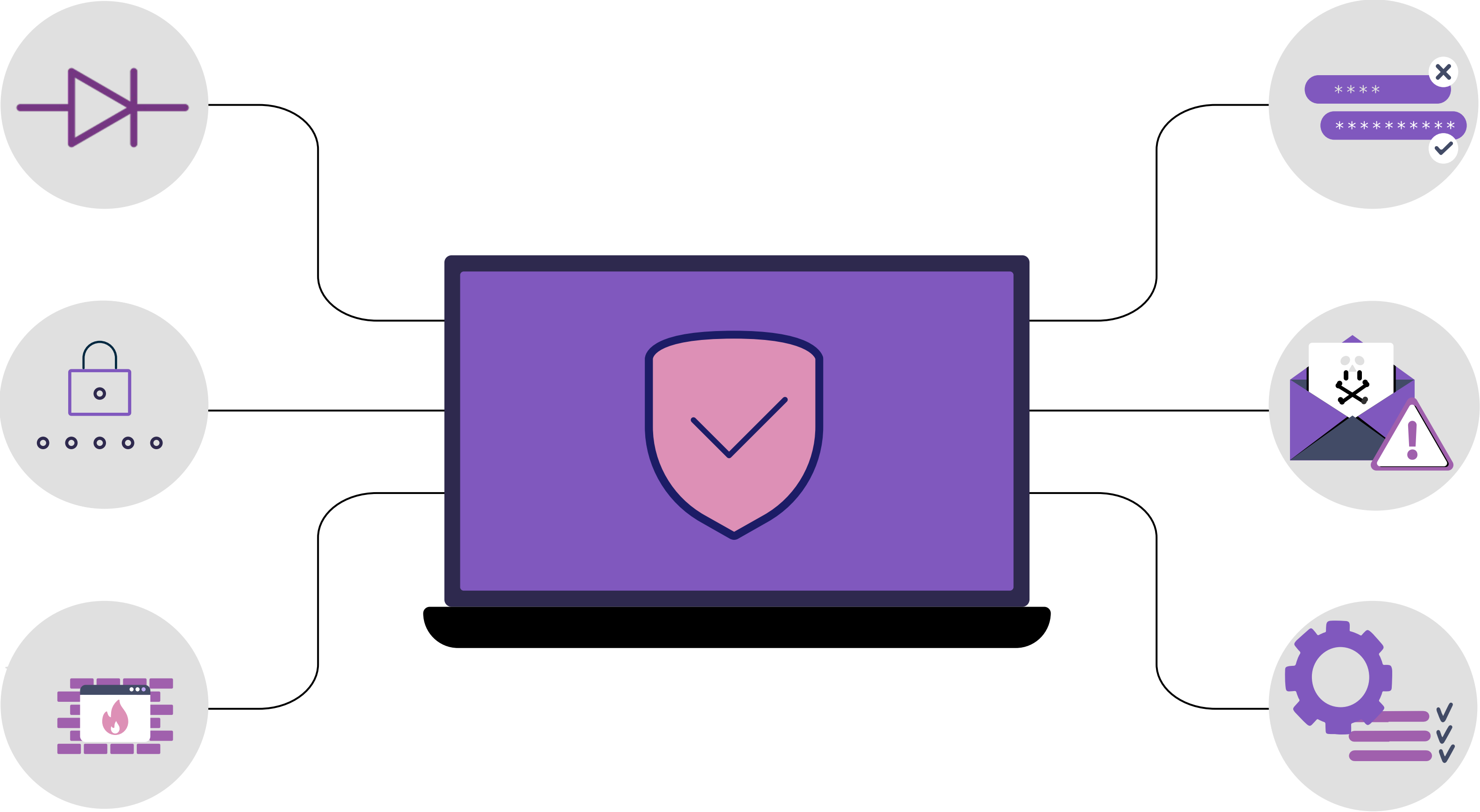
Data Diode

Al-Majd Zunquti & Yifan Zhao

DSCI519 - Foundations and Policy for Information Security | Dr. Tatyana Ryutov | Nov 9, 2022

Agenda



What

What is data diode

How

How does it work

Firewall

Compare it with firewall

Reference monitor

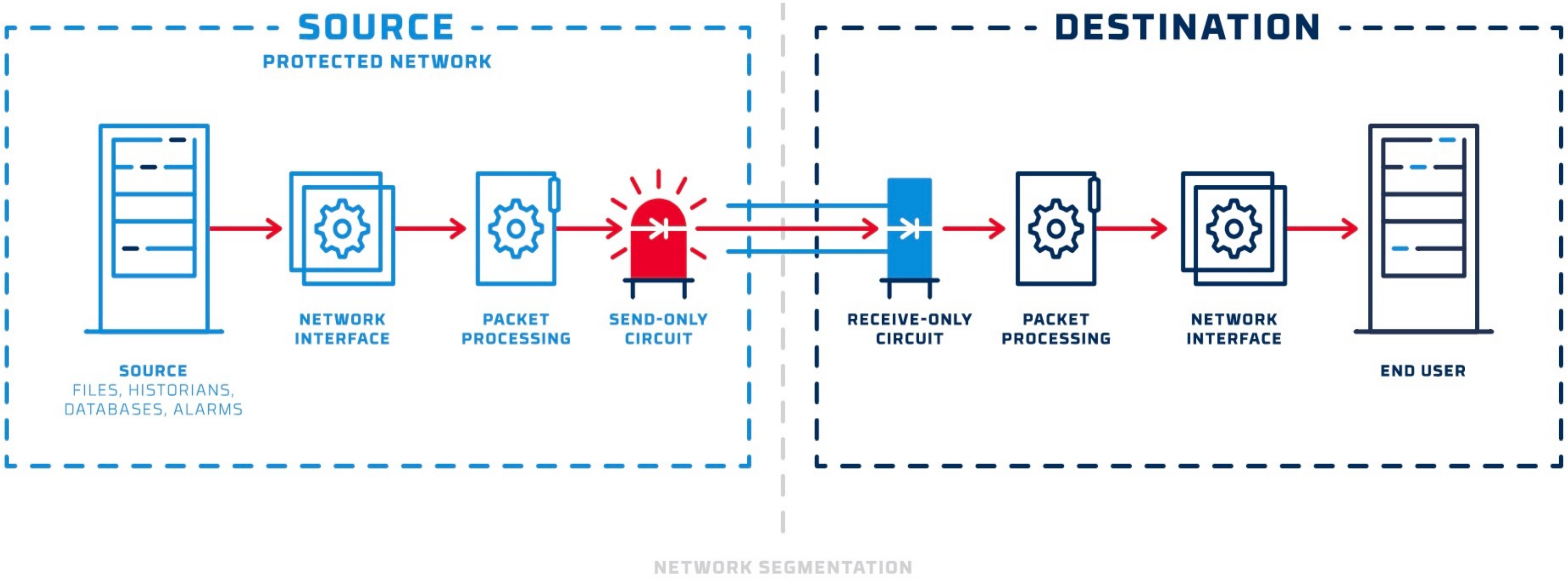
Limitations

Solutions

What is Data Diode?

- Data diode is a kind of one-way network communication device
- Data diode design maintains the physical separation of the source and destination networks
- Data diode effectively eliminates external entry points to the transmitting system

- Protect the security of network infrastructure and reduce potential losses



Implementing rules:

Only allowing incoming data

Only allowing outgoing data

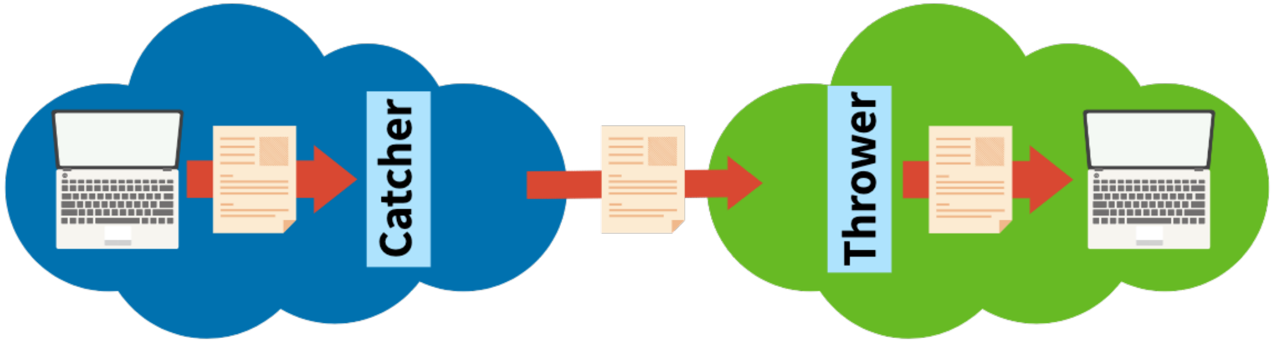
How does it work

- Data diode allows information to flow securely in only one direction to prevent data leakage and eliminate the threat of malware.
- Data diode creates a physical barrier between the two points, and agents in its network interface send data through "protocol interrupts."

The operation mode of the data diode:

- Receive-only
- Transmit-only

- System A agent: "Catcher"
- System B agent: "Thrower"
- System A sends data to Catcher
- Catcher send data to system B
- System B receives data through the Thrower

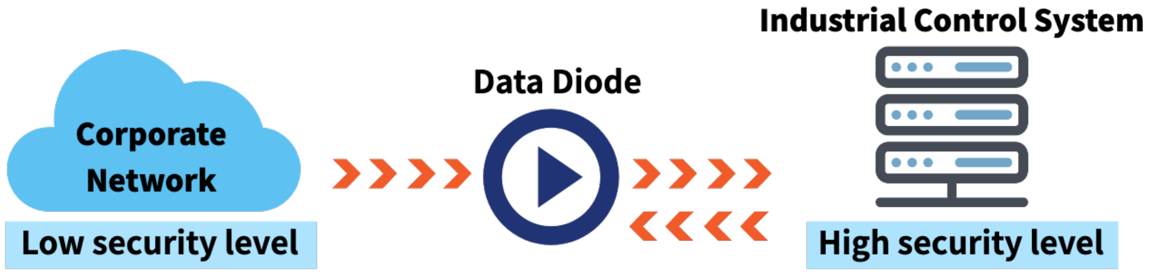


How does it work

Receive-Only(Confidentiality)

Security level:
Corporate Network: Low
Industrial Control System: High

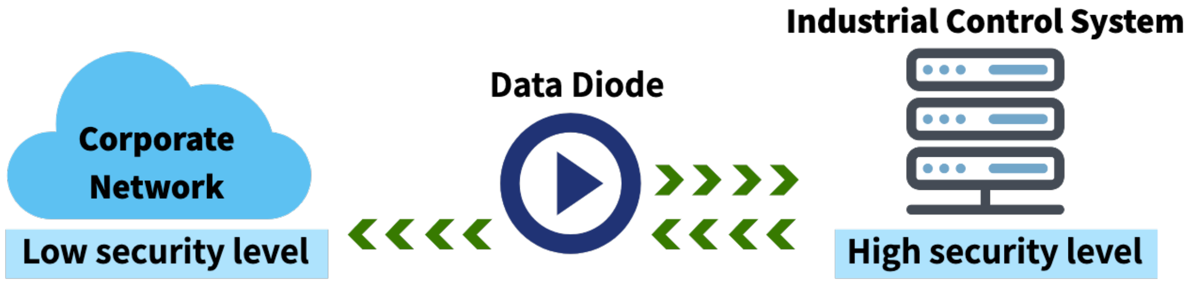
Only allow data to flow from corporate networks to industrial control systems.



Transmit-only(Integrity)

Security level:
Corporate Network: High
Industrial Control System: Low

Only allow data to flow from industrial control systems to corporate networks.



How to build it?

Advantages:

- Higher security
- No delays are introduced
- Low long-term operating costs

Creating a Bidirectional Network

- Create a bi-directional network connection using data diodes based on two optical fibers

Disconnect the RX

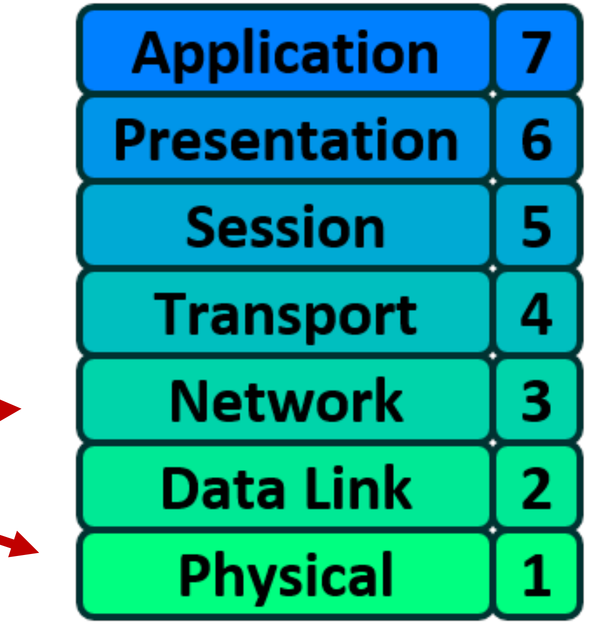
- Disconnect the fiber representing the (RX) function

Physical Layer implementation

- Using a third-party media converter

Network layer implementation

- Create static ARP entries on the switch and endpoints

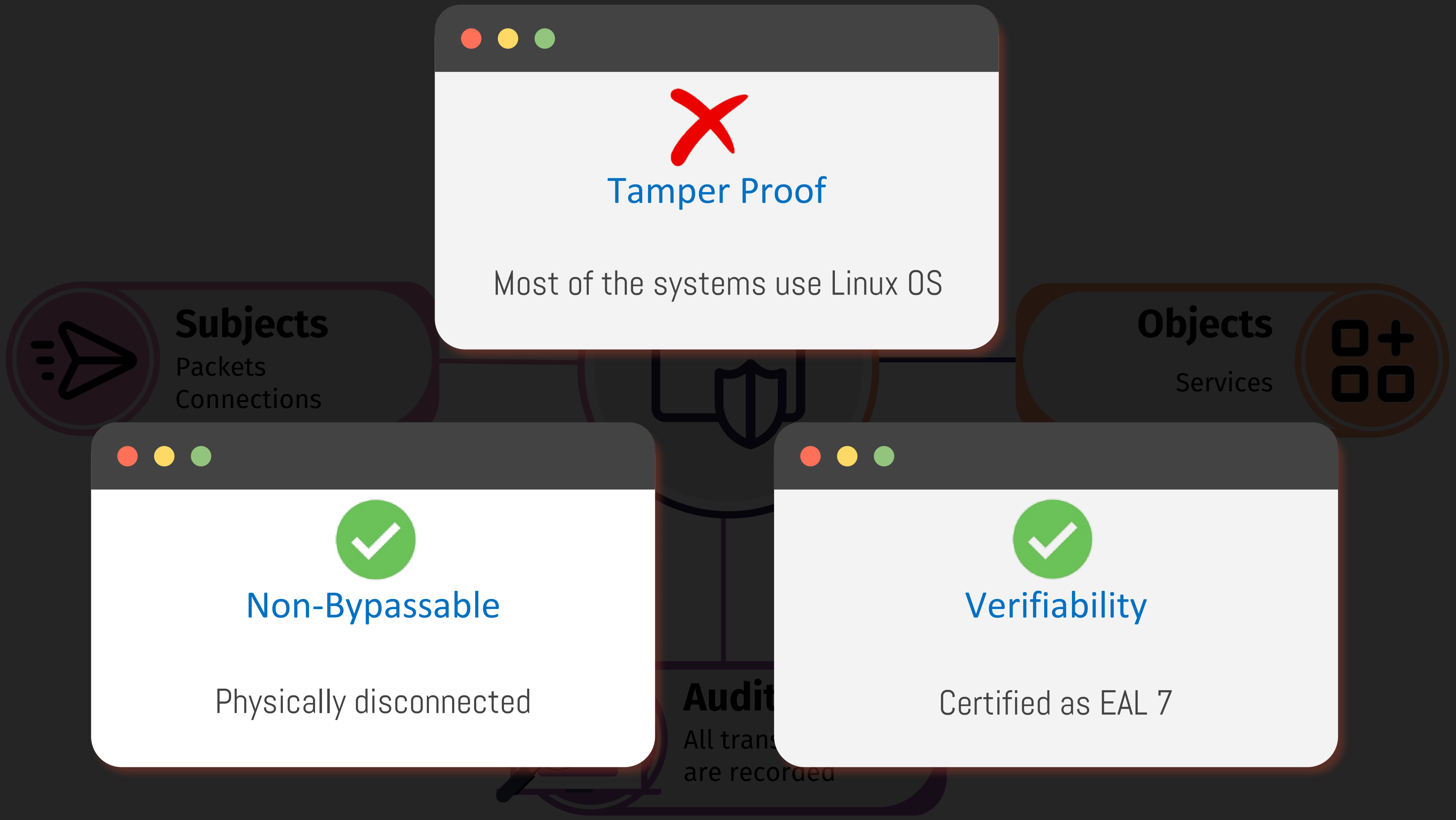


Application 7
Presentation 6
Session 5
Transport 4
Network 3
Data Link 2
Physical 1

Compare it with firewall

Firewall	VS	Data Diode
Software-Enforced (Configured) • Misconfigurations • Backdoors • Vulnerabilities	**Enforcement Mechanism**	Hardware-Enforced (Physical)
One-Way or Two-Way • Most attacks designed with two-way	**Connection**	One-Way
Varies (Based on Rules)	**Latency**	Low
Very High	**Reliability & Assurance**	Very High

Compare it with reference monitor



✗ **Tamper Proof**

Most of the systems use Linux OS

✓ **Non-Bypassable**

Physically disconnected

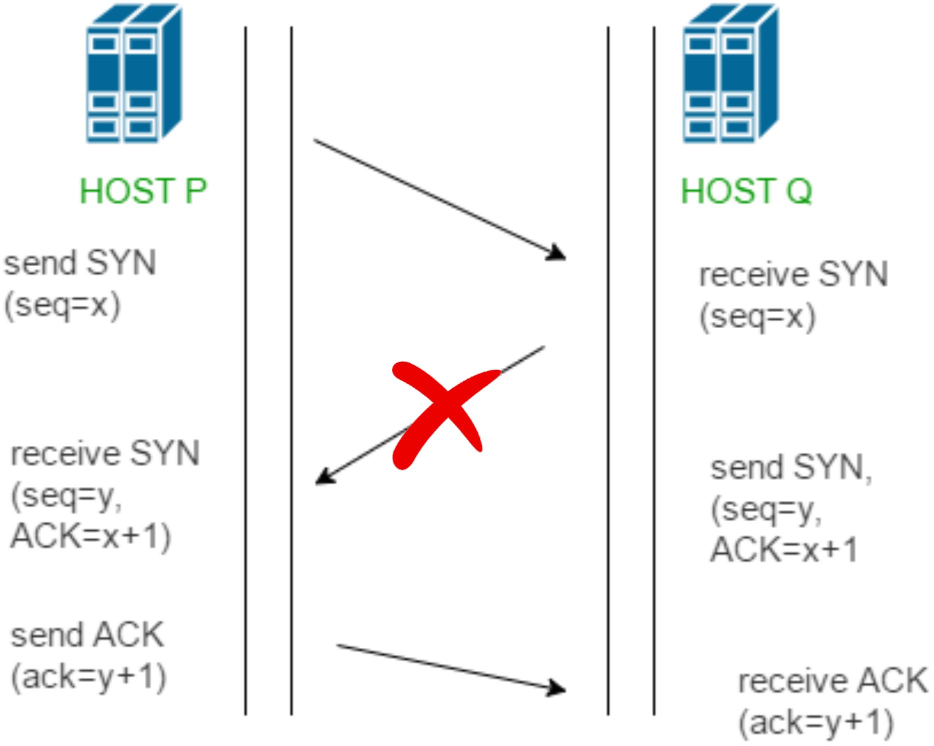
✓ **Verifiability**

Certified as EAL 7

Limitations

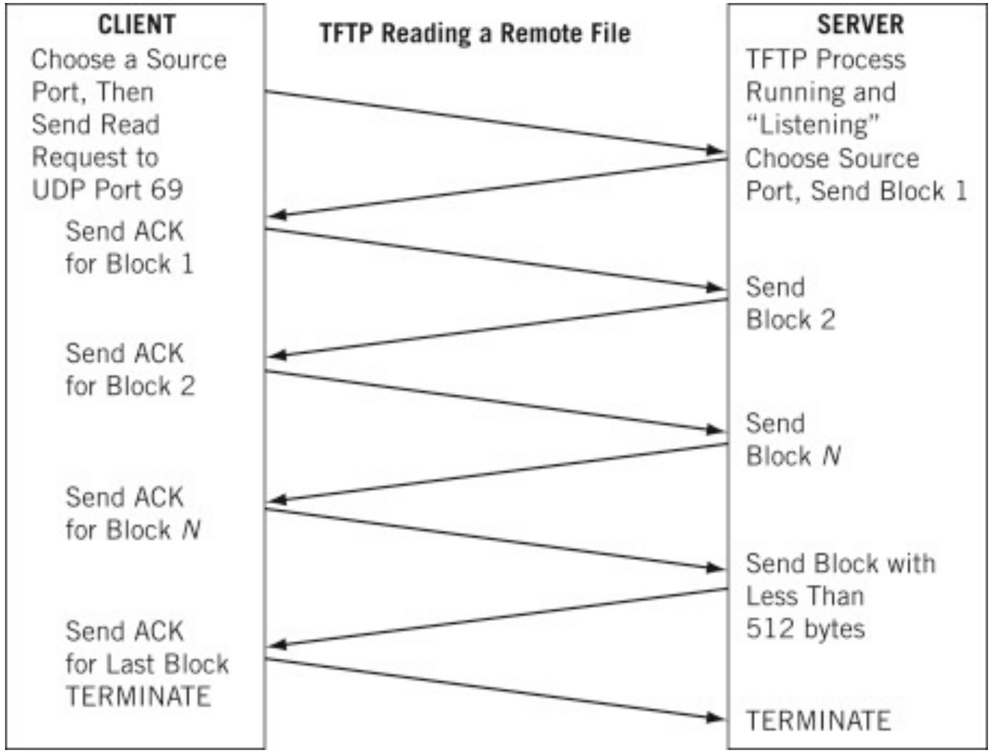
1 Most of protocols use two-way communication

2 Doesn't provide high data reliability or integrity



Solutions

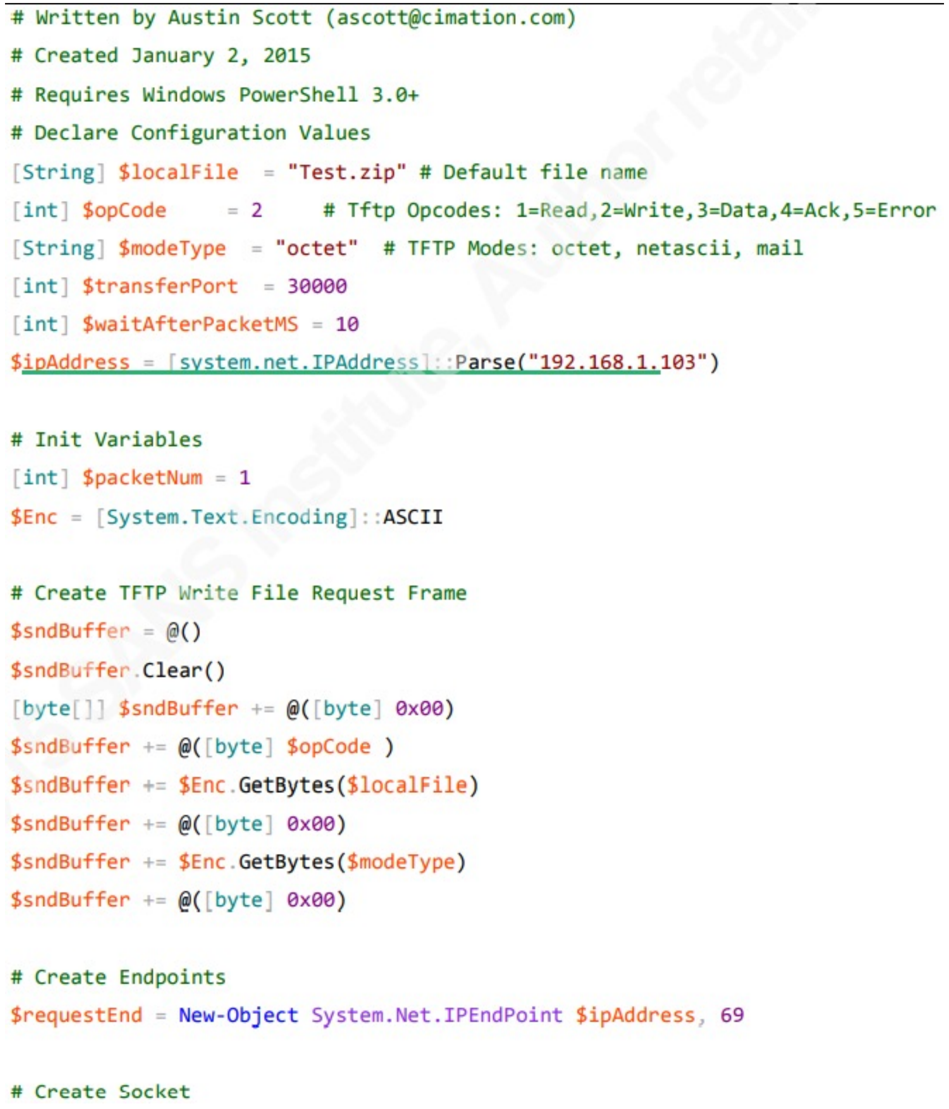
Enabling two-way	**Create a software proxy gateway** • Complex • Lack of approval
Other Protocol	**Using TFTP** • Capable of sending ASCII and Binary files (without authentication) • Uses UDP


CLIENT
TFTP Reading a Remote File
SERVER
Choose a Source Port, Then Send Read Request to UDP Port 69
TFTP Process Running and "Listening" Choose Source Port, Send Block 1
Send ACK for Block 1
Send Block 2
Send ACK for Block 2
Send Block N
Send ACK for Block N
Send Block with Less Than 512 bytes
Send ACK for Last Block TERMINATE
TERMINATE

Solutions

1 Disable Acknowledge packet

2 Wait for ten milliseconds between sending each packet



```
# Written by Austin Scott (ascott@cimation.com)
# Created January 2, 2015
# Requires Windows PowerShell 3.0+
# Declare Configuration Values
[String] $localFile   = "Test.zip" # Default file name
[int] $opCode       = 2      # Tftp Opcodes: 1=Read,2=Write,3=Data,4=Ack,5=Error
[String] $modeType   = "octet"  # TFTP Modes: octet, netascii, mail
[int] $transferPort   = 30000
[int] $waitAfterPacketMS = 10
$ipAddress = [system.net.IPAddress]::Parse("192.168.1.103")

# Init Variables
[int] $packetNum = 1
$Enc = [System.Text.Encoding]::ASCII

# Create TFTP Write File Request Frame
$sndBuffer = @()
$sndBuffer.Clear()
[byte[]] $sndBuffer += @([byte] 0x00)
$sndBuffer += @([byte] $opCode )
$sndBuffer += $Enc.GetBytes($localFile)
$sndBuffer += @([byte] 0x00)
$sndBuffer += $Enc.GetBytes($modeType)
$sndBuffer += @([byte] 0x00)

# Create Endpoints
$requestEnd = New-Object System.Net.IPEndPoint $ipAddress, 69

# Create Socket
```

References

[1] U. P. D. Ani, H. (. He and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective," *Cyber Security Technology ,* vol. 1, no. 1, pp. 32-74, 2016.

[2] A. Scott, "Tactical Data Diodes in Industrial Automation and Control Systems," 30 June 2015. [Online]. Available: https://sansorg.egnyte.com/dl/jcw5vWs4Df. [Accessed 1 November 2022].

[3] B.-S. Jeon and J.-C. Na, "A study of cyber security policy in industrial control system using data diodes," in *18th International Conference on Advanced Communication Technology (ICACT)*, Pyeongchang, 2016.

[4] N. Mead, "The Common Criteria," Cybersecurity & infrastructure security agency, 10 August 2006. [Online]. Available: https://www.cisa.gov/uscert/bsi/articles/best-practices/requirements-engineering/the-common-criteria. [Accessed 1 November 2022].

[5] B. Systems, "INTERACTIVE LINK DATA DIODE SYSTEM," 2014. [Online]. Available: https://cds.au.baesystems.com/docs/default-source/resources/brochures/bae-systems-interactive-link-brochure. [Accessed 1 November 2022].

Thank you!