How to Secure Mainframe TCP/IP

Stu Henderson
5702 Newington Road
Bethesda, MD 20816

stu@stuhenderson.com
www.stuhenderson.com
(301) 229-7187

ABSTRACT

Most mainframe data centers now have at least one mainframe connected to TCP/IP, often with some connection to the Internet. While the z/OS software gives a large number of tools to secure these connections, these tools often are not used. (If you think you don't use TCP/IP with your z/OS systems, try issuing the TSO command NETSTAT.)

In this session, Stu explains IP and TCP clearly, describes the security risks and the security tools you already have for free with z/OS, and shows you how to go about implementing the tools. You will learn why z/OS is considered the "most securable TCP/IP platform available". You will also learn how to make yours effectively secured.

AGENDA

1. Introduction

2. The Risks

3. The Protections

4. Summary: Call to Action

1. Introduction

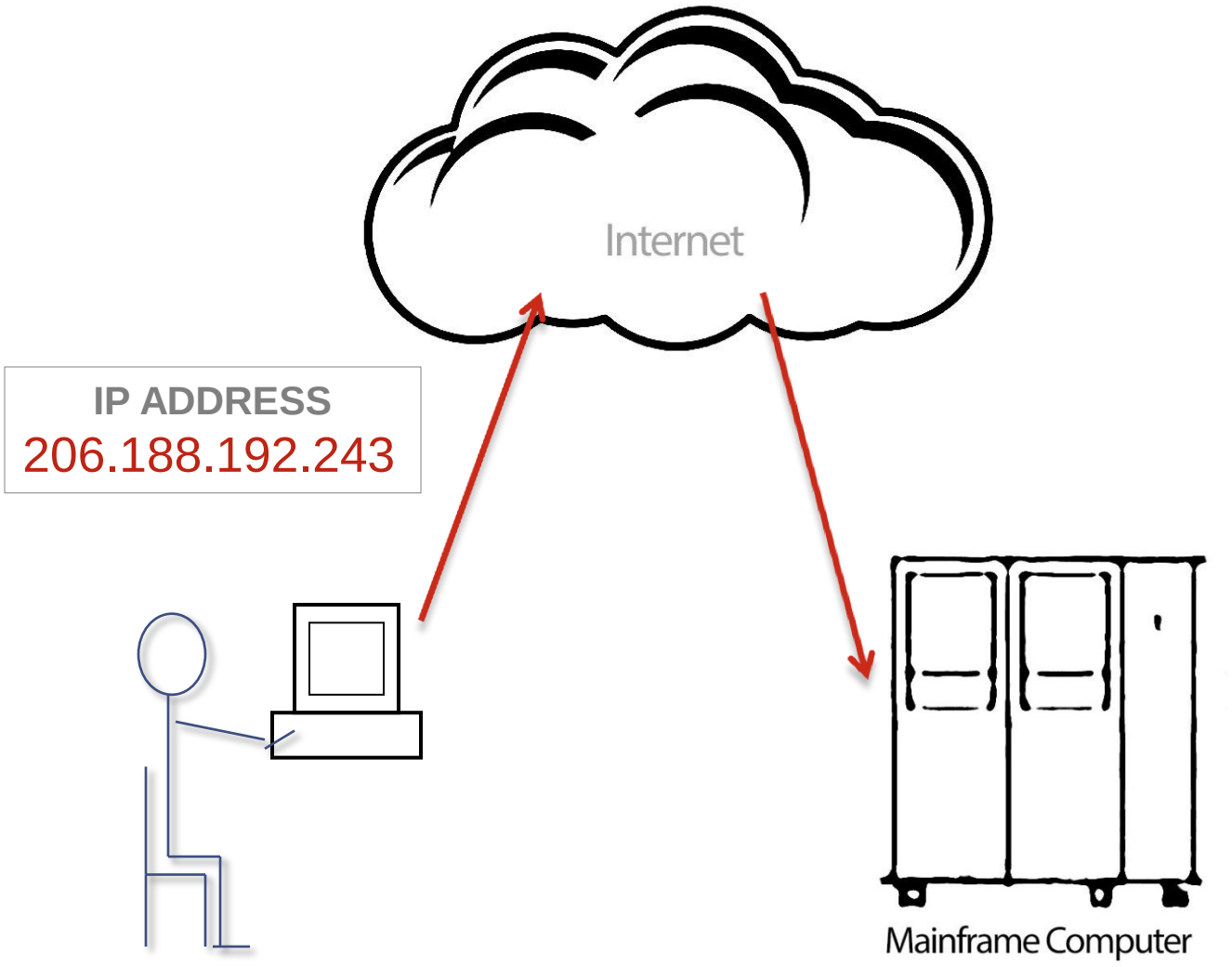
TCP/IP is:

- How a program on one computer shares data with a program on a different computer
- Transmission Control Protocol / Internet Protocol

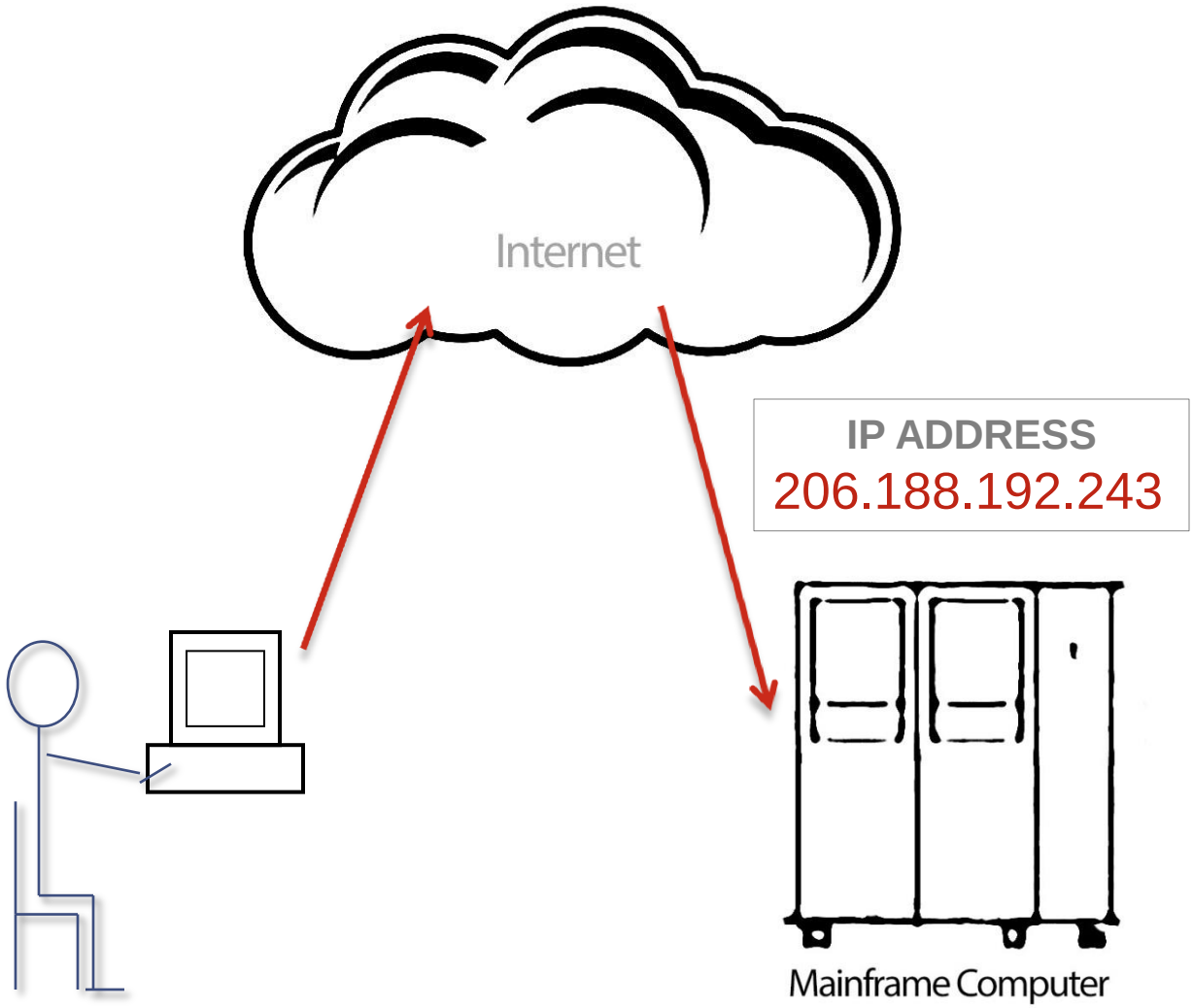
An IP Address Is

- A number like: 206.188.192.243
- Contained within each TCP/IP message
- Used to route each message to its destination computer
- Often mapped to a DNS name like www.stuhenderson.com

IP Address Routes the Message to a Computer



IP Address Routes the Message

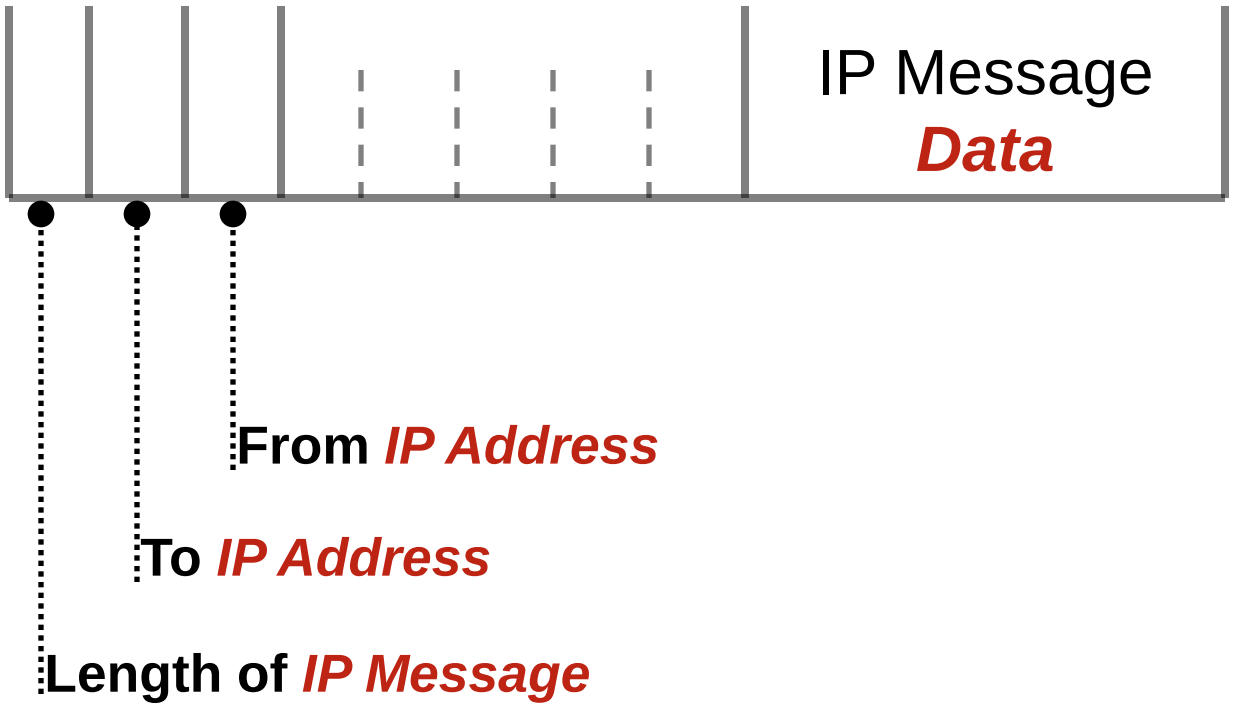


You Can't Control

The route your message takes as it is passed from computer to computer over the Internet.

Anyone in charge of any of those computers is able to view your message as it gets passed on.

IP Message Layout

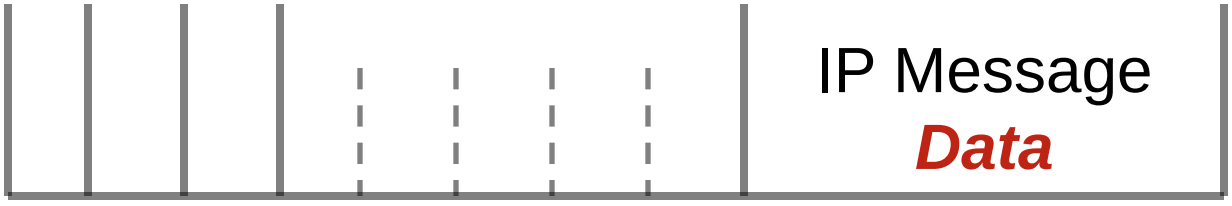


The Port Number

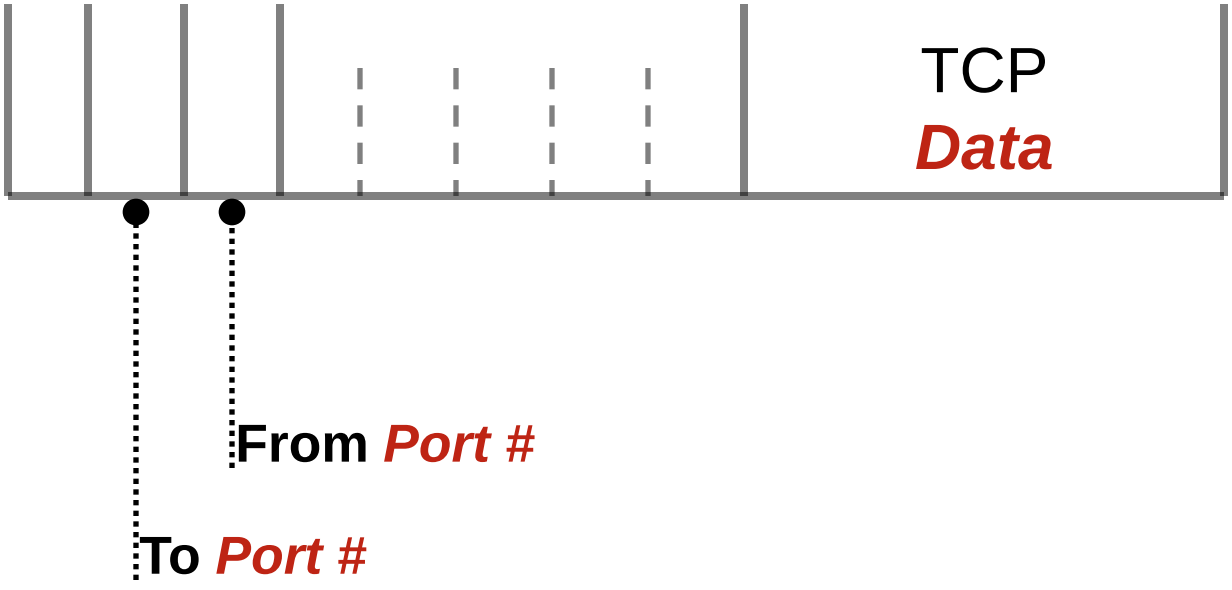
- Identifies an application like email or FTP
- Is contained in the message itself
- Is used to route the message once it arrives at its destination computer

IP Message & TCP Packet Layout

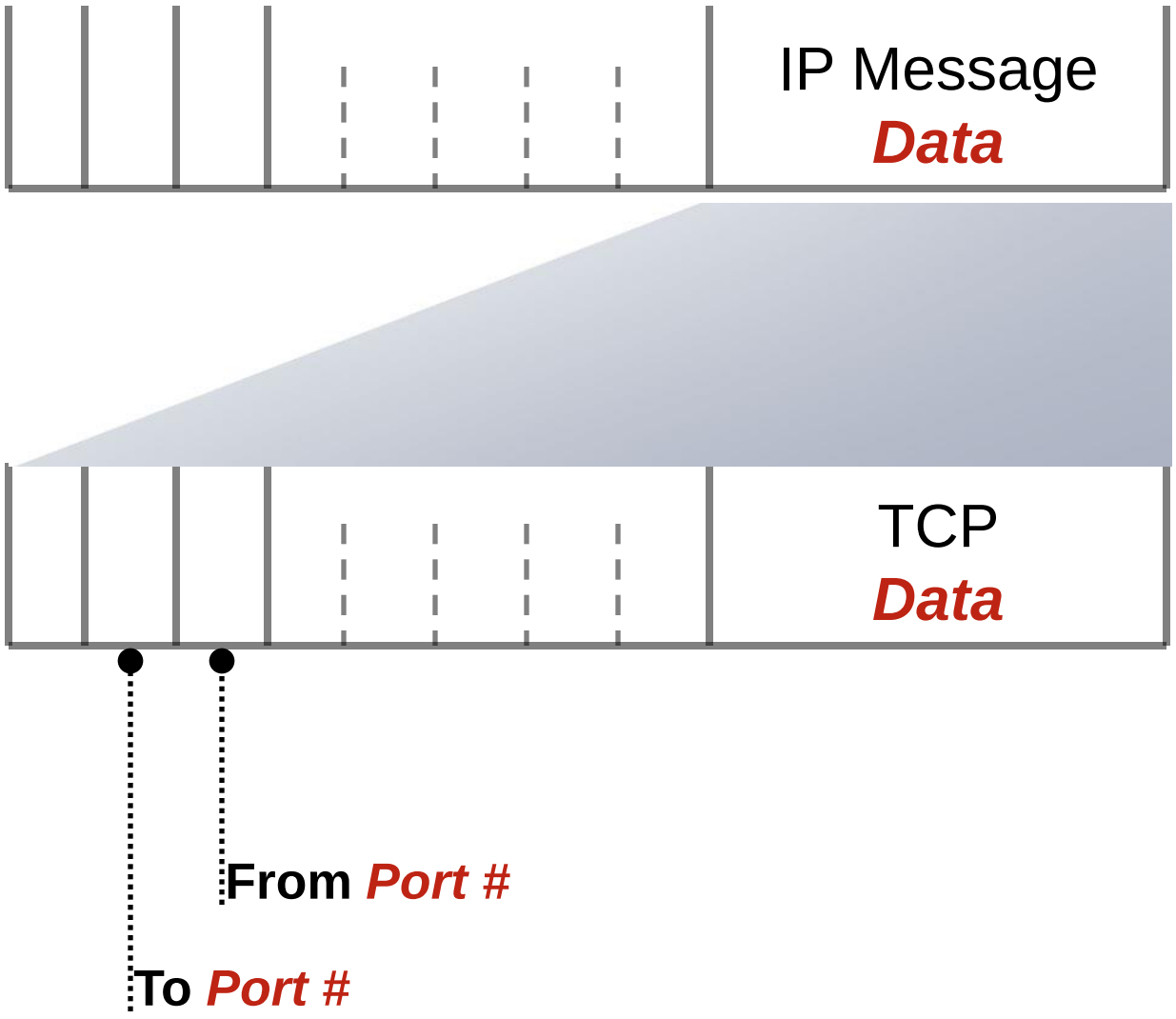
IP MESSAGE



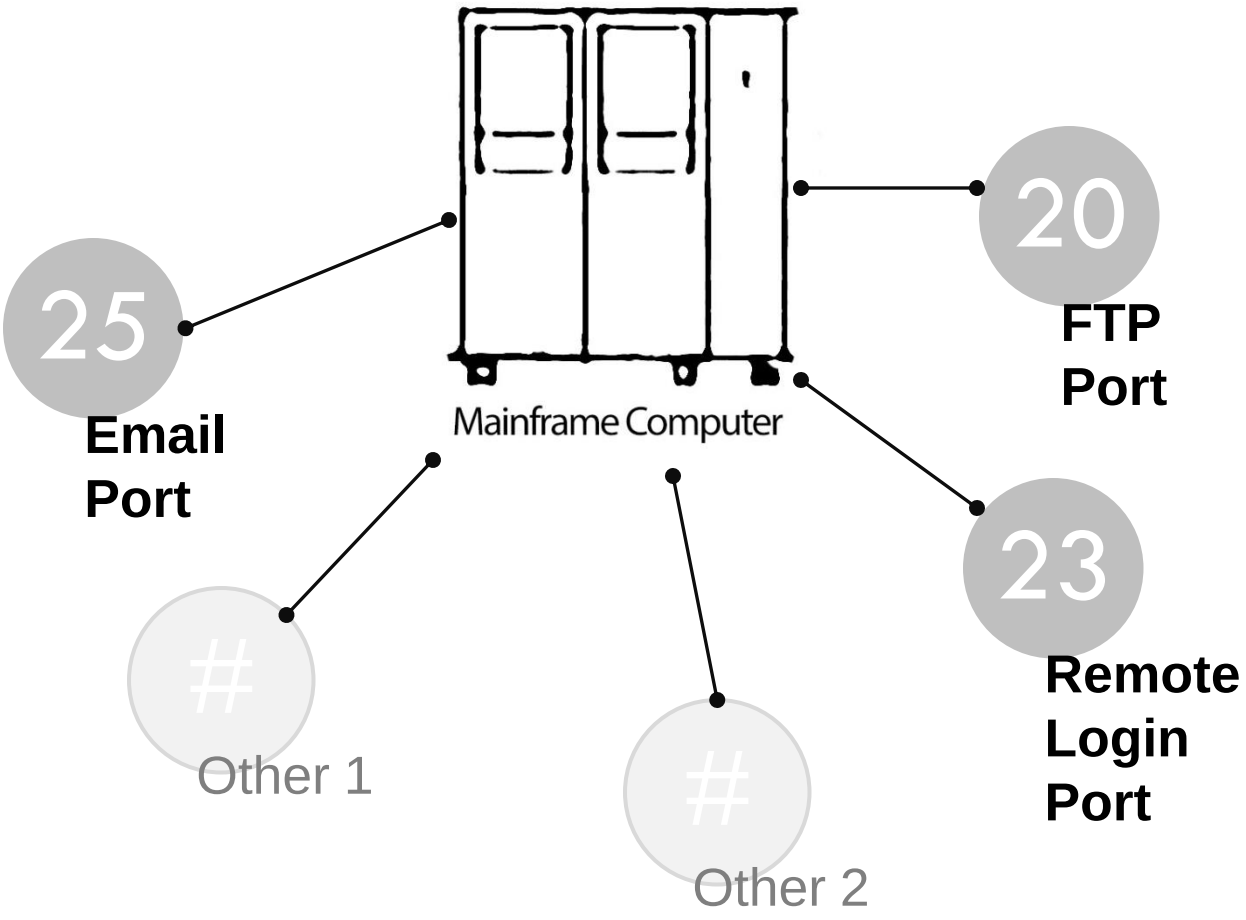
TCP PACKET



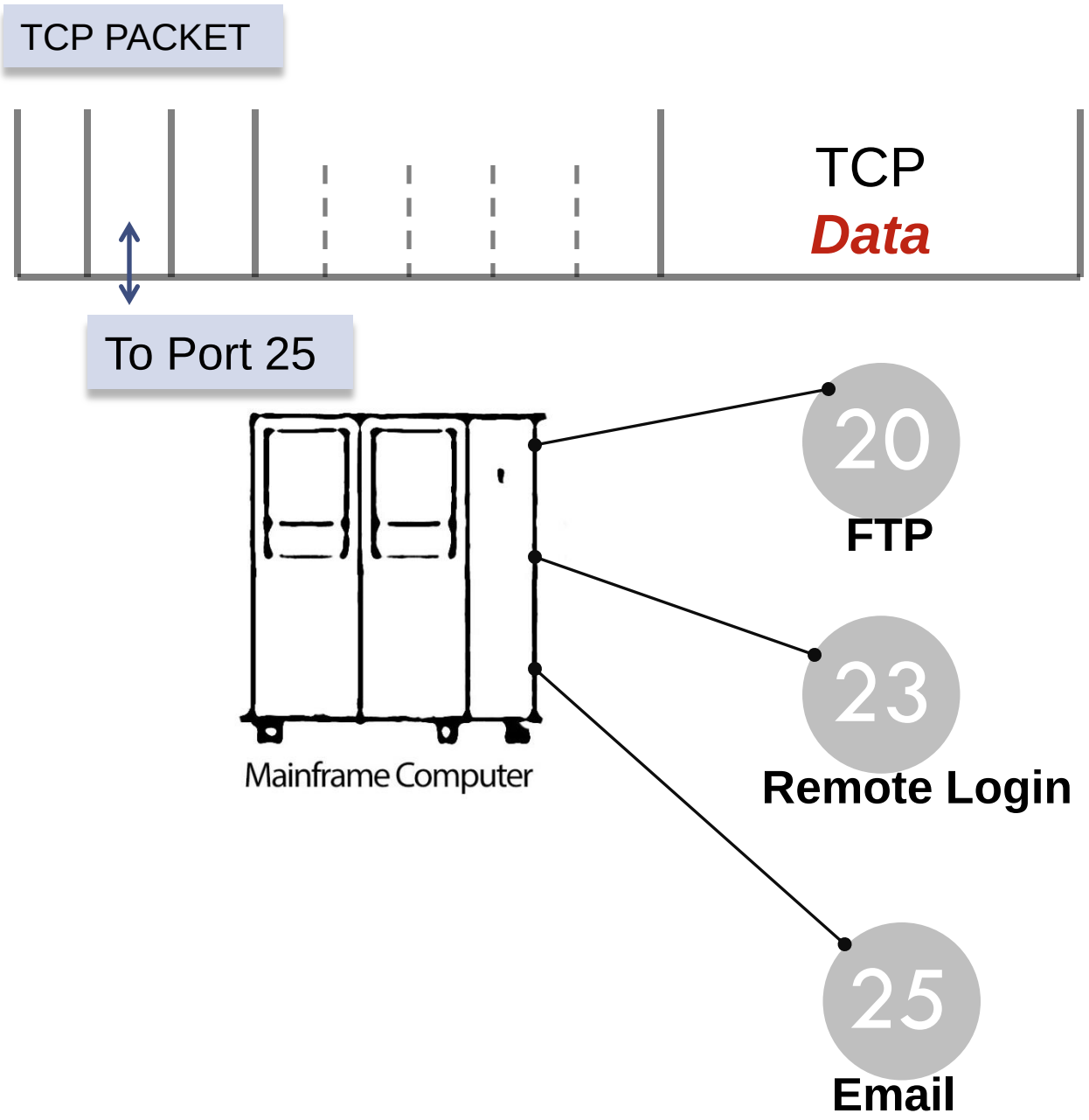
IP Message Data Contains TCP Packet Data



TCP Ports


Mainframe Computer
25
Email Port
20
FTP Port
23
Remote Login Port
#
Other 1
#
Other 2

IP Message Arrives



IP Address and DNS Name

An IP Address is a number used to route an IP message to a given computer:

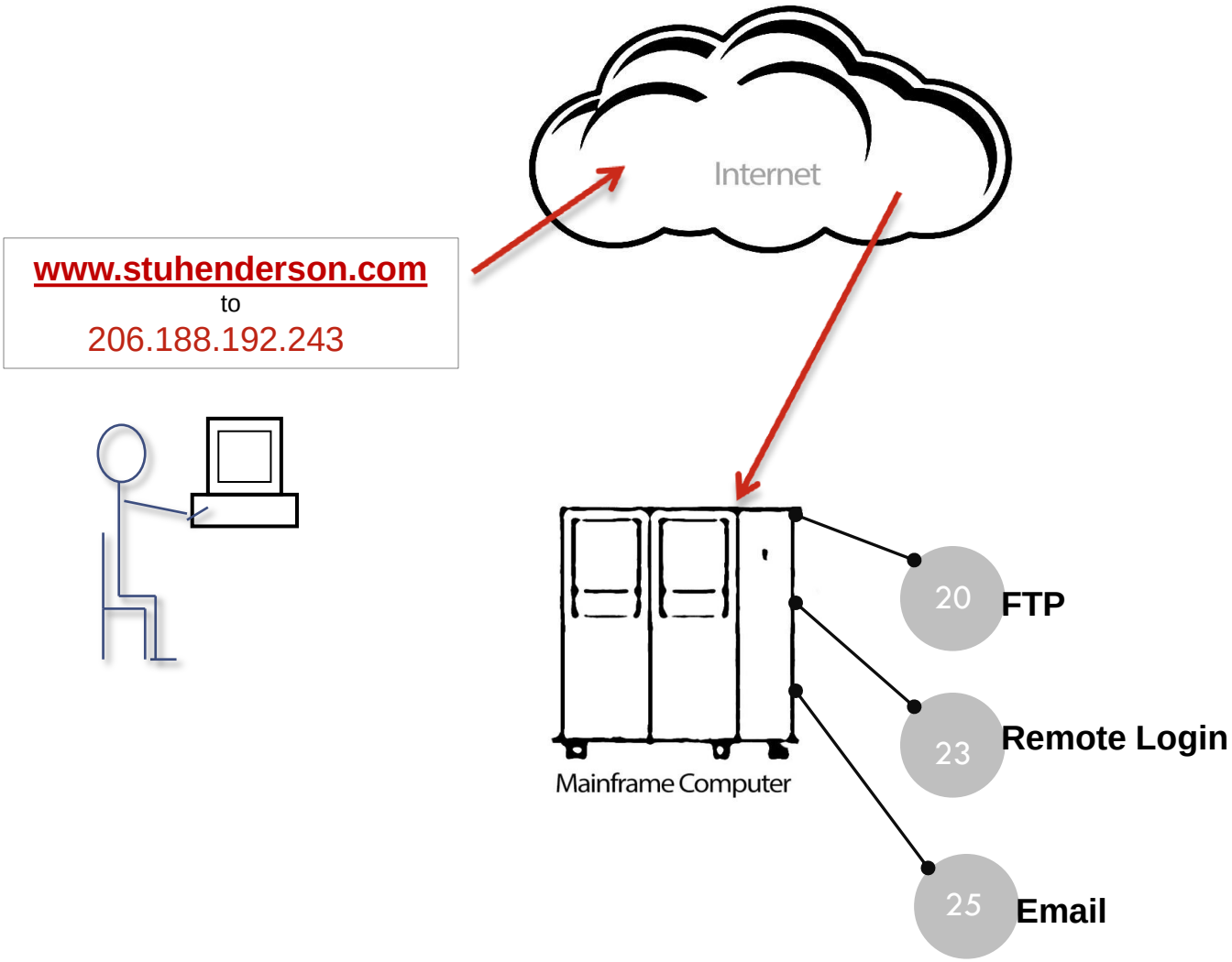
192.168.1.1

Can often be mapped to a DNS name like www.stuhenderson.com

Port Number

- Routes a message to the correct application (like email or file transfer)
- For example, port 25 is often used for email.
- Once an IP message arrives at the computer it is addressed to, TCP looks at the Port Number and hands the message to the program that handles that port number

Overall Flow



How to Learn What's Up

- The TSO command NETSTAT will tell you what TCP/IP connections are running

- Tells you:
  - To and from IP addresses
  - To and from Ports
  - Program names (such as DB2, CICS, FTP, TN3270 MQ Series)

Are Mainframes at Risk?

- Peter Hager notes a website with over 700 mainframes providing TN3270 access over the Internet.
- Every day more IP addresses are added
- More than half allow access without encryption

Is Your Mainframe Here?

- Other mainframes listed on this website enable logons with clear text connection

- (Peter's website has more info on risks of BYOD, letting users connect to your mainframe from their smartphones over TCP/IP)

2. The Risks

- Copying Sensitive Data
- Unauthorized Port Opening
- Port Scanning
- DOS (Denial of Service)
- Hijacking a Session

Copying Sensitive Data

- Passwords, PII, PCI, HIPAA…
- You can't control the route your message takes over the Internet
- Protection: Encryption

Unauthorized Port Opening

- Unauthorized program opens a port, listens for invites
- The mainframe Internet hack in Europe
- Protection: Block the Ports and Packet Filtering

Port Scanning

- Hacker maps your system by pinging every port to see what software is behind it
- Finds port backed by insecure software
- Protection: Intrusion Detection (Recognizes Patterns) and Software Quality

DOS (Denial of Service)

Two Types:

- Flood Attacks (Protection: Powerful Computer, Intrusion Detection)

- Buffer Overflow (Protection: Software Quality Assurance)

Hijacking a Session

- You can't predict the route your message takes over the Internet
- You think you're talking to the other computer, but you're actually talking to the hacker's computer.
- Protection: Encryption and Digital Certificates

3. The Protections

- Configuration Files
- SERVAUTH
- Encryption / Digital Certificates
- PAGENT (Policy Agent)

Configuration Files

- For TCP/IP itself
- For FTP, Policy Agent, others
- Provide for:
  - Blocking of ports
  - SERVAUTH calls
  - Encryption
  - Client authentication
  - Intrusion detection

SERVAUTH

- Resource Class with RACF, ACF2, TopSecret
- Restricts access to:
  - Ports and IP addresses
  - FTP
  - TCP/IP itself
  - TN3270
  - Other
- Specified in configuration files

Encryption / Digital Certificates

- SSL / TLS application transparent (Any application can invoke it based on configuration file)
- Protects Data, Also: Client Authentication, Non-Repudiation
- Digital Certificates should be in RACF, ACF2, TopSecret

PAGENT (Policy Agent)

- A Firewall For the Mainframe
- Free with z/OS

PAGENT Functions

- IPSEC (Port Blocking and VPN)
- Encryption
- Intrusion Detection
- Packet Filtering

4. Summary: Call to Action

- Use TSO NETSTAT to learn what is running
- Is PAGENT running?
- What else is running?

4. Summary: Call to Action

Review configuration files:

- DB2: DSNZPARM
- CICS: DFHSIT, TCPIPSERVICE
- TCP/IP: PROFILE, TCPDATA
- FTP: FTPDATA
- TN3270 same as TCP/IP
- …

- Change control on configuration files (NewEra's Image Focus and The Control Editor)

4. Summary: Call to Action

- Who decides what data to encrypt?
- How do they decide?
- What knowledge is relevant?

4. Summary: Call to Action

- Review Policy Agent configuration file
- It points to other configuration files for specific functions
- Which functions do you want?

4. Summary: Call to Action

- Review port control
- How do you block the ports?
- Who decides?

4. Summary: Call to Action

- Watch red flags for auditors:
  - No baseline documents
  - DSO doesn't know how TCP/IP is secured
  - No encryption over passwords
  - No change control
  - No risk assessment
  - Not using PAGENT
  - Digital certificates not in RACF, ACF2, TopSecret

4. Summary: Call to Action

- Review the risks listed above
- Use the tools listed above to manage the risks
- Ensure change control
- Clarify who is responsible, who has authority

For More Information

- ACF2, TopSecret Manuals from CA Technologies
- RACF and z/OS Communications Server Manuals (www.ibm.com/servers/eserver/zseries/zos/bkserv/)
- Articles on FTP Security and SERVAUTH and Other Topics at www.stuhenderson.com/XARTSTXT.HTM

For More Information

- ***Mainframe Audit News*** and ***RACF User News*** at www.stuhenderson.com/Newsletters-Archive.html

- Website listing mainframes accessible over the Internet http://mainframesproject.tumblr.com/

For More Information

- Peter Hager's website (BYOD and mainframe TCPIP) www.net-q.com
- NewEra's website (change control tools for configuration files) www.newera.com

Thanks for Your Kind Attention.

Questions to Stu Henderson

(301) 229-7187 stu@stuhenderson.com