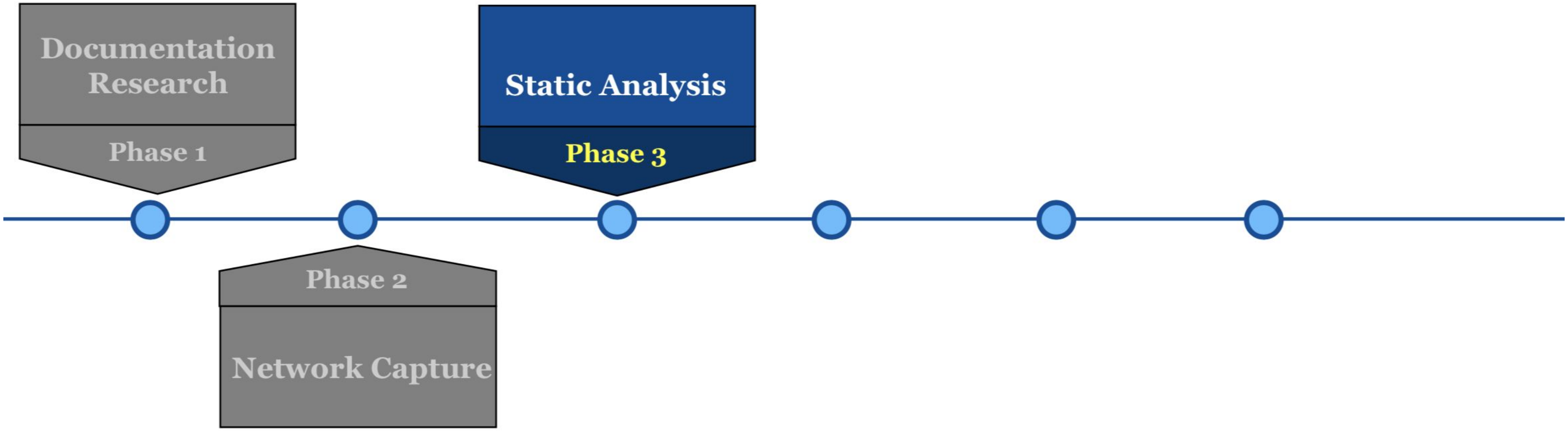
Challenge: Obfuscation



Duo Mobile

Duo Security, Inc.

Challenge: Obfuscation



Documentation Research

Phase 1

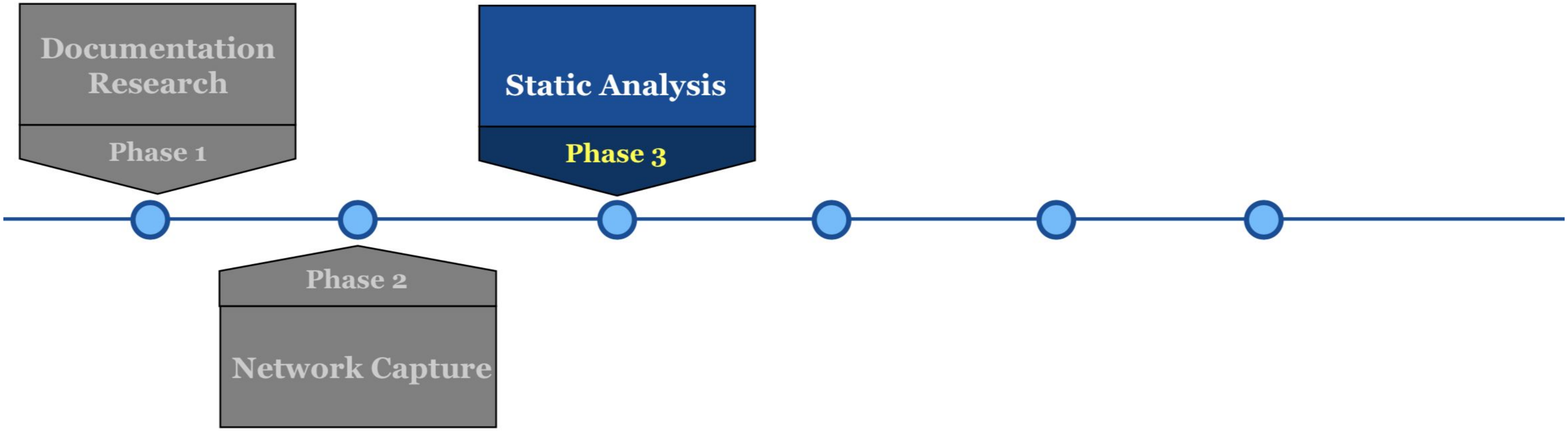
Phase 2

Network Capture

Static Analysis

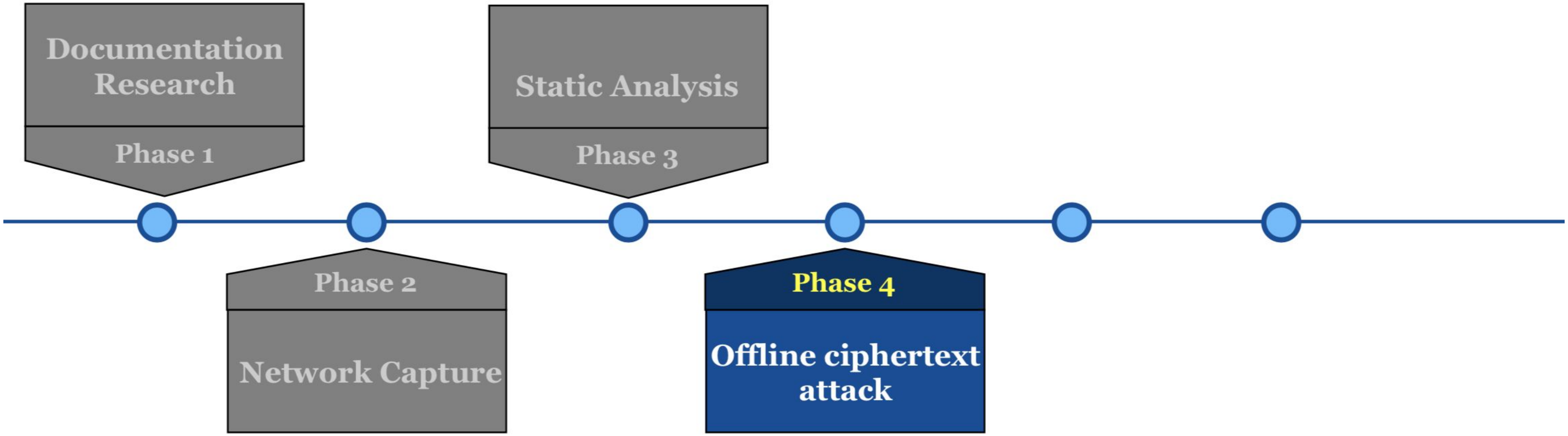
Phase 3

Static Analysis



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

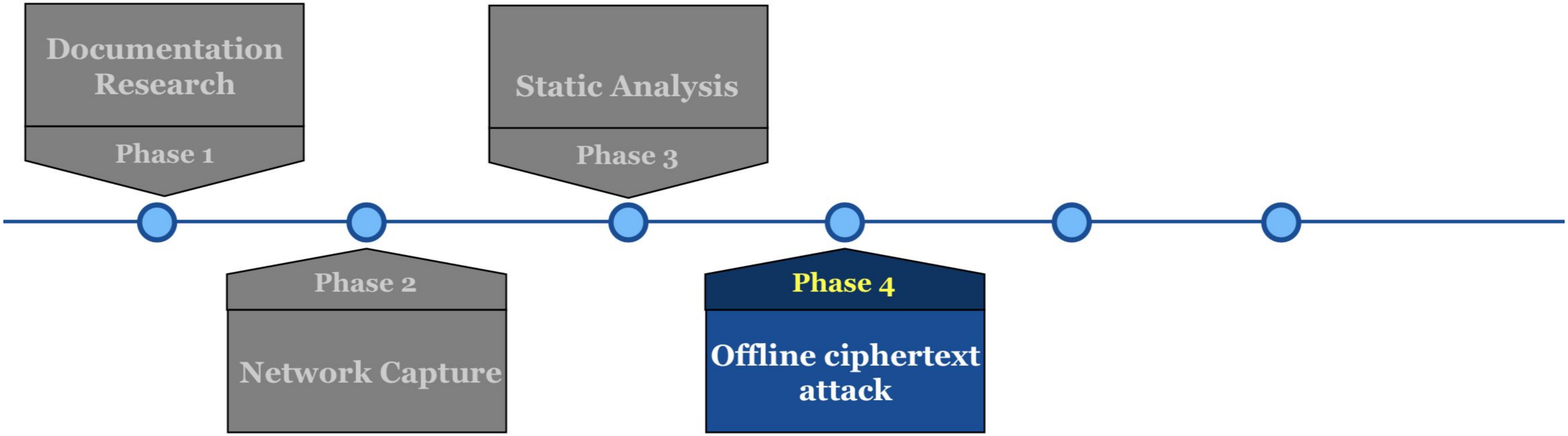
Attack Ciphertext Offline



Goals

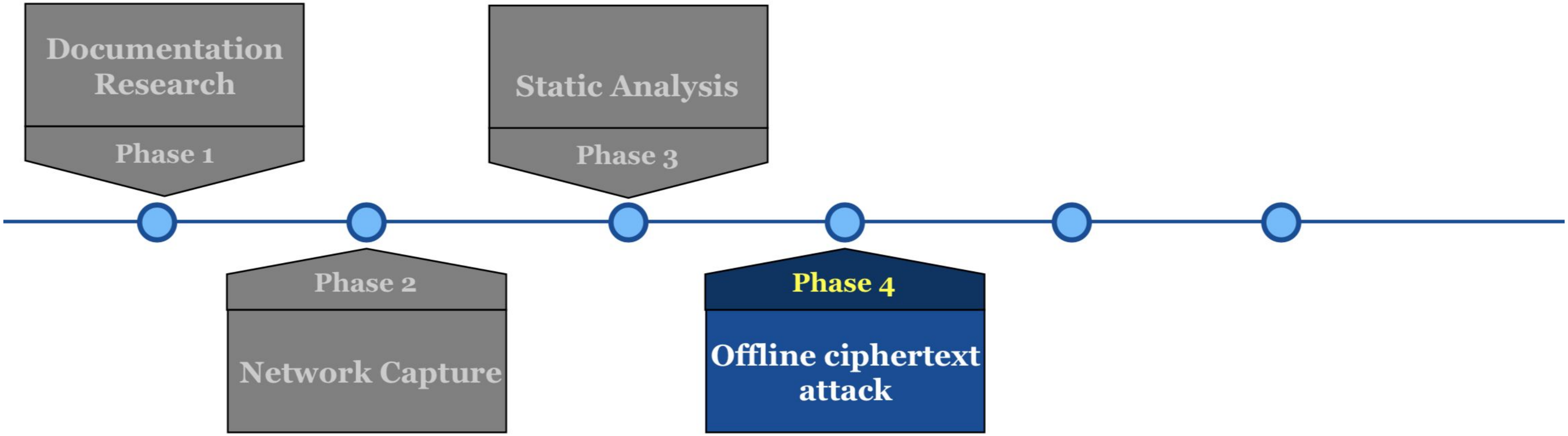
1. Difficulty of ciphertext => plaintext?

Attack Ciphertext Offline



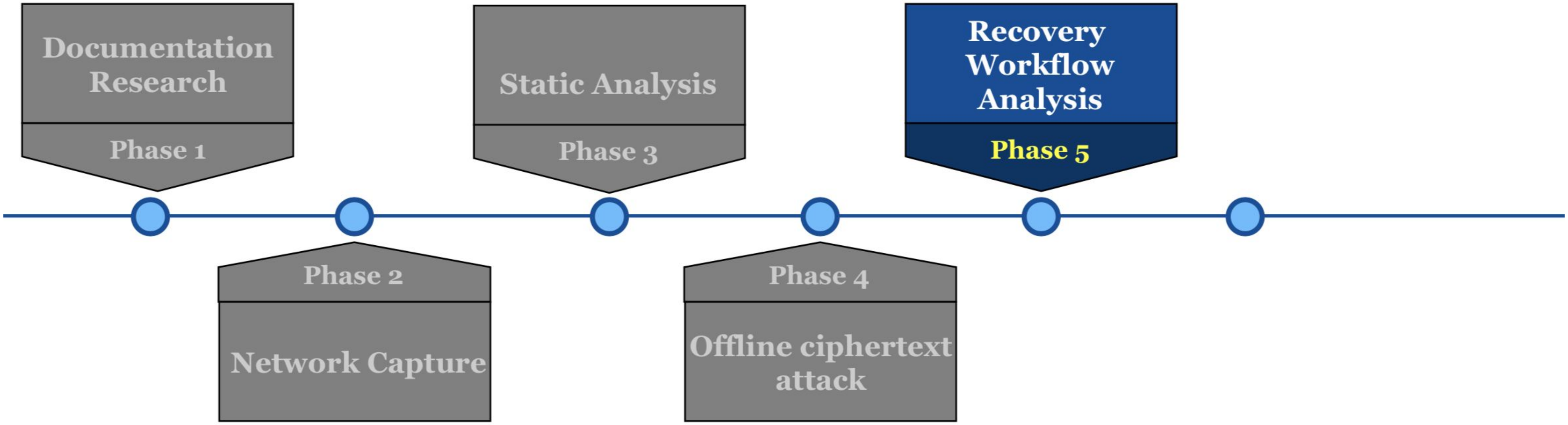
- Adapt password cracking tools to “crack” ciphertexts
  - e.g. Hashcat module framework

Attack Ciphertext Offline



- How many possible TOTP secrets?
  - base32 format will match many key guesses
  - attacker forced into an online attack

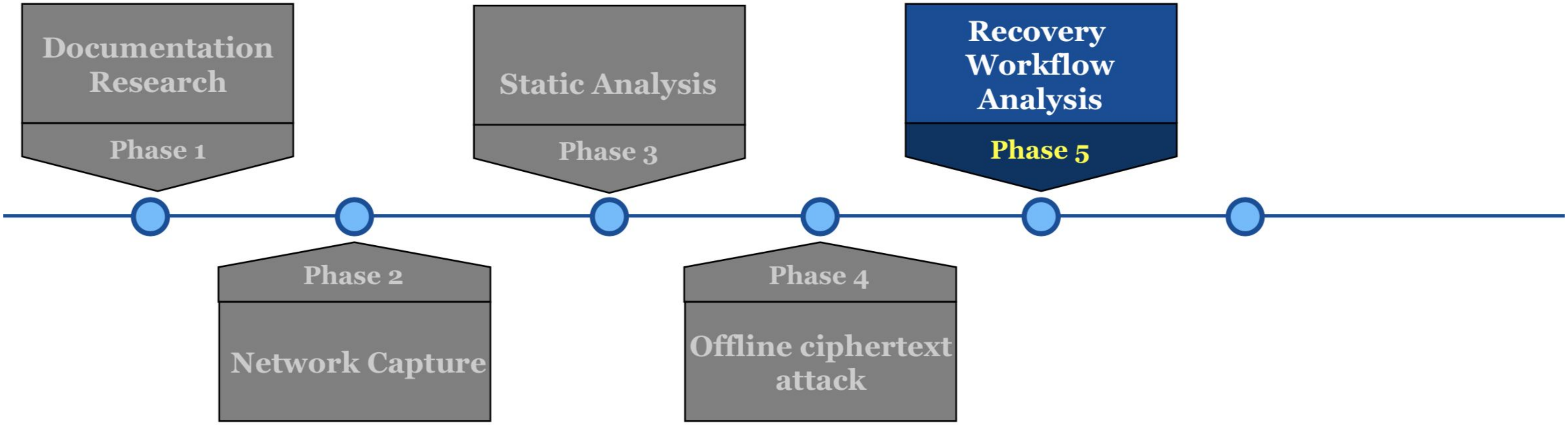
Recovery Workflow Analysis



Goals

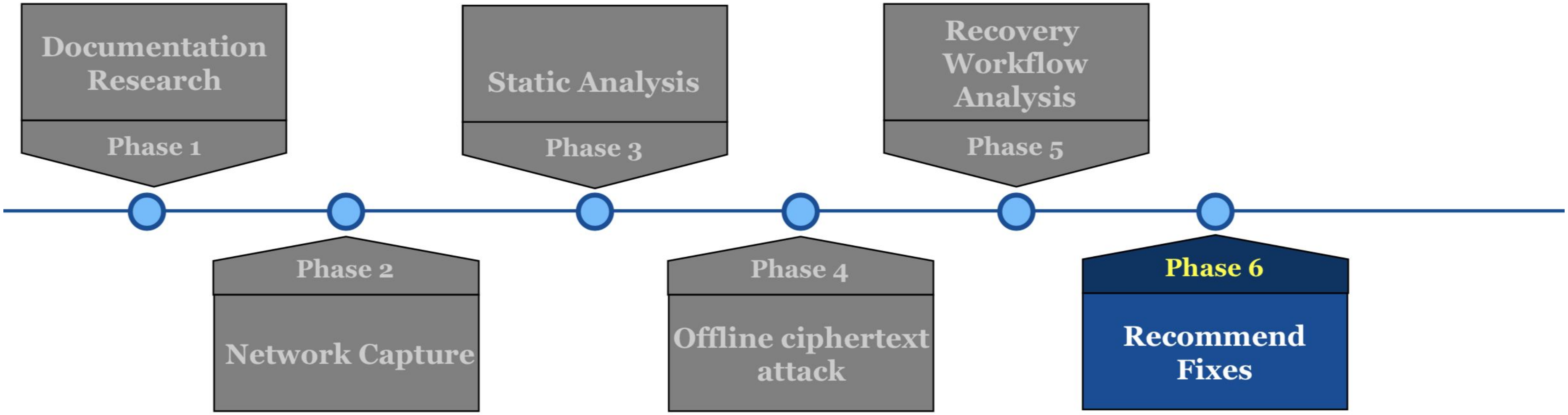
1. Diagram the recovery workflow
   a. How could an attacker access the ciphertext?
   b. Opportunities for user to identify/stop the attack?

Recovery Workflow Analysis

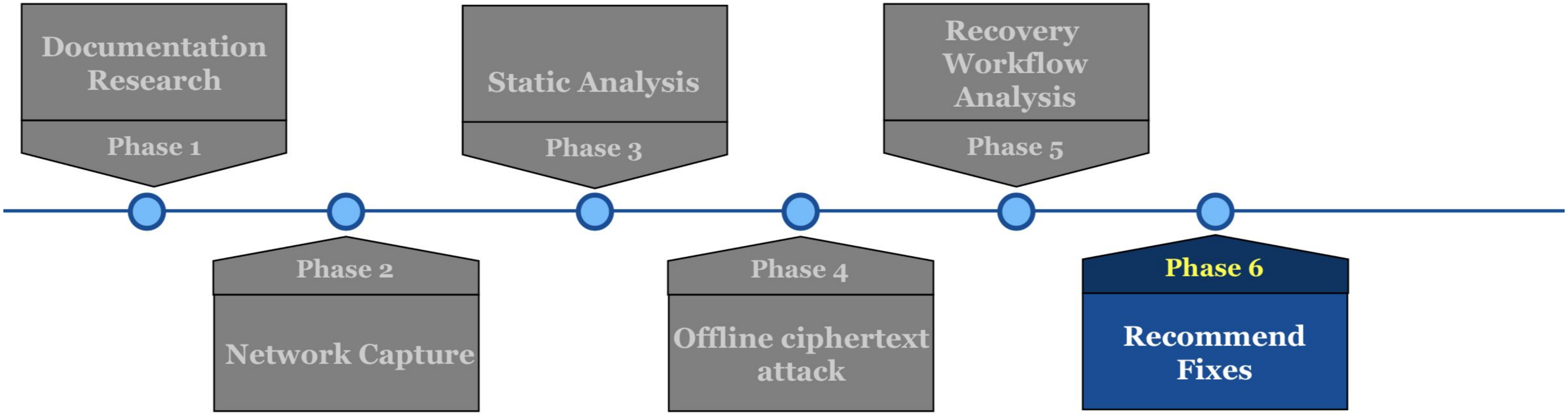


- Authy claims a 24 hour delay
  - User sent SMS and email
  - Recovery available after only ~10 hours

Recommend Fixes



Recommend Fixes



- Encrypt name and issuer fields
- Strengthen key derivation

Thank you!

Please, ask us questions!