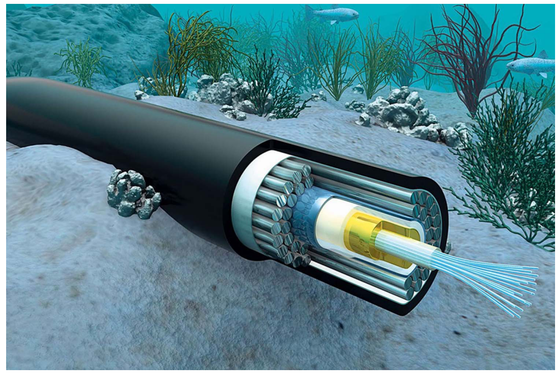
Computer Network Measurement and Security

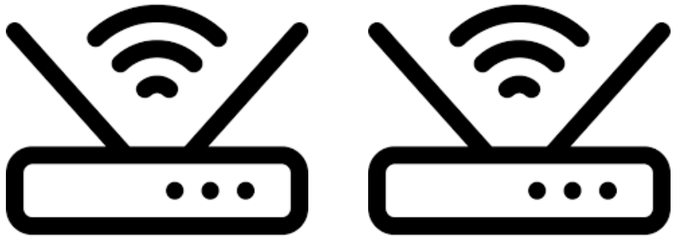
ECE 239AS

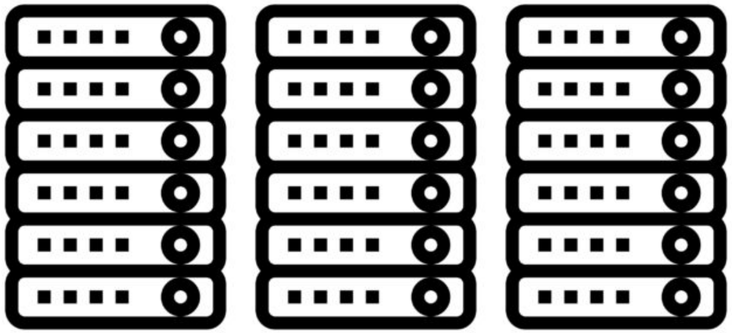
Liz Izhikevich

The Internet is composed of multiple constituents

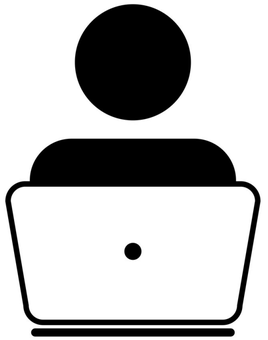


Networks



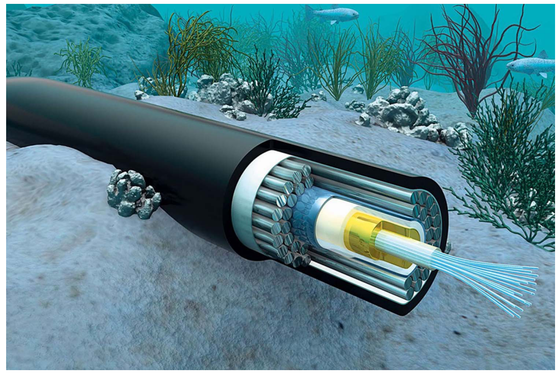


Devices
(+Services)

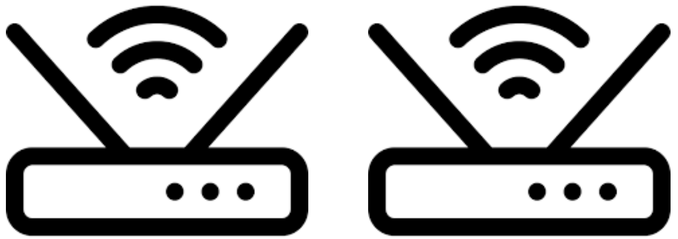


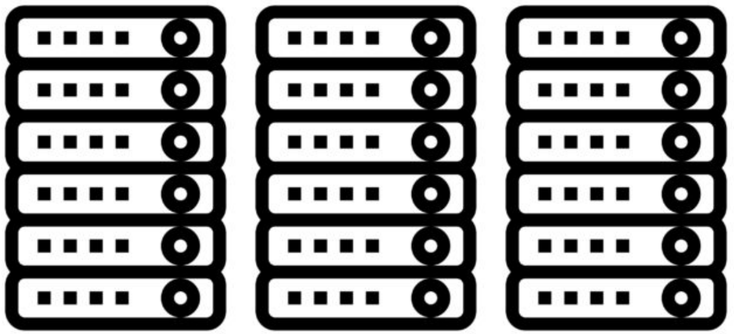
Users
(+Attackers)

The Internet is composed of multiple constituents

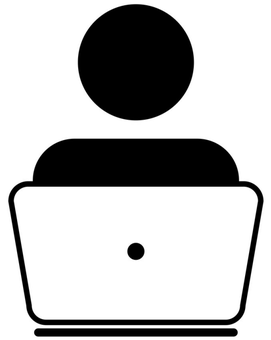


Networks





Devices
(+Services)

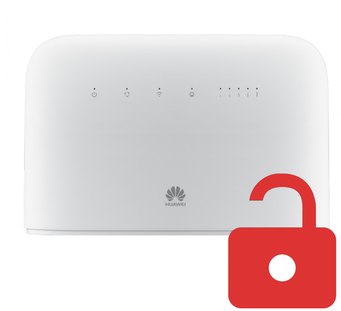


Users
(+Attackers)

The Internet consists of many devices

The Internet consists of many devices…that are (unintentionally) publicly-accessible

Attackers are finding and abusing Internet exposed devices

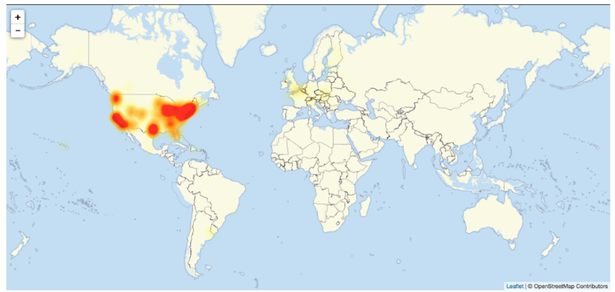


Attackers are finding and abusing Internet exposed devices

The New York Times

Hackers Used New Weapons to Disrupt Major Websites Across U.S.

Share full article



A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com.

Attackers are finding and abusing Internet exposed devices

The New York Times

Hackers Used New Weapons to Disrupt Major Websites Across U.S.

Share full article

A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com.

Why are operators not securing their devices?

The New York Times

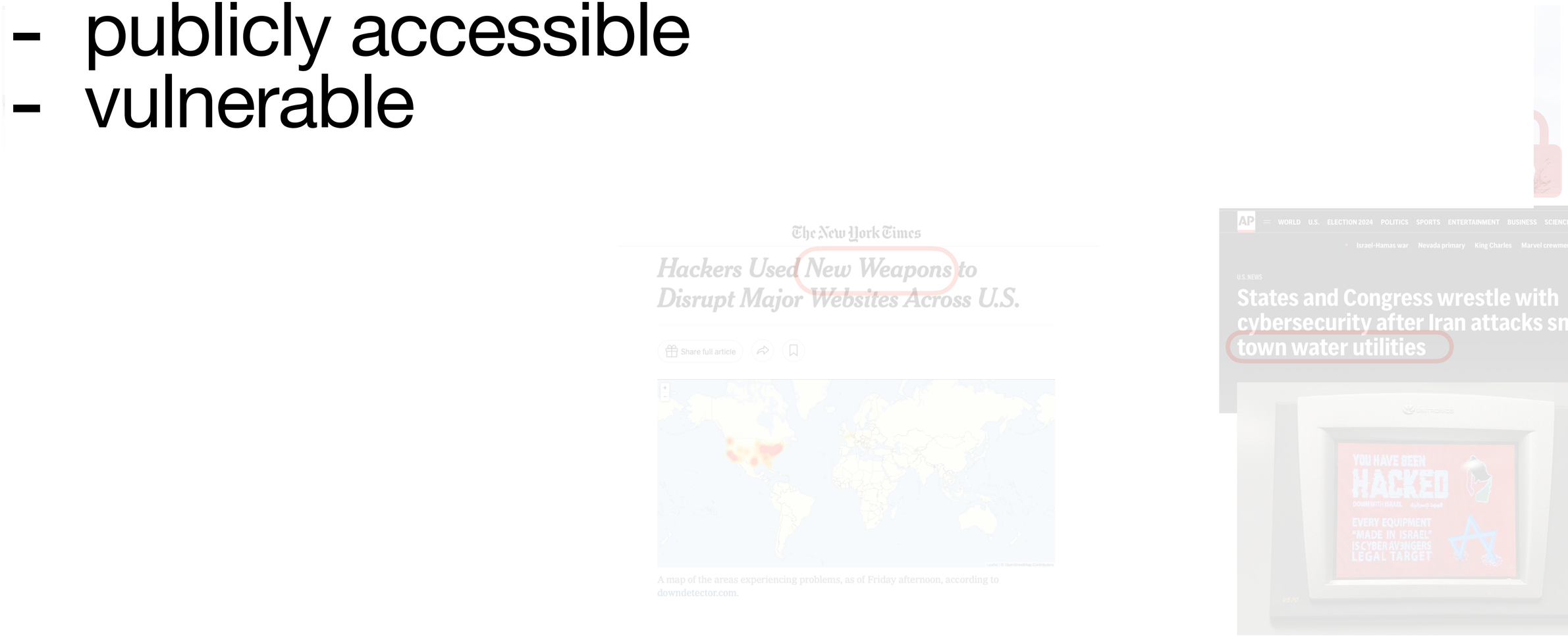
Hackers Used New Weapons to Disrupt Major Websites Across U.S.

Share full article

A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com.

Why are operators not securing their devices?

Operators often do not know their devices are
- publicly accessible
- vulnerable



Why are operators not securing their devices?

Operators often do not know their devices are
- publicly accessible
- vulnerable

The New York Times

Hackers Used New Weapons to Disrupt Major Websites Across U.S.

Share full article

A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com.

Why are operators not securing their devices?

Operators often do not know their devices are
- publicly accessible
- vulnerable

Protecting the Internet requires visibility into devices, networks, and their users

Why are operators not securing their devices?

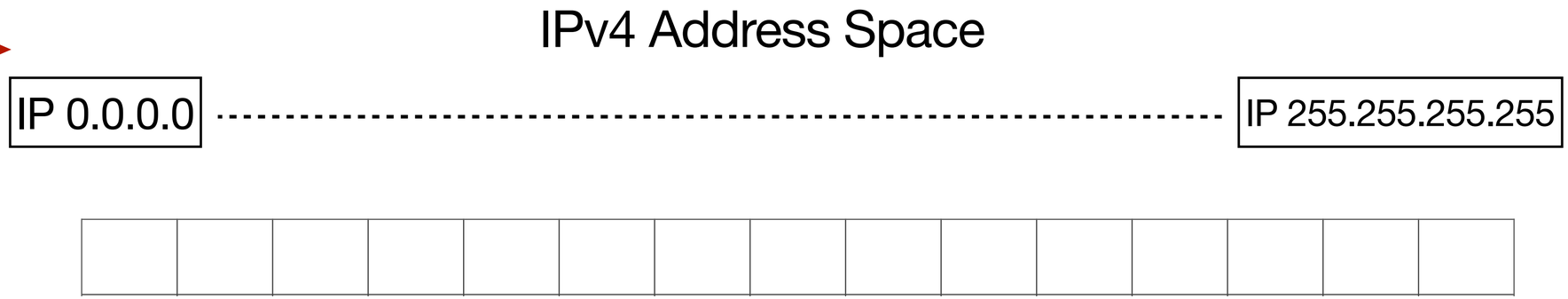
Operators often do not know their devices are
- publicly accessible
- vulnerable

Internet Measurement!

Protecting the Internet requires visibility into devices, networks, and their users

Visibility is challenging because the Internet is large and sparse

4.2 billion (2^32) possible addresses



Visibility is challenging because the Internet is large and sparse

4.2 billion (2^32)
possible addresses

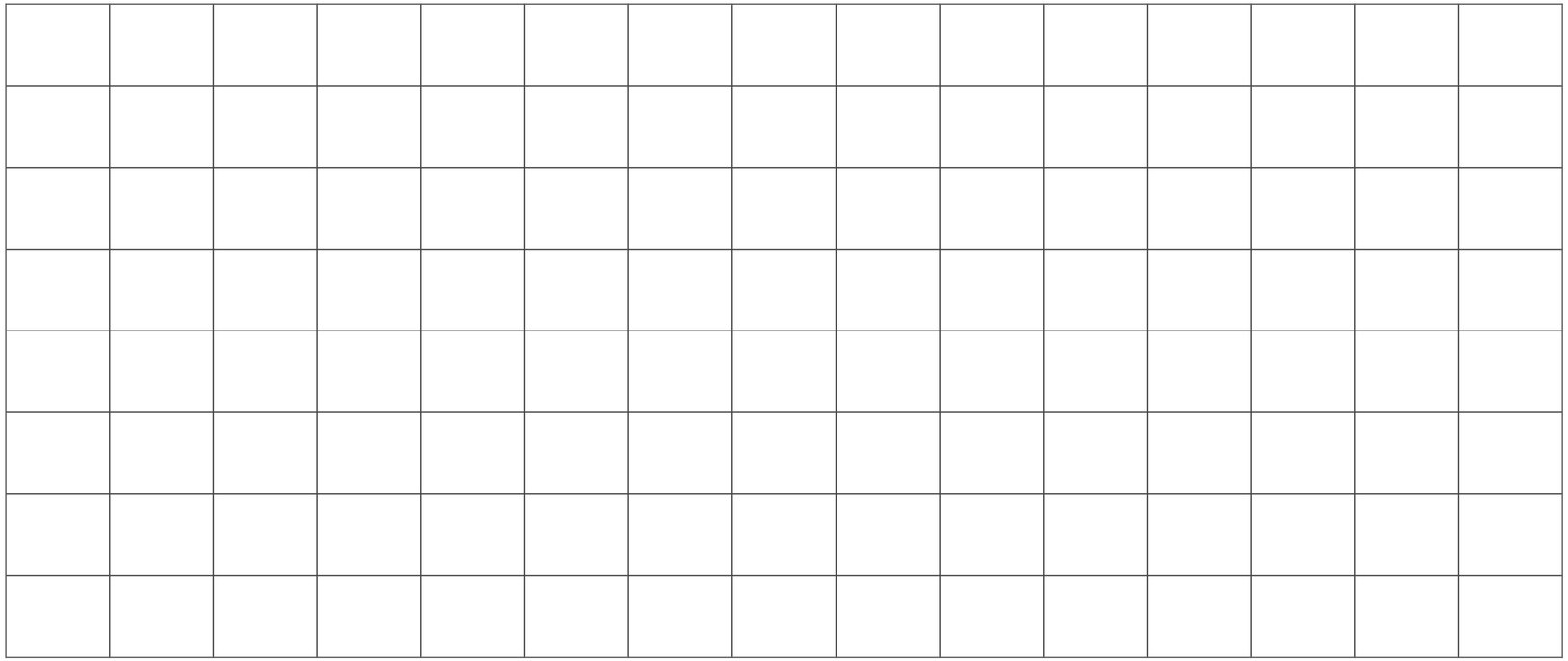
IPv4 Address Space

IP 0.0.0.0 ---------- IP 255.255.255.255

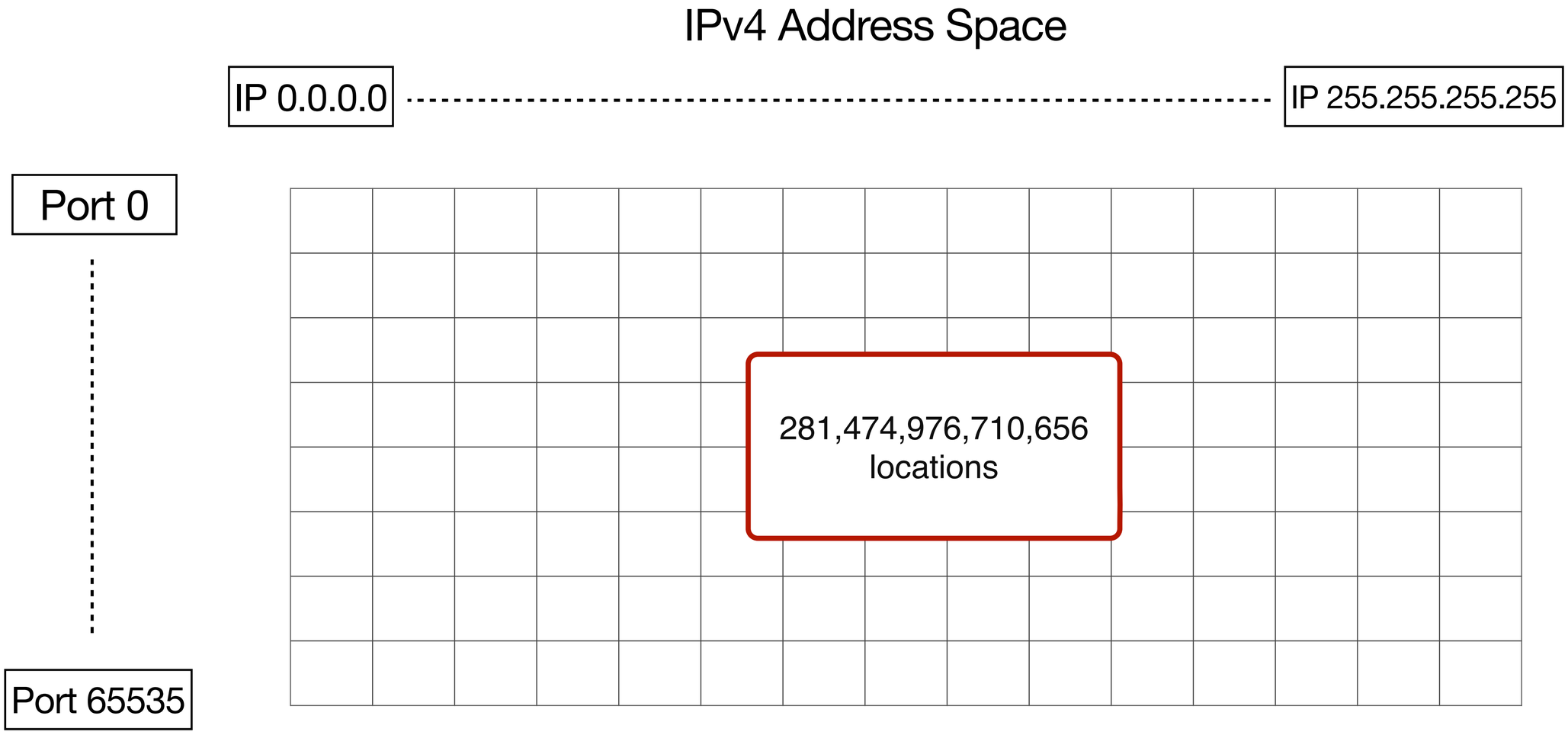
Port 0

65536 (2^16)
possible ports

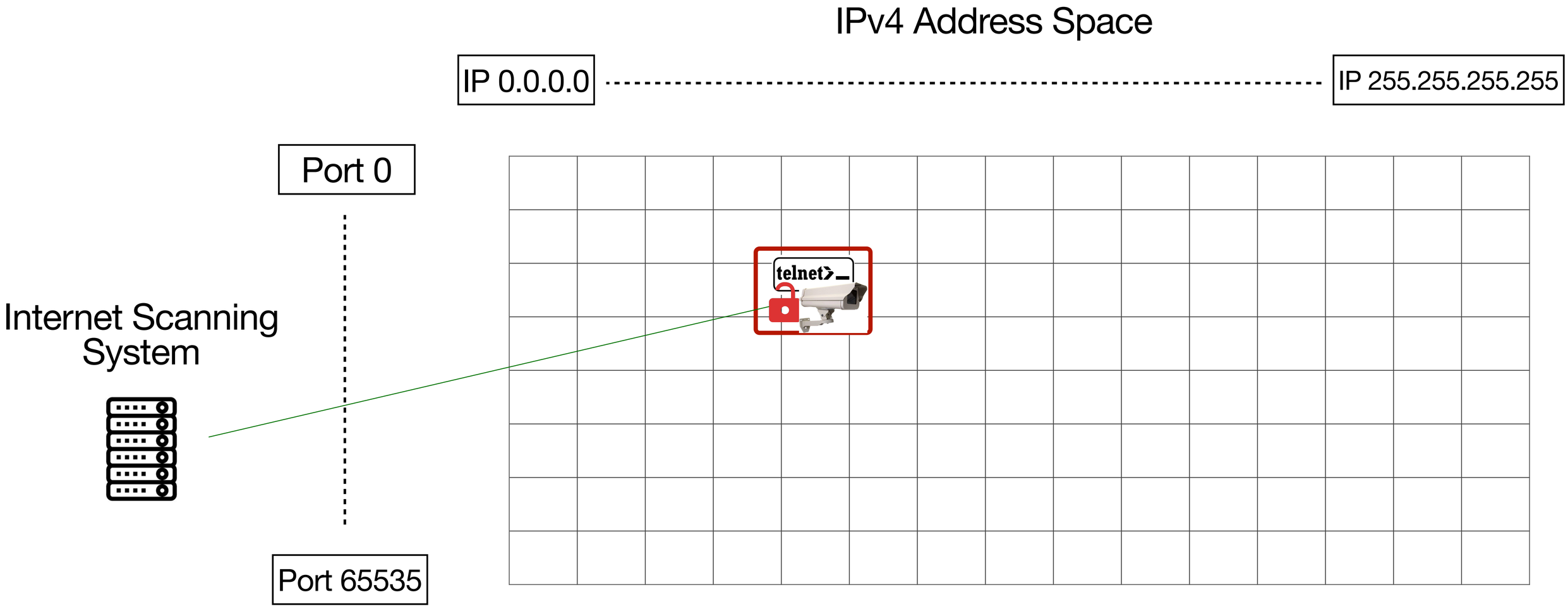
Port 65535



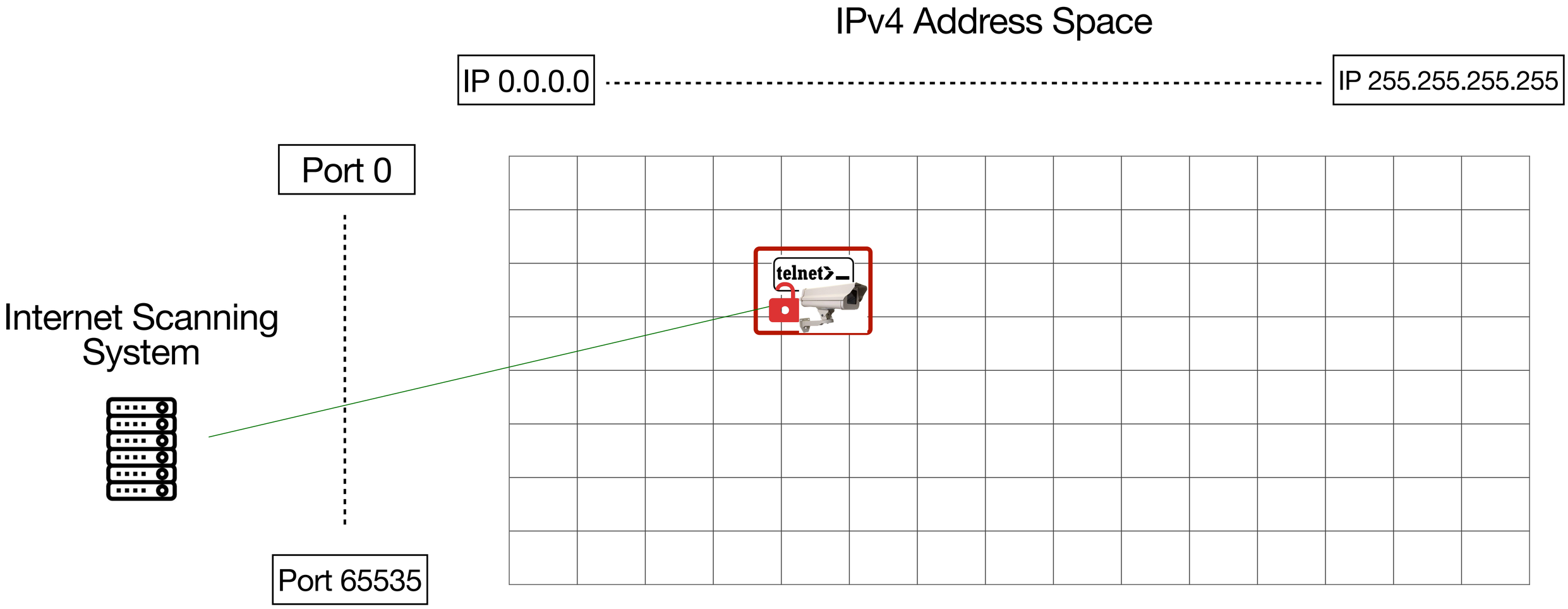
Visibility is challenging because the Internet is large and sparse



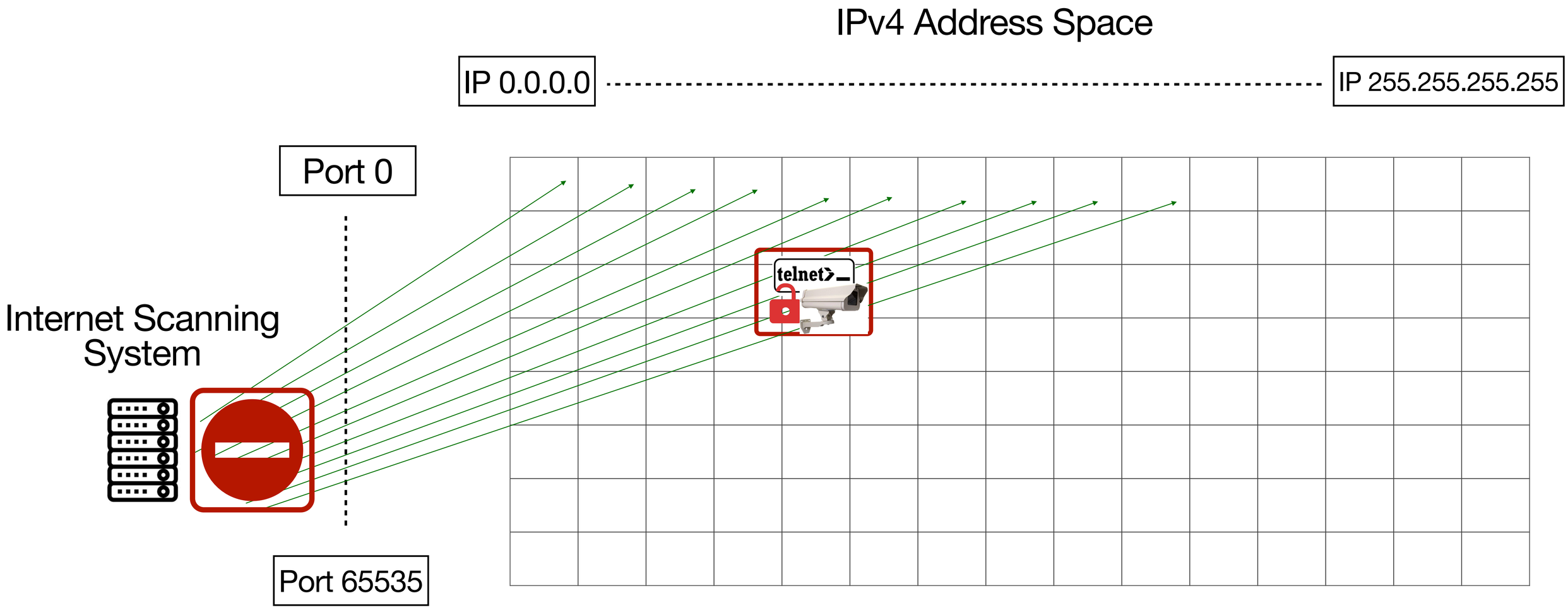
To detect services, “Internet scanning” probes (IP,Port) pairs



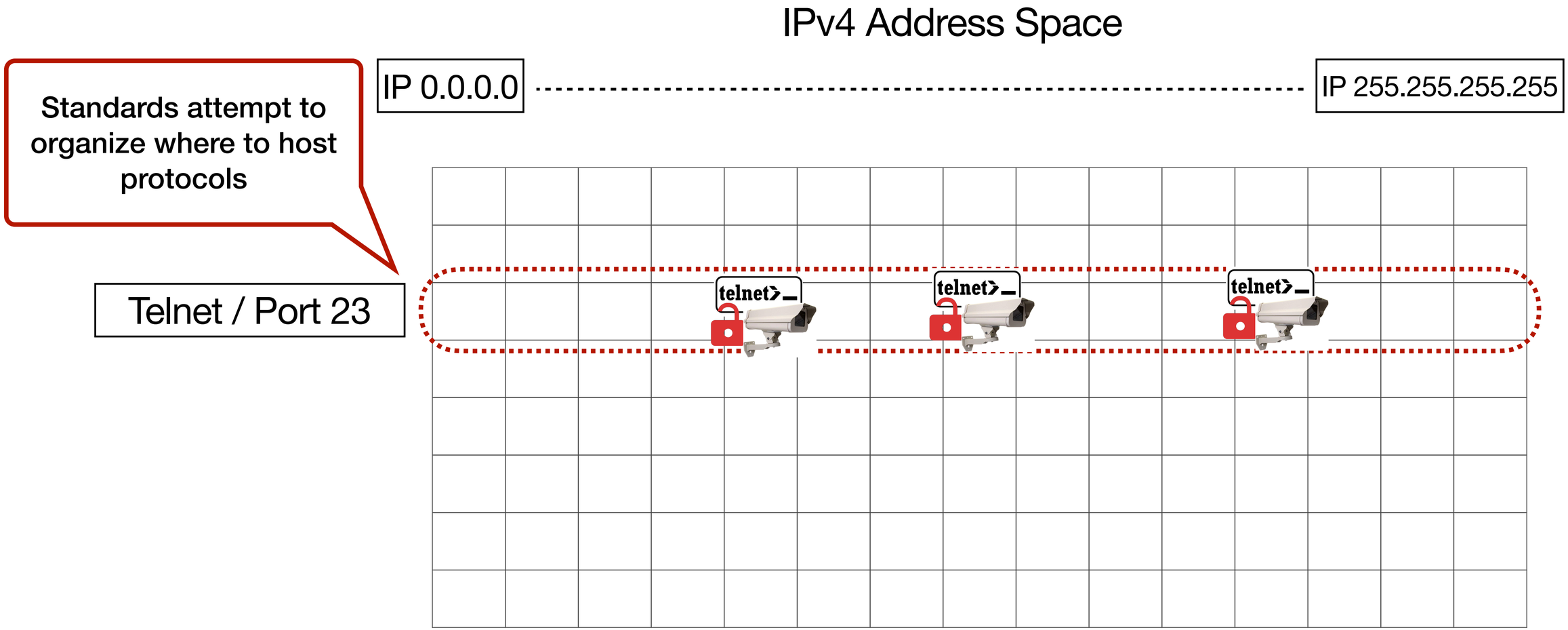
How do scanning systems know where to find services?



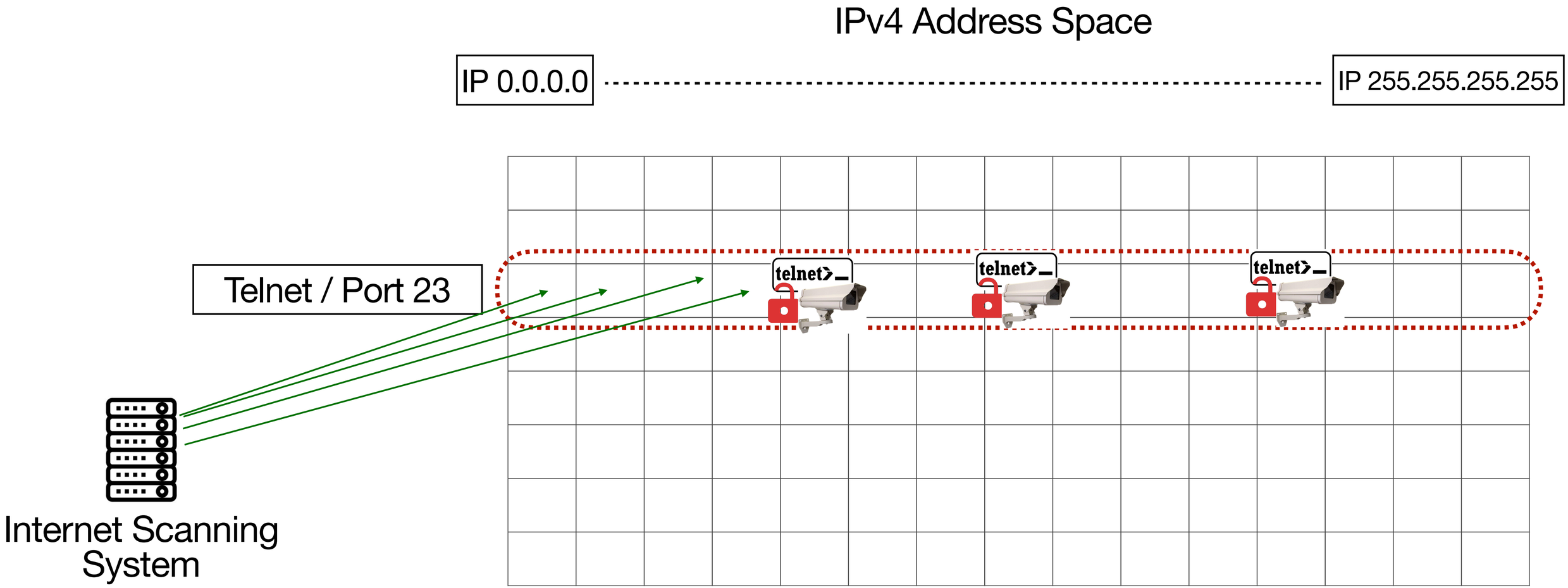
The Internet is too large to exhaustively search



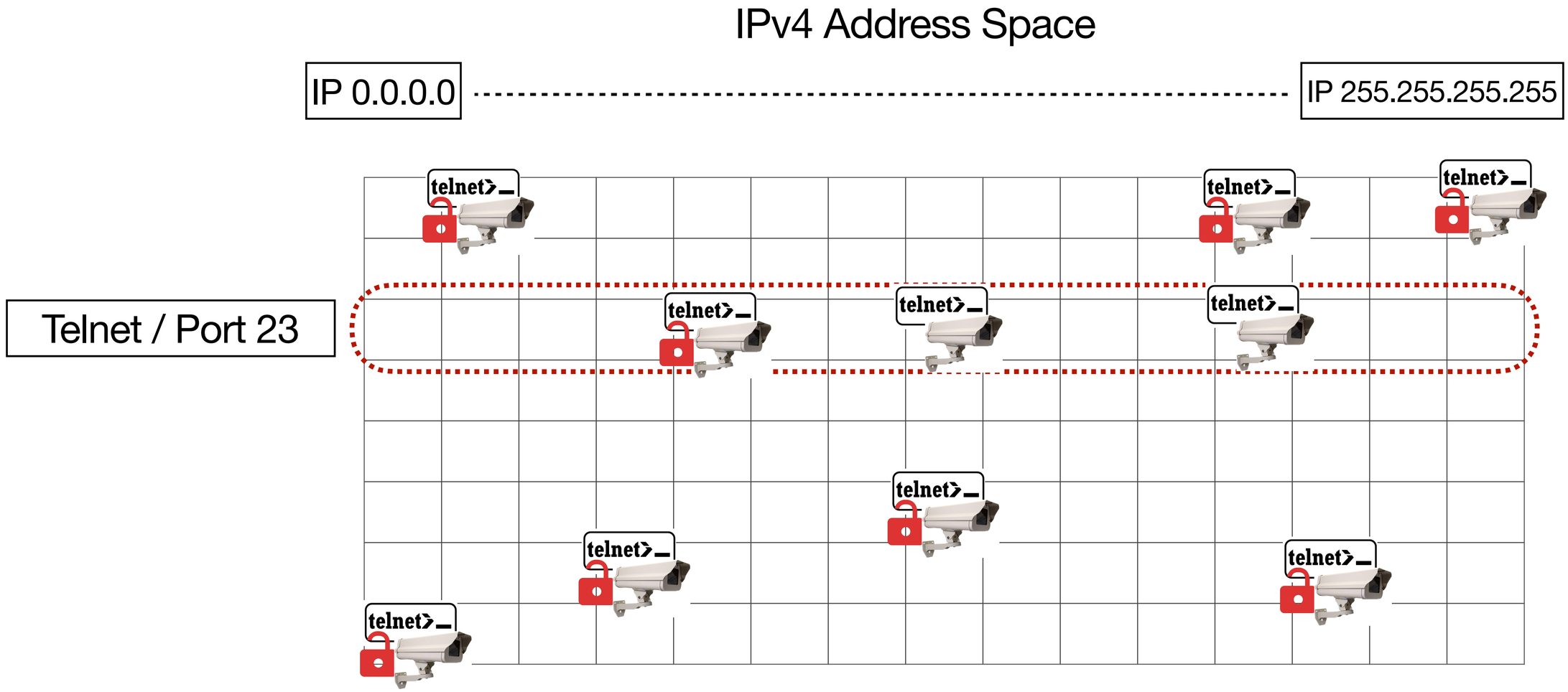
Existing Internet scanning systems use standards to find services



Existing Internet scanning systems use standards to find services



But, the majority of services are non-compliant!



LZR: Identifying Unexpected Internet Services. USENIX Security' 21.

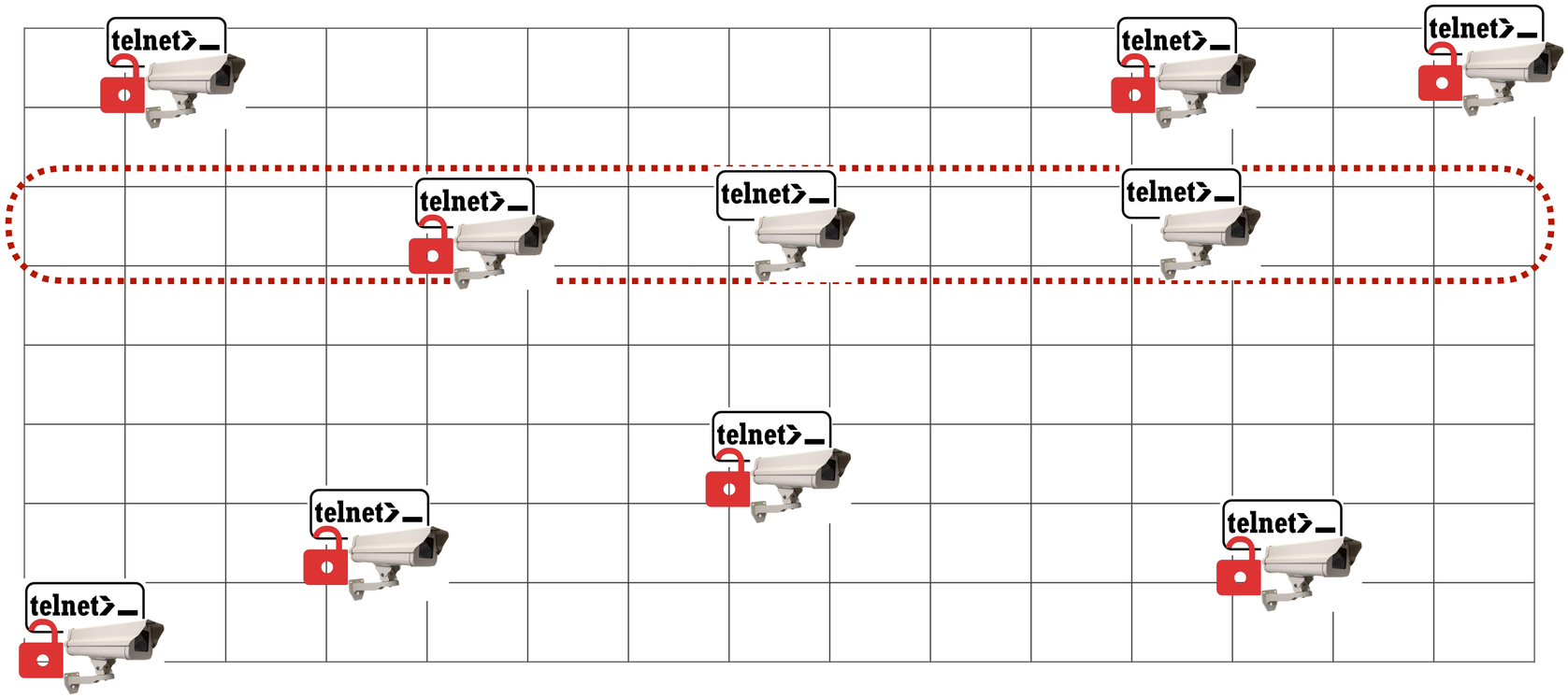
But, the majority of services are non-compliant!

95% of Telnet is not on port 23

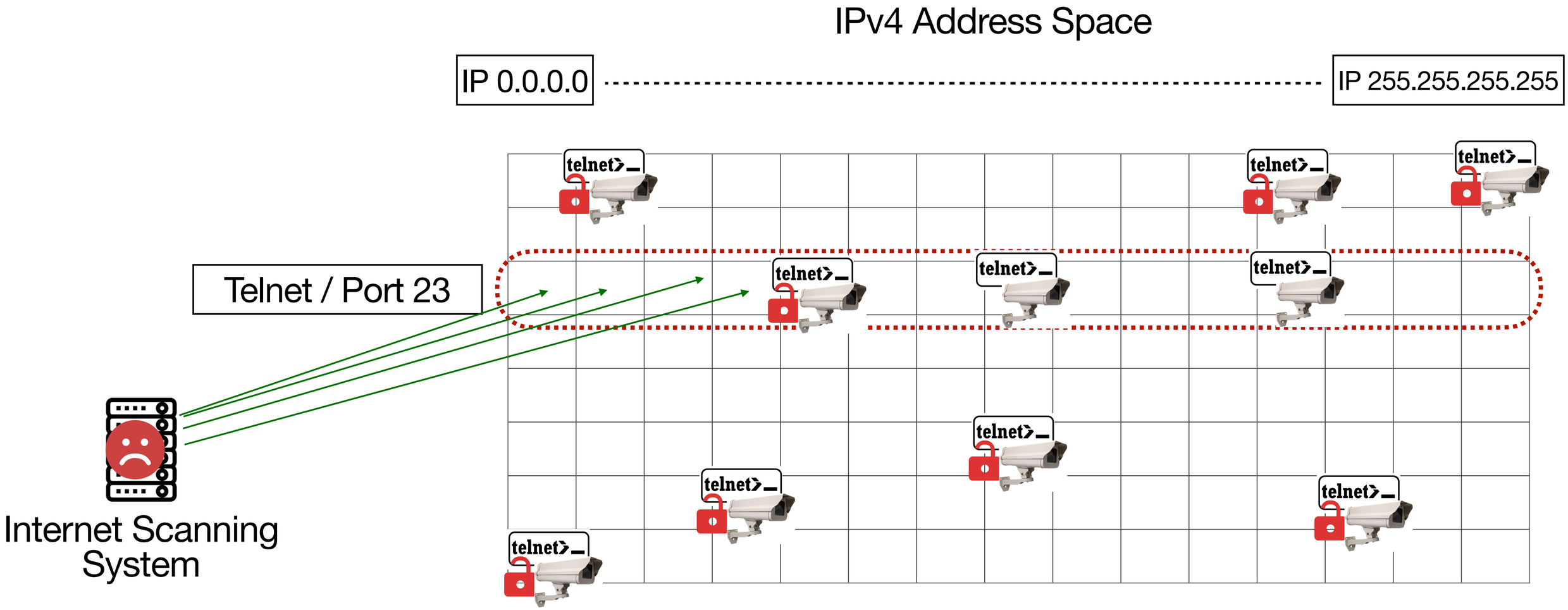
IPv4 Address Space

IP 0.0.0.0 ---------- IP 255.255.255.255

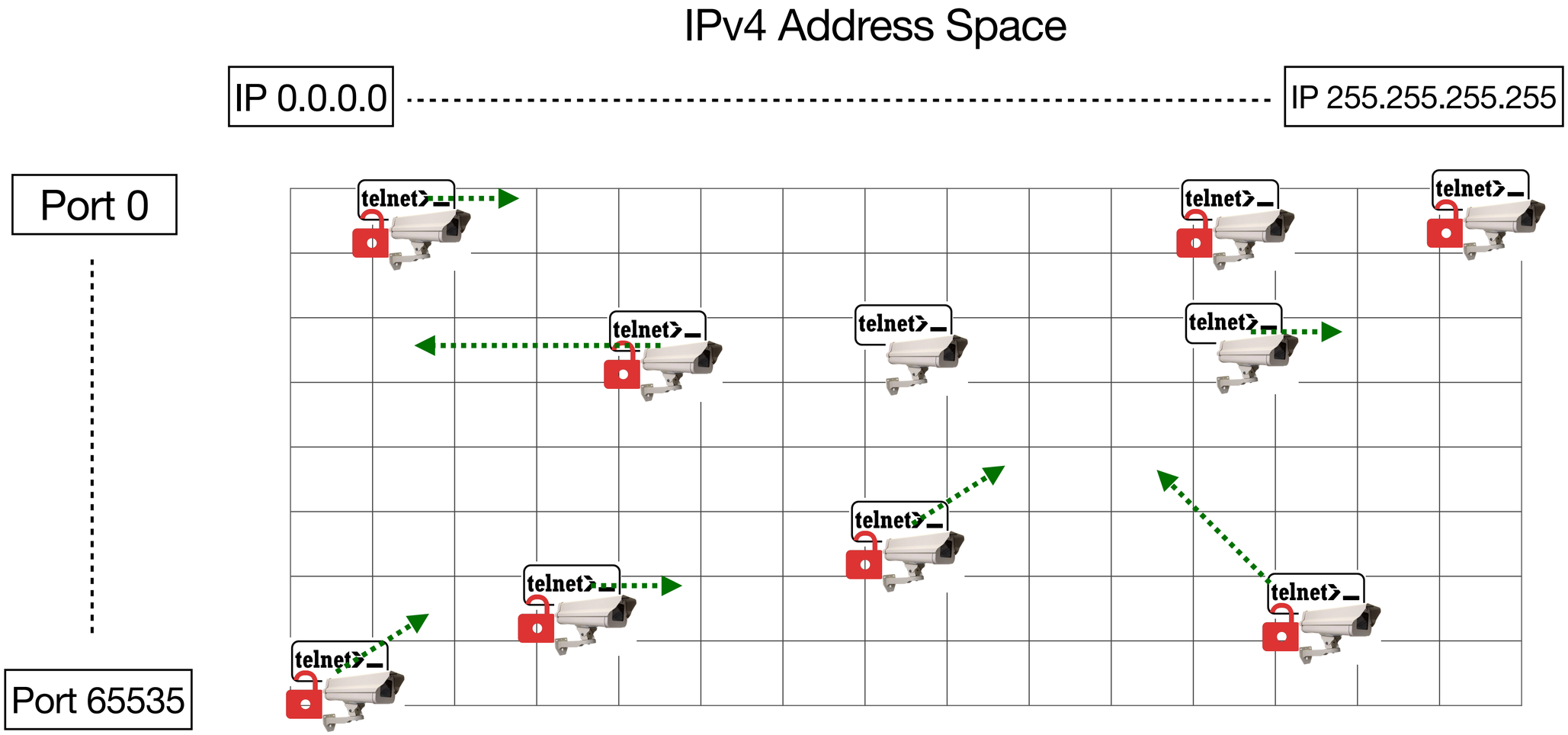
Telnet / Port 23



Existing systems miss the *majority* of devices



Internet service location constantly changes



The Internet is Complex

Internet

Inconsistent

Large

Ephemeral

This course covers many aspects the Internet and its Security

IPv4 

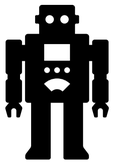
Internet Scanning Techniques

Abusing Internet Scanning (Botnets)

Satellites 

Insecure GEO Satellite Networks

Measuring LEO Satellite Networks

Machine Learning 

Applications for Network Security

Large Language Models

IPv6 

Internet Scanning Techniques

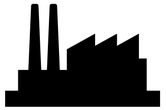
Internet of Things (IoT) 

Internet Criminals 

Cloud 

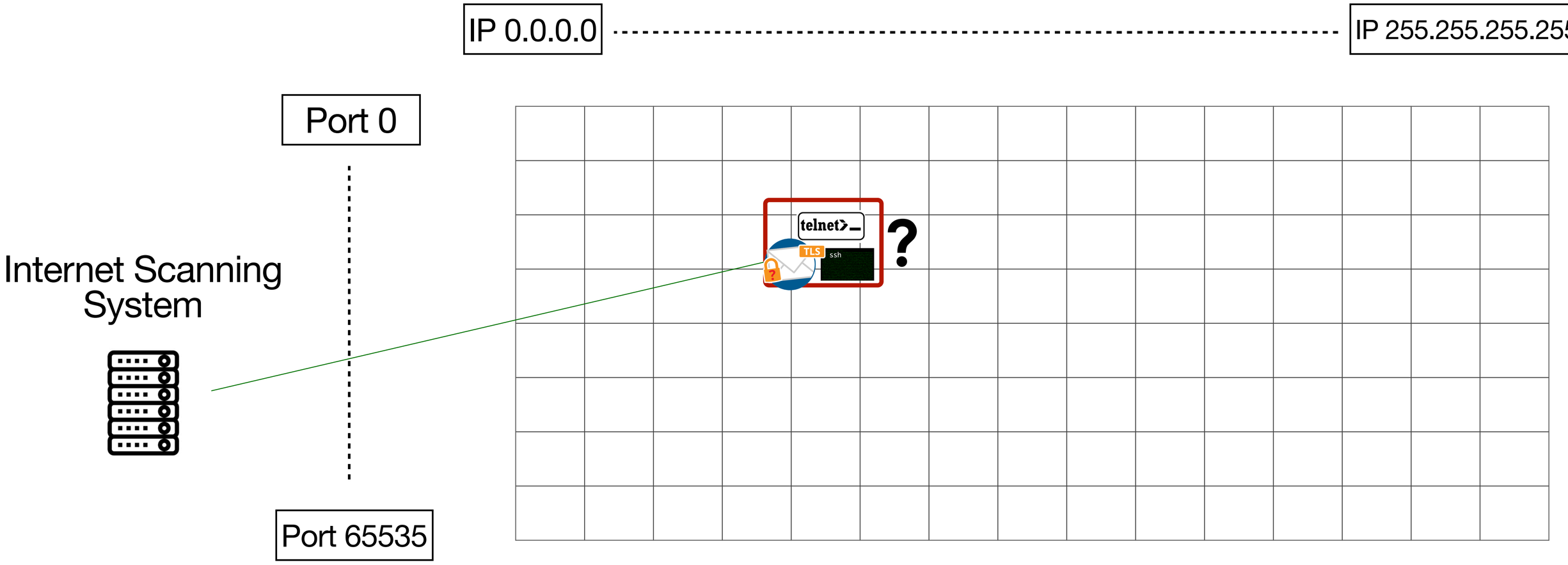
Scanning and Abuse of Storage

Abuse of Compute

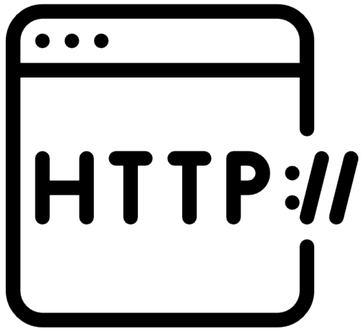
Industrial Control Systems (ICS) 

LZR: Identifying Unexpected Internet Services

How do we efficiently identify services on unexpected ports?



Community Standards assigns services to ports



IP 1.2.3.4

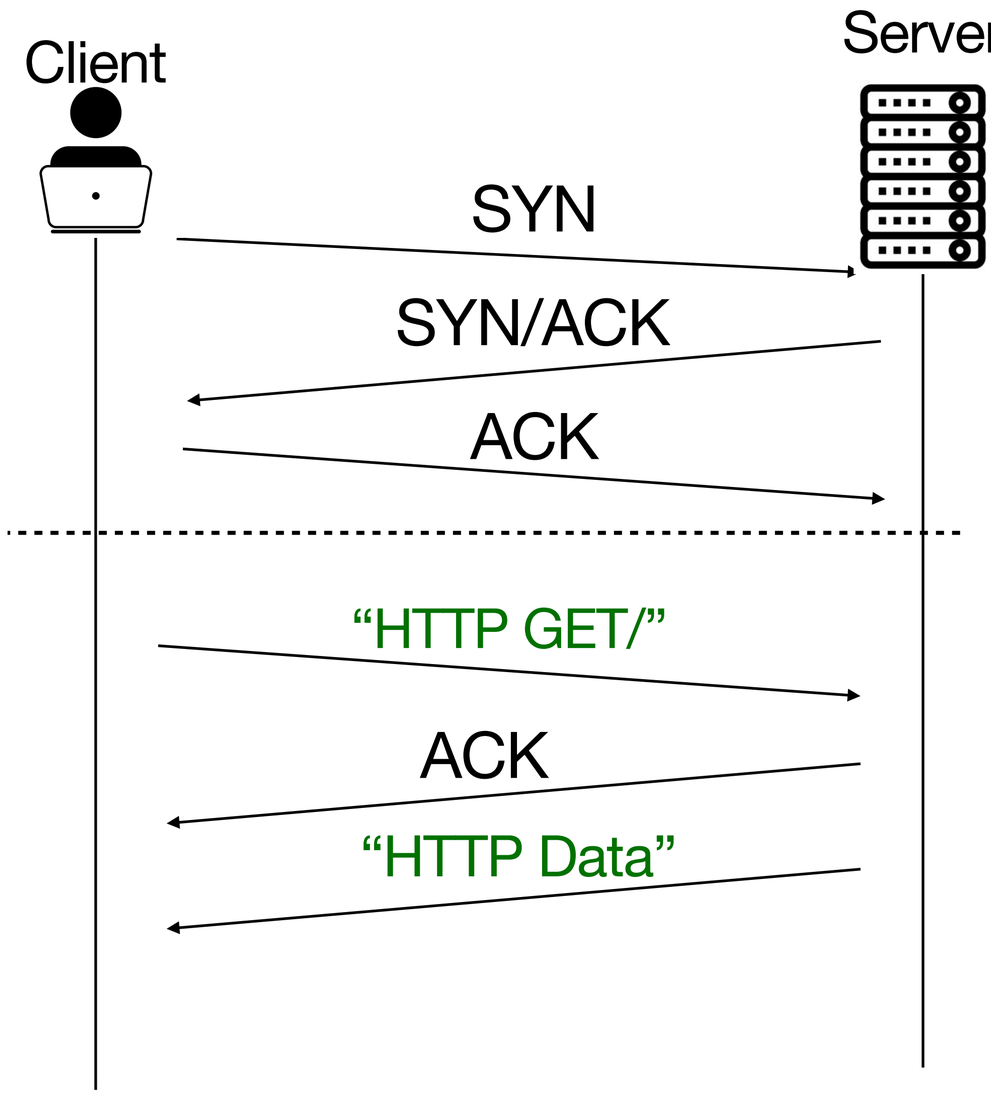
Port 22

Port 80

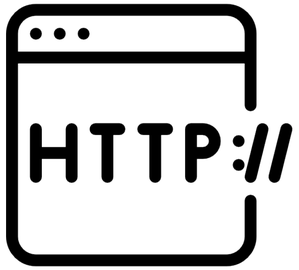
Port 443

Port 23

Traditional TCP Handshake Assumes Service

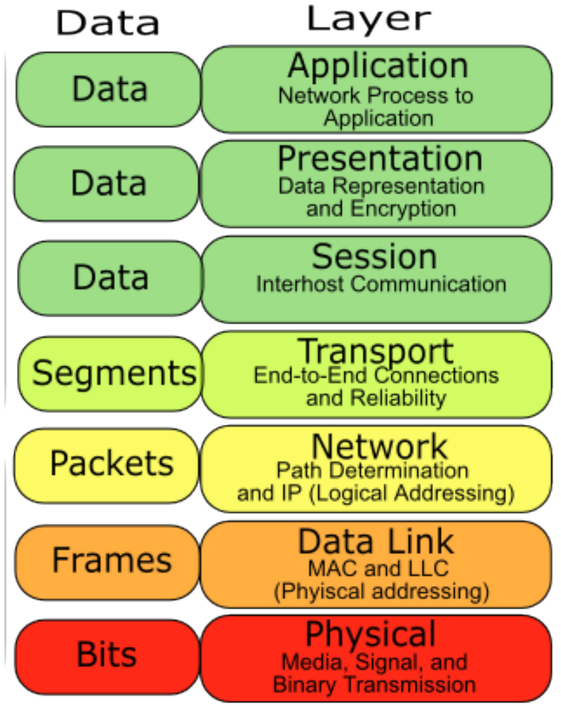


IP:Port (11.22.33.44:80)

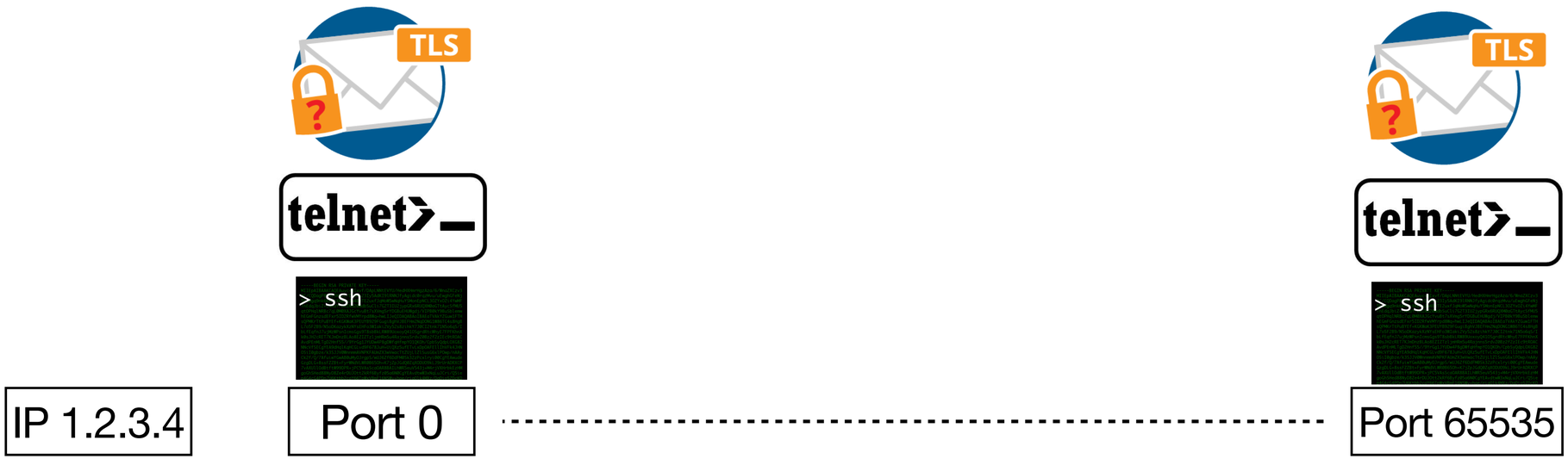


Layer 4 Handshake

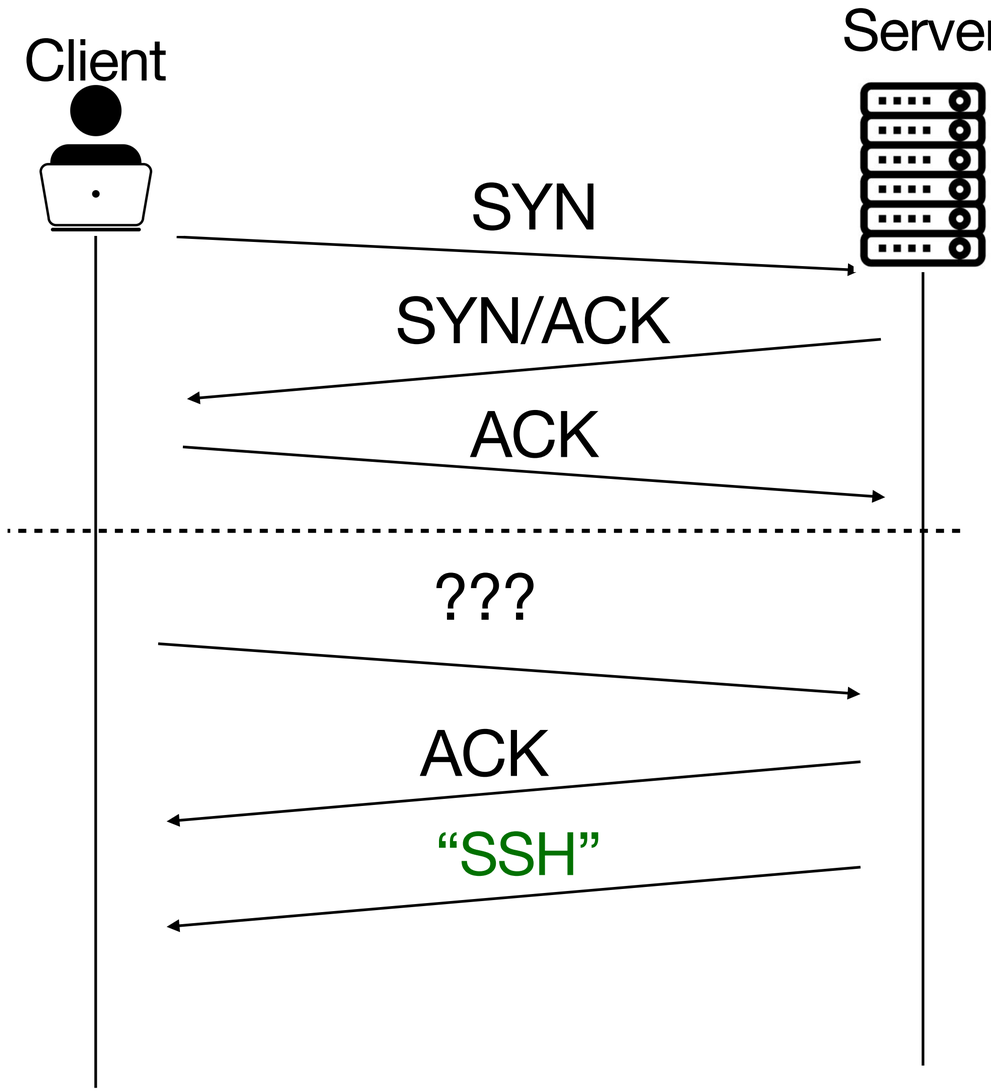
Layer 7 Handshake



But technically, any service can be hosted on any port



Traditional TCP Handshake Does Not Know True Service



IP:Port (11.22.33.44:80)

Layer 4 Handshake

Layer 7 Handshake

LZR: Identifying Unexpected Internet Services

Liz Izhikevich, *Stanford University;* Renata Teixeira, *Inria;*
Zakir Durumeric, *Stanford University*

https://www.usenix.org/conference/usenixsecurity21/presentation/izhikevich

- Where are Internet services deployed in practice?

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

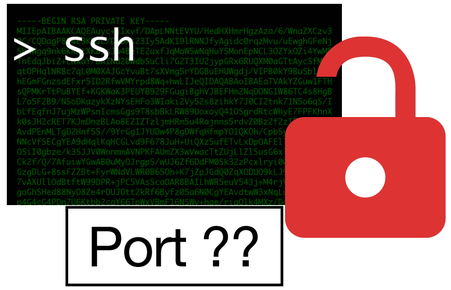
LZR: Identifying Unexpected Internet Services

Liz Izhikevich, *Stanford University;* Renata Teixeira, *Inria;*
Zakir Durumeric, *Stanford University*

https://www.usenix.org/conference/usenixsecurity21/presentation/izhikevich

- Where are Internet services deployed in practice?

- What is the security posture of services on unexpected ports?

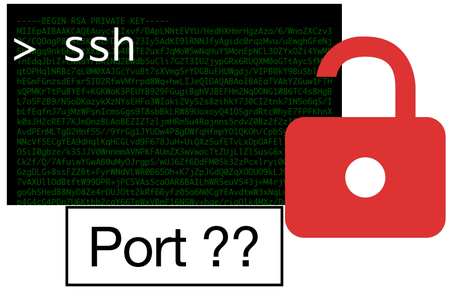


usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

LZR: Identifying Unexpected Internet Services
Liz Izhikevich, *Stanford University;* Renata Teixeira, *Inria;*
Zakir Durumeric, *Stanford University*
https://www.usenix.org/conference/usenixsecurity21/presentation/izhikevich

- Where are Internet services deployed in practice?

- What is the security posture of services on unexpected ports?



- How do we efficiently identify services on unexpected ports?

Questions?