Guests ‘N Goblins:

EXPOSING WI-FI EXFILTRATION RISKS AND MITIGATION TECHNIQUES

Presenter: Pete Desfigies

- By day : Security Analyst @ TELUS Communications
- By night: break things
- Hobbies: Break more things

TELUS the future is friendly®

Presenter: Joshua Brierton

- By Day: SIEM Geek
- By Night: Boat Geek
- Hobbies: Cards against humanity + watching Holy Mountain

TELUS the future is friendly®

Presenter: Naveed Islam

- By day: Intelligent Analysis team lead @ TELUS Communications
- By night: Family management, as a father of 2, +1 on the way anytime now
- Hobbies: Learning about religion, science and philosophy etc. Traveling and starting projects that just not complete.

Background

Anonymity is a big thing

Many ways to hide your identity

1. TOR
2. L2P
3. Spotflux
4. Hola

Proxyham?

Introduction

Wifi is everywhere

Is Wifi secure enough?

It has its own network isolation

WPA 2.0 with AES added

Sure it is secure, no one can get in from outside

And yet, it is open to public for “competitive” convenience

TELUS the future is friendly®

Problem Space

Public Wifi = Risks

- **“Wifi Exfiltration”**
- **Host Implication**

Security Challenges

Insufficient authentication, a catch 22 situation

Lack of Egress monitoring

Default SSL

Spoofed MAC addresses

Intro to Our Concept

- A custom mobile App + batch scripts + two servers with dedicated IPs.
- Scans for open Wifi
- Tags the location
- Connects automatically
- Learns about the network
- Collects public fingerprints
- Syncs with a central server

TELUS the future is friendly®

Programs + Tools Used

- Python
- Java
- Bash
- SQLITE
- JSON
- Apache
- github
- Crash course mentality
- Android SDK Toolkit

Hardware + Tools

- Laptop Kali Linux
- Android Phone
- CentOS Servers

Automated Tookit - Wargarble

- Warscanble – Initial Area Scan / Discovery
- Wargarble – Connectvity / Data collection
- Warrepo - Reporting / Results

What is WarScanble basically

- Nutshell definition:
  - Dead simple WiFi scanner to coordinate the gathering of access points for whatever purpose.

TELUS the future is friendly®

How do it do?

Step 1

- Scan for all access points

How do it do?

Step 2

- Put all results into a hashable object that stores
  - Static values
  - Location values paired with signal strength

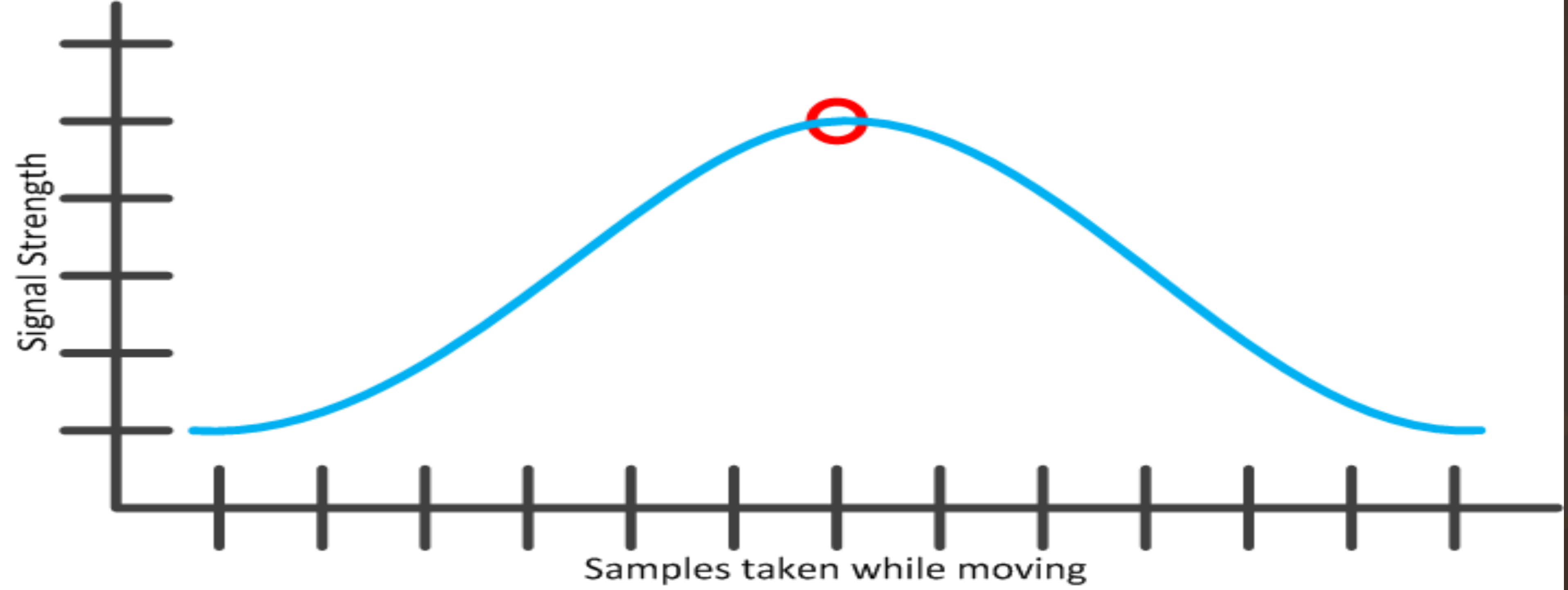
How do it do?

Step 3

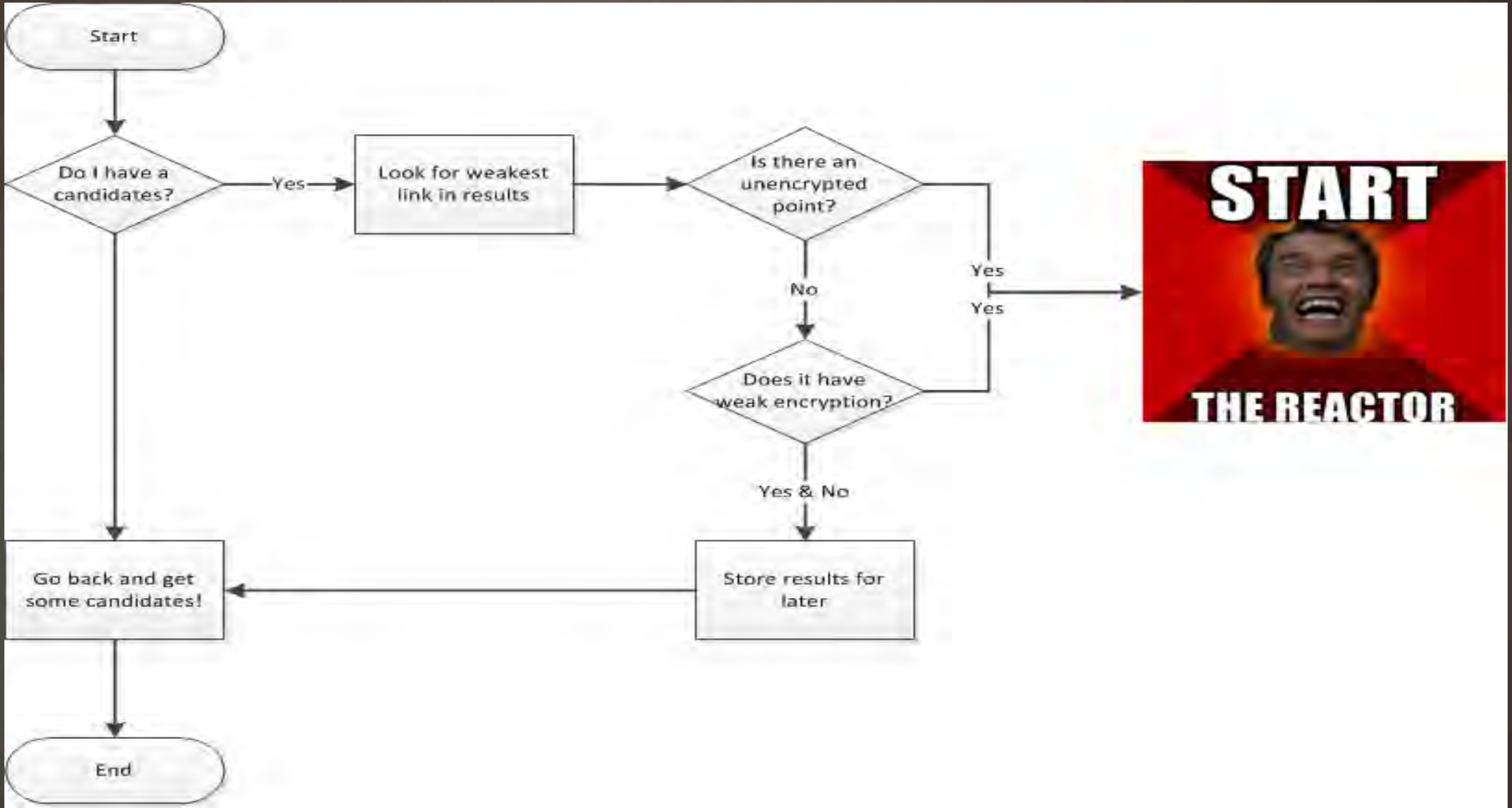
- Enhance location data by comparing new data to existing data and select a “candidate”

Updating entries

- Location and Strength approach



Selecting a candidate



Start

Do I have a candidates?

Yes

Look for weakest link in results

Is there an unencrypted point?

Yes

No

Yes

Does it have weak encryption?

Yes & No

Store results for later

Go back and get some candidates!

End

Roadmap? Oh yes.

- Better triangulation algorithms
- Real-time WiFi map across all devices
- Easier integration points for any other tool to use

Wargarble – Part II

- Purpose: Connectivity + Data collection

- What does it do:

  - Strips and parses the info that Warscanble collected, specifically looking for open networks.
  - Connects and determines public gateway
  - Makes outbound handshake connections to remote server to determine what ports are open based on range or ports specified in config.
  - Stores results in database for final phase of reporting and plotting

- How Does it work:

  - Uses a combination of bash/sed/awk/Sqlite and python sockets to remote server

“Warrepo” – Part III

- Purpose:
  - Multiport traffic ACK server
  - Central collection of information
- What does it do:
  - Opens all ports to let anyone connect using any TCP port and responds. This provides a way to find out allowed Egress ports from anywhere for Wargarble.
  - Collects results from Warscanble’s data and plots centrally.
- How does it work:
  - SQLlite + PHP + IPtables + bash

Mitigation For The Masses

- Audit and review your traffic and firewall policies both ways
- Tune your appliances and/or applications
- Plan / deploy / segment your infrastructure
- Listen to your minions + cross dept relationships are key