

DYNAFA


DYNAMIC FIREWALL AUTHENTICATOR

David Reeves – EIT Hawke's Bay




WHAT IS IT?

A firewall which is able to periodically change over time, therefore limiting the ability for adversaries to spy on the state of any given port on the public facing interface of a router




WHY DID I MAKE IT?


To attempt to create a
100% impenetrable network



FUNDAMENTAL ASPECTS

- ▶ Access restriction (Address lists)
 - ▶ Configurable parameters (Total phases x No. of ports)
 - ▶ Creation of unpredictable mathematical relationships
 - ▶ Authentication process
 - ▶ Dynamic firewall rules
- 

BASIC CHARACTERISTICS

- ▶ Narrow aperture minimizes attack surface significantly
 - ▶ Counters port scanners
 - ▶ Counters replay attacks
 - ▶ Ambushes attackers with “poisoned” ports
 - ▶ Resource efficient filtering process
 - ▶ Nearly impossible to crack with brute force
- 

HOW DOES IT COMPARE?

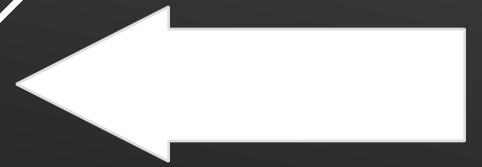
	Authentication	Encryption
<i>No firewall</i>	<i>No</i>	<i>No</i>
<i>Simple Brute-force Protection</i>	<i>Partial</i>	<i>No</i>
<i>DYNAFA</i>	<i>Yes</i>	<i>No</i>
<i>IPsec</i>	<i>Yes</i>	<i>Yes</i>
<i>Total lockdown</i>	<i>N/A</i>	<i>N/A</i>



HOW DOES IT WORK?



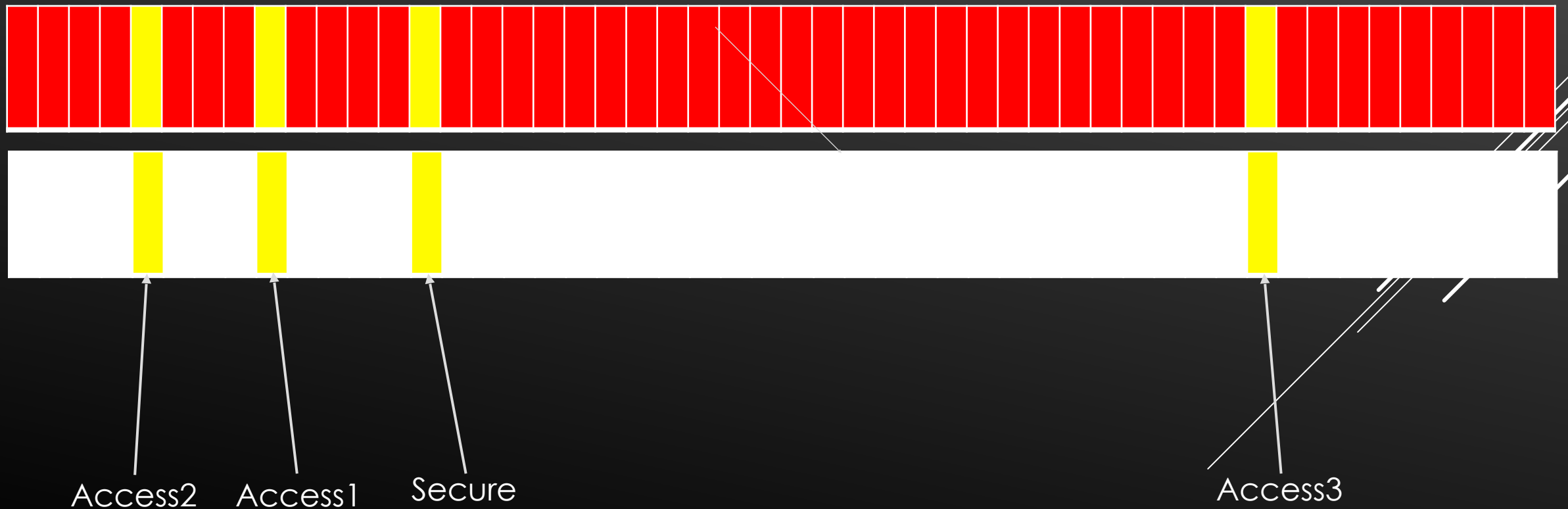
Firewall rule
changes



Authentication
Packets

CLIENT - ROUTER RELATIONSHIP

Blacklist Whitelist



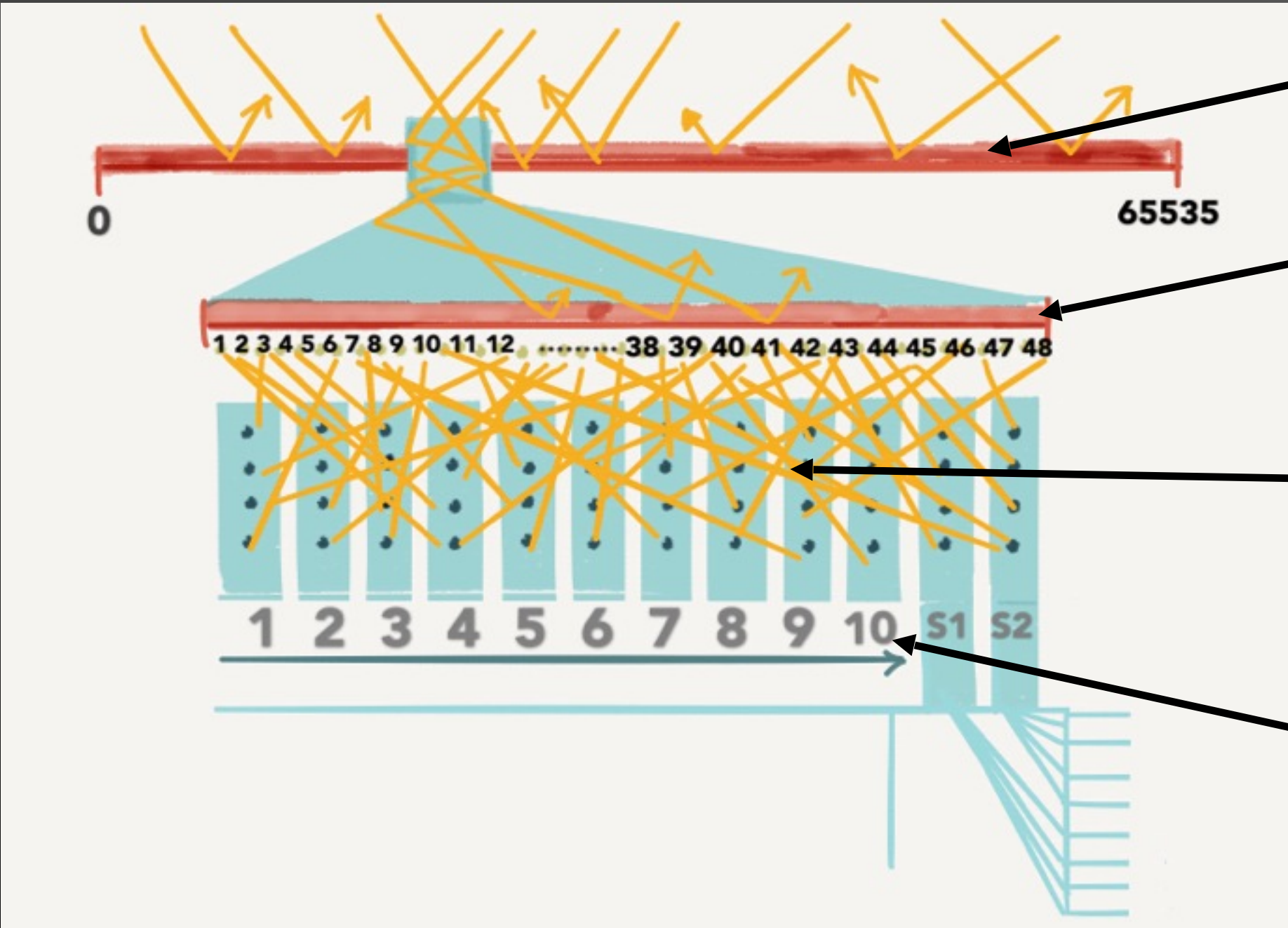
RULE CONTROL METHODS

Host	Network Address	Tool
<i>Routerboard</i>	<i>127.0.0.1</i>	<i>Scheduler</i>
<i>Local Host</i>	<i>192.168.xxx.xxx</i>	<i>Crontab - SSH</i>
<i>Remote Host</i>	<i>xxx.xxx.xxx.xxx</i>	<i>SSH</i>



IMPLEMENTATION AUTHENTICATION

- ▶ Add basic firewall rules
- ▶ Generate unique number set
- ▶ Apply hard-coded values to firewall rules using an automatically generated script
- ▶ Automatically generated script creates 4 SYN packets using Nmap
- ▶ TCP SYN Packets transit the internet and arrive at firewall
- ▶ Router will add the IP to each sequential address list if each packet matches the set rules



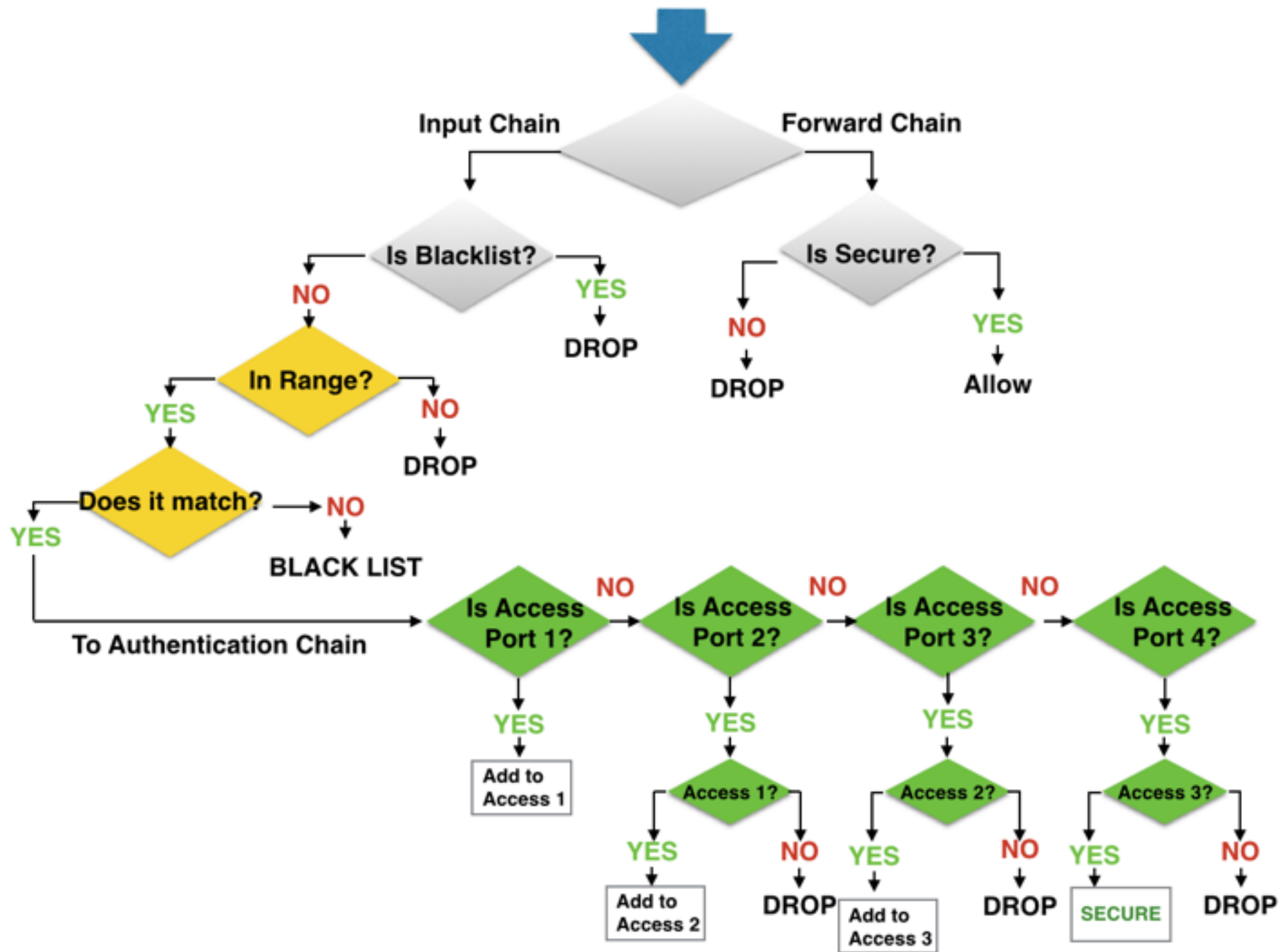
TOTAL SURFACE OF INTERFACE

REDUCED SURFACE AREA

RELATIONSHIP BETWEEN SURFACE AND AUTH CHAINS

DIFFERENT POSSIBLE STATES OF FIREWALL OVER TIME





PROBABILITY OF BRUTE FORCE

$$1 / 65535 = A$$

$$A = 1.53e-5$$

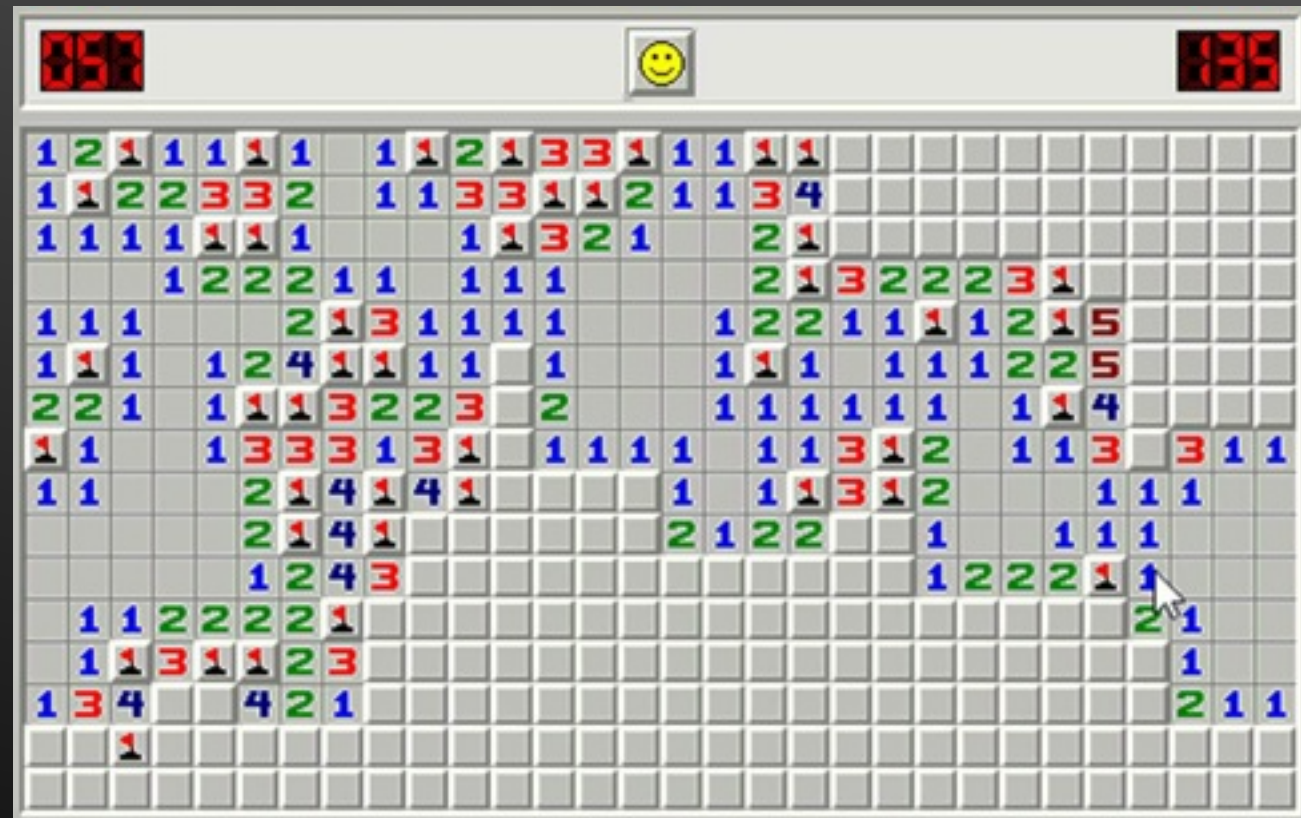
$$A^4 = 5.42e-20$$

$$A^8 = 2.93e-39$$

$$4! = 24$$

$$8! = 40320$$

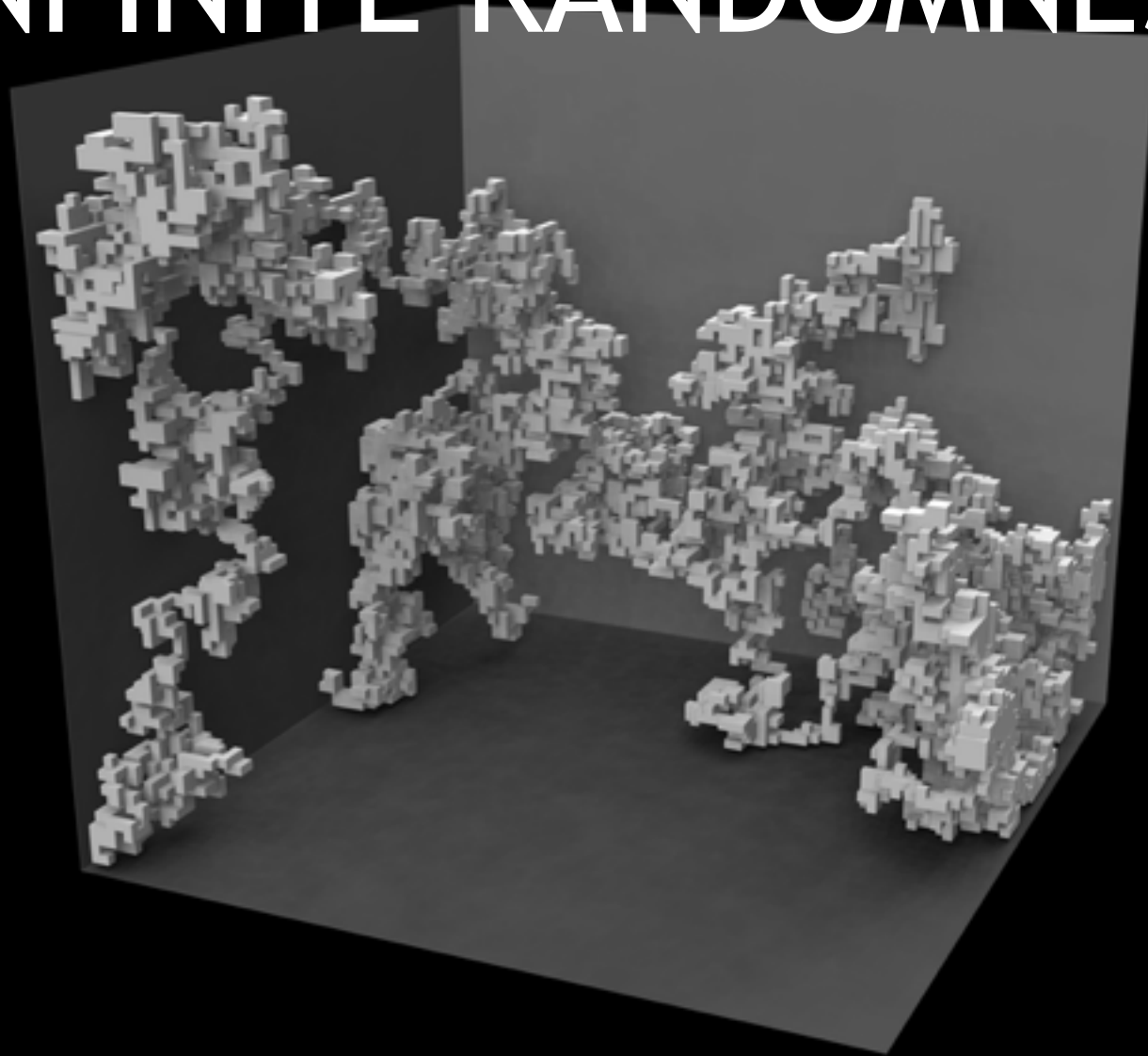
$$12! = 479,001,600$$



DYNAFA Vs NMAP



INFINITE RANDOMNESS

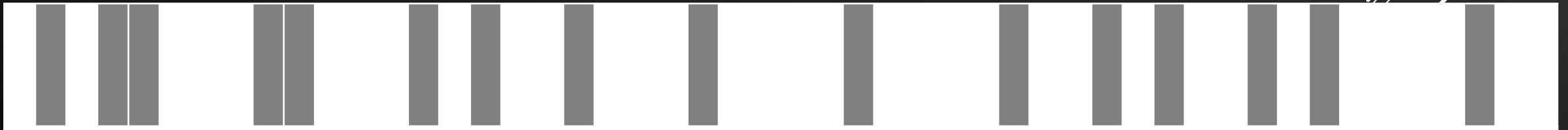
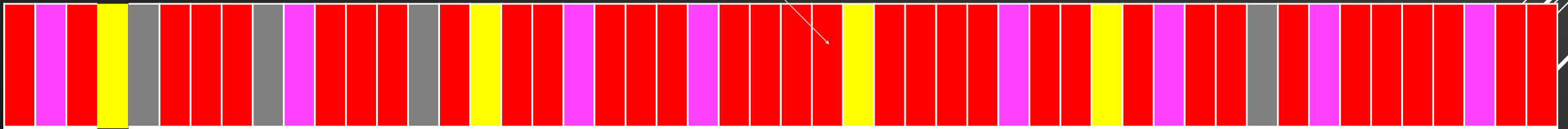


COUNTERING PORT SCANS


Service Ports

Backdoor Auth Chain


Dynamic Auth Chain



COUNTERING REPLAY ATTACKS


- ▶ Use of a VPN to prevent Wi-fi sniffing attacks
 - ▶ Sending of fake packets to occlude the real ones
 - ▶ Autonomous monitoring and statistical analysis using AI
 - ▶ Manually blacklisting known threats
 - ▶ Never using the same sequence twice
- 
- A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

WHERE TO NEXT?

- ▶ Continue to educate others
 - ▶ Continue researching black-hats
 - ▶ Continue developing security software
 - ▶ DYNABOT
 - ▶ DYNAFA v2
- 

Code is available at
www.dynafa.com

Let me know your thoughts!
80257@protonmail.com

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.