

TWOFAY

Multifactor Authentication System

THE AEROSPACE CORPORATION

Fay Wu, Chris Orcutt, Jonathan Woong, Anthony Nguyen, Rossen Chemelekov, Vu Le

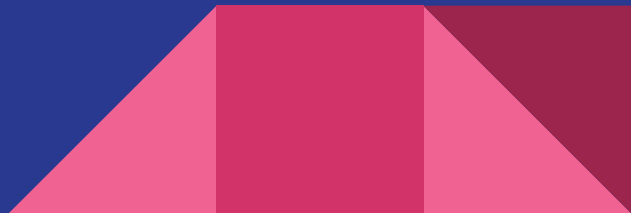
Intro & Problem Statement

- ▶ Current log-in systems: 1-factor authentication (password)
- ▶ Easy to get hacked
- ▶ Adding additional factors raises security
- ▶ Problem Statement: Create a multi-factor authentication system that easily integrates into existing website log-in systems



Motivation

- ▶ Easier to use --> More likely to use
- ▶ Simplifies and greatly improves website security
- ▶ Integrate Twoefay into log-in system
- ▶ Install app on iPhone
- ▶ 3-factor: password, phone, fingerprint





DEMO

File Edit View Search Terminal Help

Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |=====| 100.00 %

2 hosts added to the hosts list...

mining
ARP poisoning victims:

DCAST GROUP: 10: 192.168.2.1 EC: 1A:59:36:E1:F6

.131 netmask 255.255.255.0 broadcast 192.168.233.255

29ff: GROUP: 25: 192.168.2.18 DC: 0E:A1:FD:78:E8 k>

1:42 Starting Unified sniffing...

bytes 2552590 (2.4 MiB)

opped 0 overruns 0 frame 0

by: Text only Interface activated...

opped Hit Ctrl+C for inline help collisions 0

, RUN: SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

netm: SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

xlen: SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

0 SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

byte: HTTP: 45.55.227.27:80 -> USER: fay PASS: haha INFO: http://faystore.twoefay.xyz/login/

opped CONTENT: csrfmiddlewaretoken=rMK7YSUDDGjlu2ygeufckg09INASGy2&username=fay&password=haha

bytes: 35640 (34.8 KiB)

opped SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

SNMP : 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

User requested a CTRL+C... (deprecated, next time use proper shutdown)

root@kali:~#

File Edit View Search Terminal Help

Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |=====>| 100.00 %

2 hosts added to the hosts list...

mining
ARP poisoning victims:

DCAST GROUP: 10: 192.168.2.1 EC: 1A:59:36:E1:F6

.131 netmask 255.255.255.0 broadcast 192.168.233.255

29ff: GROUP: 25: 192.168.2.18 DC: 0E:A1:FD:78:E8 k>

1:42 Starting Unified sniffing (vnet)

bytes 2552590 (2.4 MiB)

opped 0 overruns 0 frame 0

by: Text3 only Interface3 activated...

opped Hit: 0 (for inline help) collisions 0

, RUN: SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

netm: SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

xlen: SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

0 SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

byte: HTTP: 45.55.227.27:80 -> USER: fay PASS: haha INFO: http://faystore.twoefay.xyz/login/

opped CONTENT: csrfmiddlewaretoken '192.168.1.5:161' tuzyeufckg09INASGy2&username=fay&password=haha

bytes: 35640 (34.8 KiB)

opped SNMP: 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

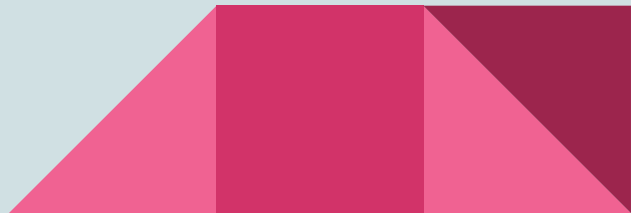
SNMP : 192.168.1.5:161 -> COMMUNITY: public INFO: SNMP v1

User requested a CTRL+C... (deprecated, next time use proper shutdown)

root@kali:~#

Infrastructure

- Digital Ocean (3 droplets)
- twoefay.xyz
- systemd daemons
- Let's Encrypt!





https://45.55.160.135:8080



https://45.55.160.135:8080/register



Animeee

UCLA

7M 7Min

@live

@ucla

/a/Archive

/a/Catalog

CS 130

GDrive

29 Report Summary

Deli

Anison World Matsuri

Other bookmarks



Elements

Console

Sources

Network

Timeline

Profiles

Resources

Security

Audits



Overview

Main Origin

Reload to view details

Security Overview



This page is insecure (broken HTTPS).



Certificate Error

There are issues with the site's certificate chain (net::ERR_CERT_AUTHORITY_INVALID).

[View certificate](#)



Secure TLS connection

The connection to this site is using a strong protocol version and cipher suite.



Secure Resources

All resources on this page are served securely.

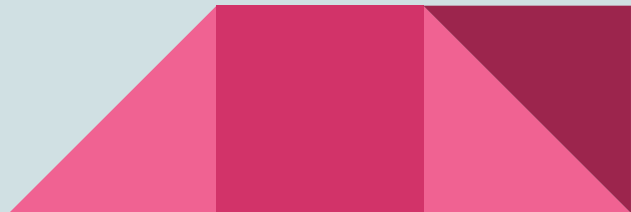
Client Website

- ▶ **Purpose:** Demo
- ▶ **Tech:** Python + Django web framework
- ▶ **Issues:**
 - ▶ Client website existing user authentication library inflexibility
 - ▶ Lack of async requests



Twoefay Server

- **Purpose:** Main mediator
- **Tech:** Python + Hyper, Twisted framework
- **Issues:**
 - HTTP/2.0 (required for APN communication)
 - Certificate verification woes



APN Communication

- ▶ **Purpose:** Apple push notifications
- ▶ **Tech:** Python + Flask framework
- ▶ **Issues:**
 - ▶ Apple certificates and provisioning profiles
 - ▶ Integrating with nghttp2




iOS Client

▸ Purpose:

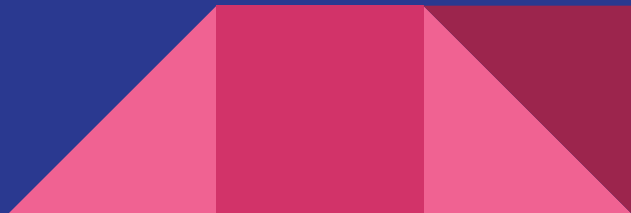
- Register with Client website
- Receive Push Notifications
- Send Authentication/Denial Message to Python ServerRealm (History)

▸ Libraries:

- Alamofire (HTTP Requests)
 - SwiftyJSON (APN Parsing)
 - Realm (History)
- 

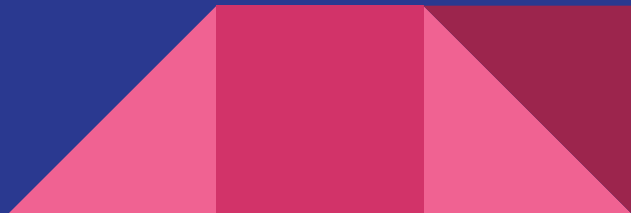
For the Future...

- ▶ Limitations:
 - ▶ iOS client only - Android / Windows for the future
 - ▶ Client-specific app - app should be able to integrate with 1+ log-in sites
 - ▶ Set up additional endpoint for back-up email option
- ▶ Protocol fall-back to HTTP/1.1
- ▶ Tighten security & improve performance / reliability



Known Vulnerabilities (1)

- ▶ Man in the Middle (MITM) Attacks
 - ▶ Attack: Captured username, password from using logging into Client
- ▶ Replay Attacks
 - ▶ Attack: Captured entire message, encrypted and all in transit
 - ▶ Countermeasure: Add nonce to encrypted message



Known Vulnerabilities (2)

- ▶ Attacker Steals id_token

- ▶ Attack: Attacker can then register their phone and replace your phone, so push notifications get pushed to them instead

- ▶ Countermeasure: Flag the account if the dev_token changes too often

- ▶ DDoS Attacks

- ▶ Attack: Client websites will be unable to communicate with our Server, iOS App will be unable to receive push notifications

- ▶ Countermeasure: Have extra servers



The background is a solid dark blue. In the top right corner, there is a decorative pattern of triangles in various shades of blue, including a lighter blue and a darker blue, creating a geometric, abstract design.

THANK YOU