



**WATERFALL**®  
*One Way to Connect*

FROST & SULLIVAN

2012 BEST PRACTICES AWARD

NORTH AMERICAN NETWORK SECURITY  
FOR INDUSTRIAL CONTROL SYSTEMS  
ENTREPRENEURIAL COMPANY OF THE YEAR AWARD

*One Way to*

*One Way to Connect*

*Industrial Control Systems Joint Working Group – 2012 Fall Meeting*

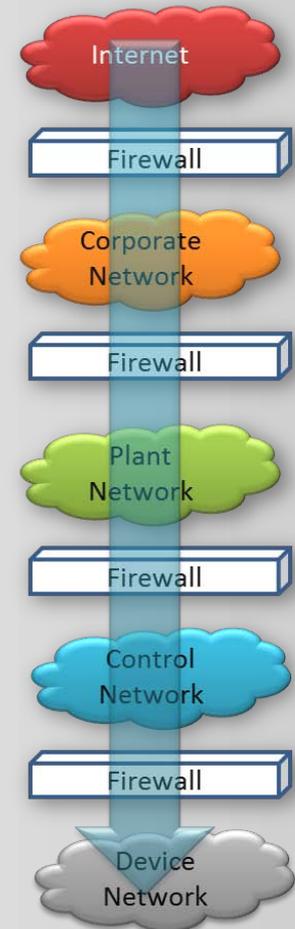
# 13 Ways Through A Firewall

Andrew Ginter  
Director of Industrial Security  
Waterfall Security Solutions



# Firewalls

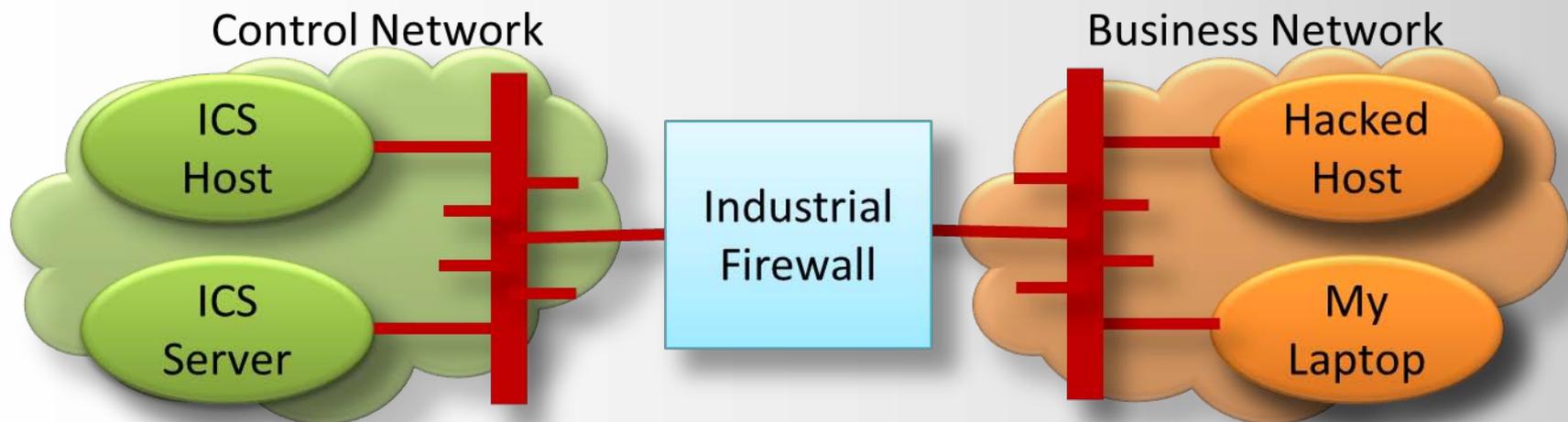
- Firewalls – separate networks and sub-networks with different security / connectivity needs
- Often first investment any site makes when starting down the road to an ICS cyber security program
- “Unified Threat Managers” – firewalls with stateful inspection, VPNs, in-line anti-virus scanning, intrusion detection, intrusion prevention, anti-spam, web filtering, and much more – but are they secure?
- DMZ – “in-between” network(s)
- ICS best practice: layers of firewalls, layers of host and network-based defenses





## Setup for Demo Scenarios

- Industrial firewall / UTM
- Business network – my laptop + “hacked host” virtual machine
- Control network – ICS server to attack / take over + one other ICS host virtual machine
- 2x virtual switches – one for each network, each connected to firewall
- Consider only one-hop compromise – into DMZ, or into ICS from DMZ





## Compensating Measures

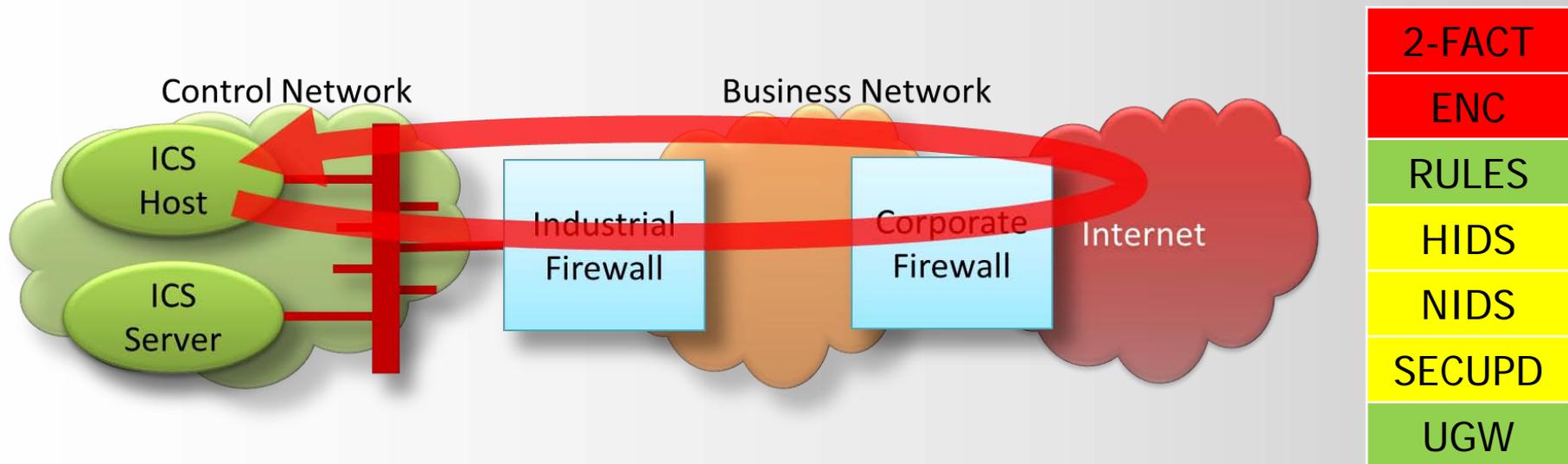
Abbrev	Compensating Measure
2-FACT	2-Factor authentication
ENC	Encryption
RULES	Better firewall rules
HIDS	Host intrusion detection / prevention system / SIEM
NIDS	Network intrusion detection / prevention system / SIEM
SECUPD	Security updates / patch program
UGW	Unidirectional security gateway

Graphic	Impact
	Would have prevented / detected the attack
	Would prevent / detect some variants of the attack
	Would not have prevented / detected the attack



## #1 Phishing / Spam / Drive-By-Download

- Single most common way through (enterprise) firewalls
- Client on business network pulls malware from internet, or activates malware in email attachment
- “Spear-phishing” – carefully crafted email to fool even security experts into opening attachment





## #2 Social Engineering – Steal a Password

- VPN password on sticky note on monitor, or under keyboard
- Call up administrator, weave a convincing tale of woe, and ask for the password
- Or ask the administrator to give you a VPN account
- Shoulder-surf while administrator enters firewall password
- Guess
- Install a keystroke logger



2-FACT

ENC

RULES

HIDS

NIDS

SECUPD

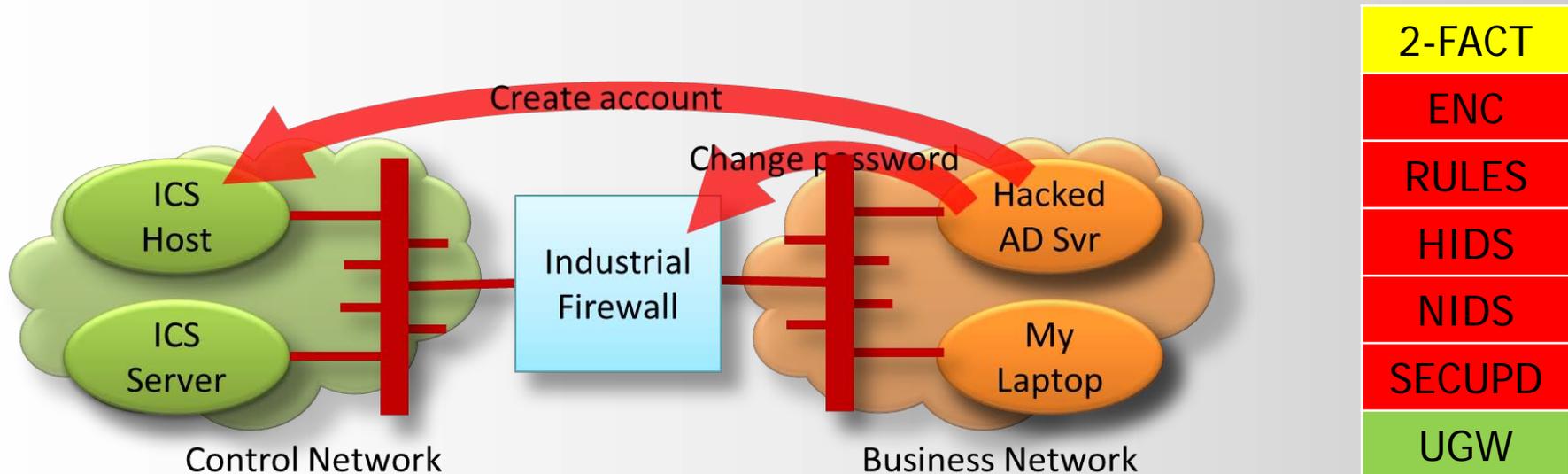
UGW





## #3 Compromise Domain Controller – Create Account

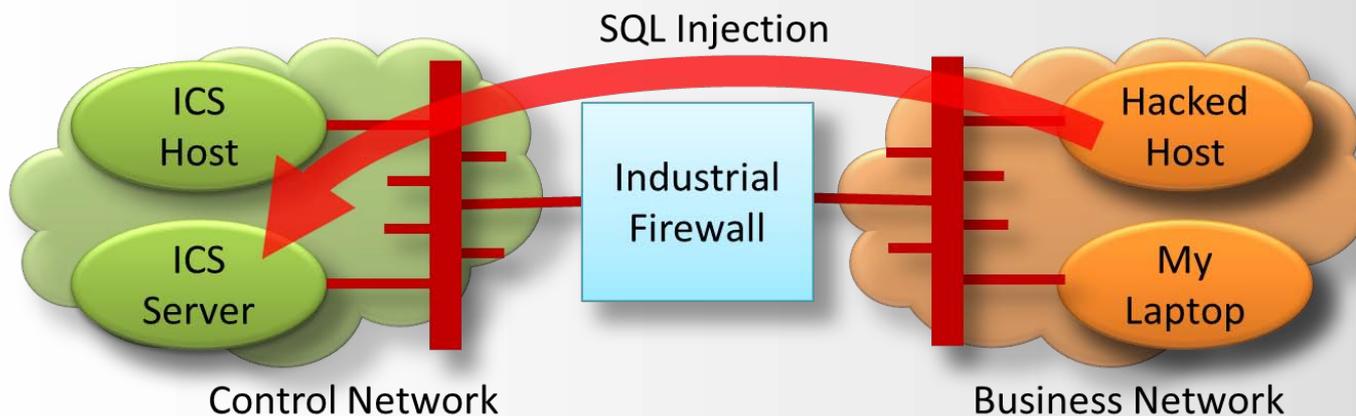
- More generally – abuse trust of external system
- Create account / change password of exposed ICS server, or firewall itself
- Other external trust abuse – compromise external HMI, ERP, DCS vendor with remote access, WSUS server, DNS server, etc.





## #4 Attack Exposed Servers

- Every exposed port is vulnerable – eg: SQL injection, buffer overflow, default passwords, hard-coded password, denial of service / SYN-flood, stored procedure injection
- 100,000 vulnerabilities: 2% x 50,000 calls x 10 vendors x 5 verticals x 3 products x 75%

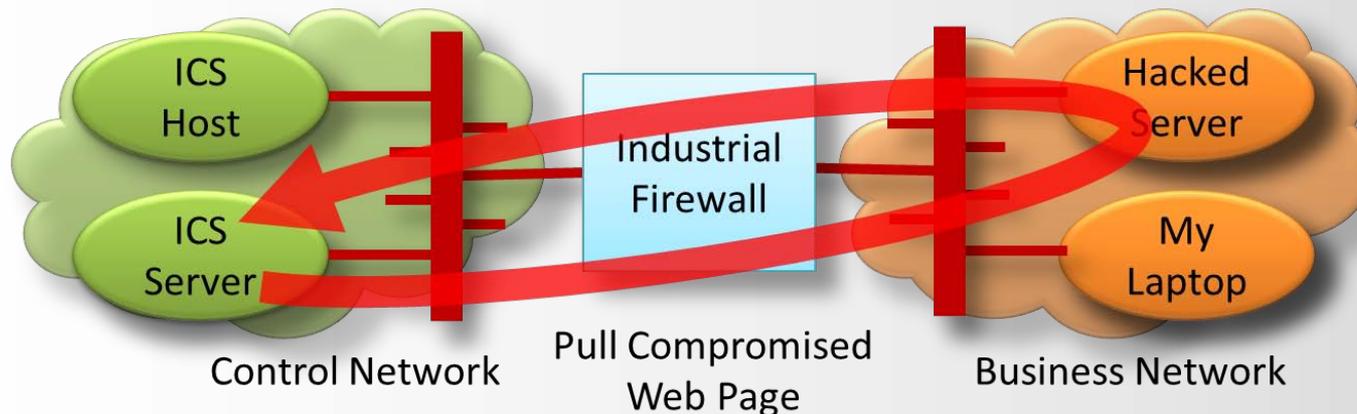


2-FACT
ENC
RULES
HIDS
NIDS
SECUPD
UGW



## #5 Attack ICS Clients via Compromised Servers

- Best practice: originate all cross-firewall TCP connections on ICS / trusted side
- Once established, all TCP connections are bi-directional – attacks can flow back to clients: compromised web servers, compromised files on file servers, buffer overflows
- 100,000 vulnerabilities

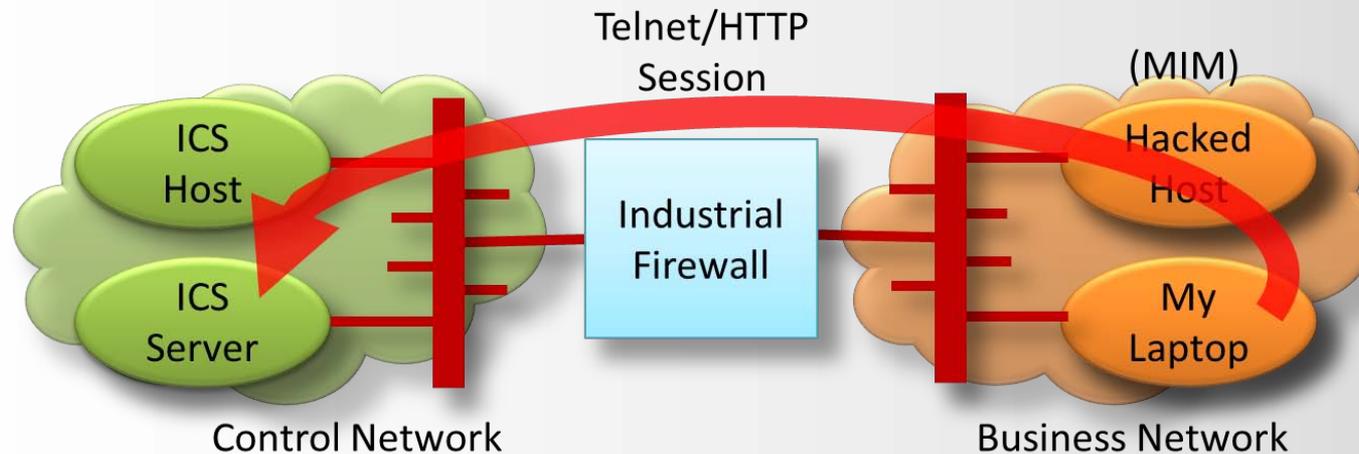


2-FACT
ENC
RULES
HIDS
NIDS
SECUPD
UGW



## #6 Session Hijacking / Man-in-the-Middle

- Requires access to communications stream between authorized endpoints – eg: ARPspooF (LAN), fake Wi-Fi access point, hacked DNS server
- Insert new commands into existing communications session
- Sniff / fake session ID / cookie and re-use



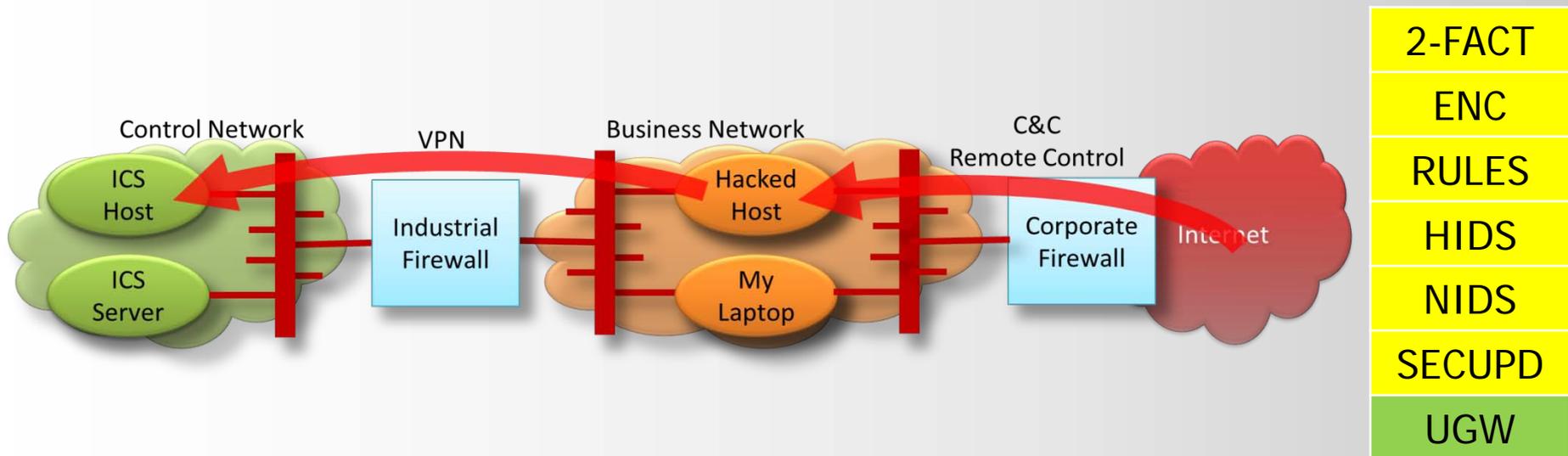
2-FACT
ENC
RULES
HIDS
NIDS
SECUPD
UGW





## #7 Piggy-Back on VPN

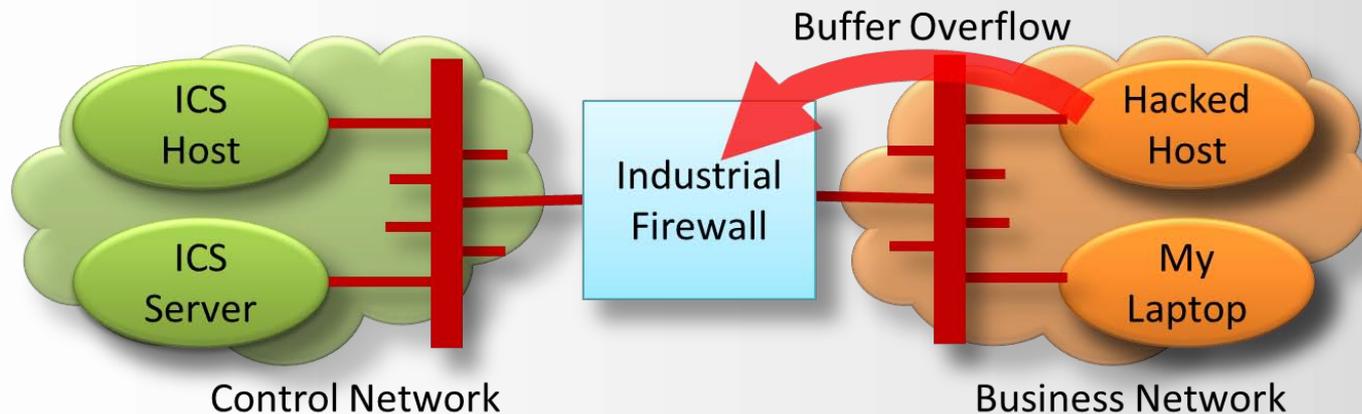
- You may trust the person you have granted remote access, but should you trust their computer?
- Broad VPN access rules – “I trust this user to connect to any machine, on any port” makes it easy for worms and viruses to jump
- Split-tunneling allows interactive remote control





## #8 Firewall Vulnerabilities

- Firewalls are software. All large software artifacts have bugs, and some of those bugs are security vulnerabilities
- Vendor back-doors / hard-coded passwords
- Supply chain issues – do you trust the manufacturer? The manufacturer's suppliers?
- Occasional design vulnerabilities



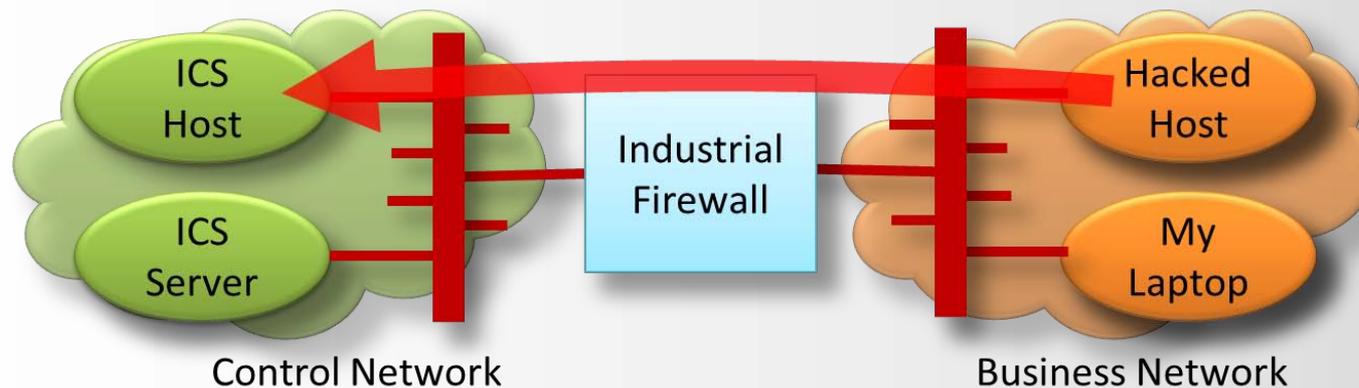
2-FACT
ENC
RULES
HIDS
NIDS
SECUPD
UGW





## #9 Errors and Omissions

- Modern firewalls require 6-8 weeks full-time training to cover all features and all configurations
- The smallest error exposes protected servers to attack
- Over time, poorly-managed firewalls increasingly resemble routers
- Well-meaning corporate IT personnel often control firewall configurations and can reach through to “fix” ICS hosts



2-FACT

ENC

RULES

HIDS

NIDS

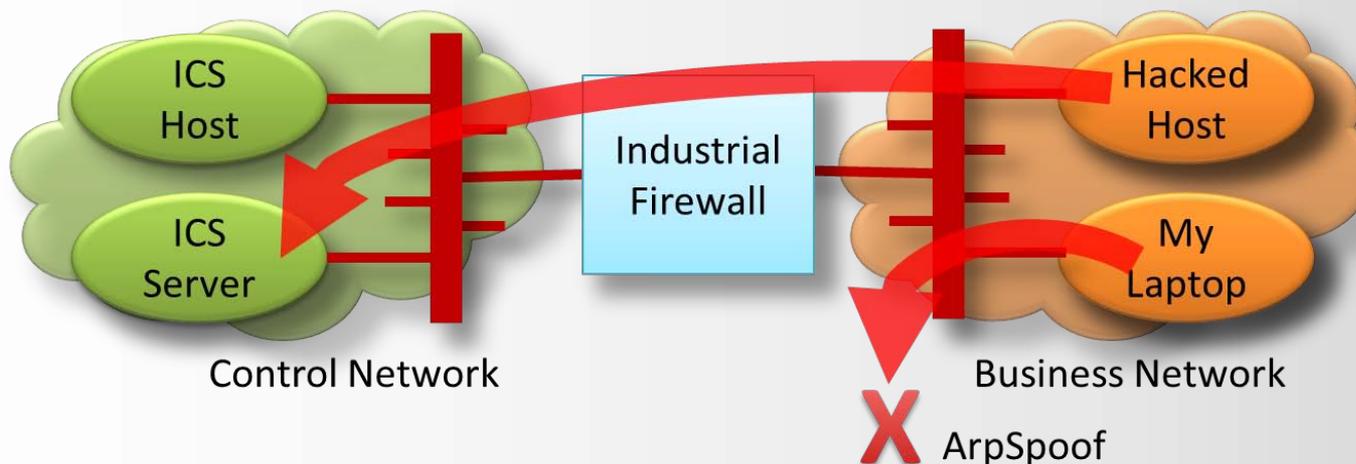
SECUPD

UGW



## #10 Forge an IP Address

- Most firewall rules are expressed in terms of IP addresses
- Any administrator can change the IP address on a laptop or workstation
- Works only if attacker is on same LAN segment as true IP address – or WAN routers route response traffic to a different LAN
- May need ARPSpoof to block machine with real IP

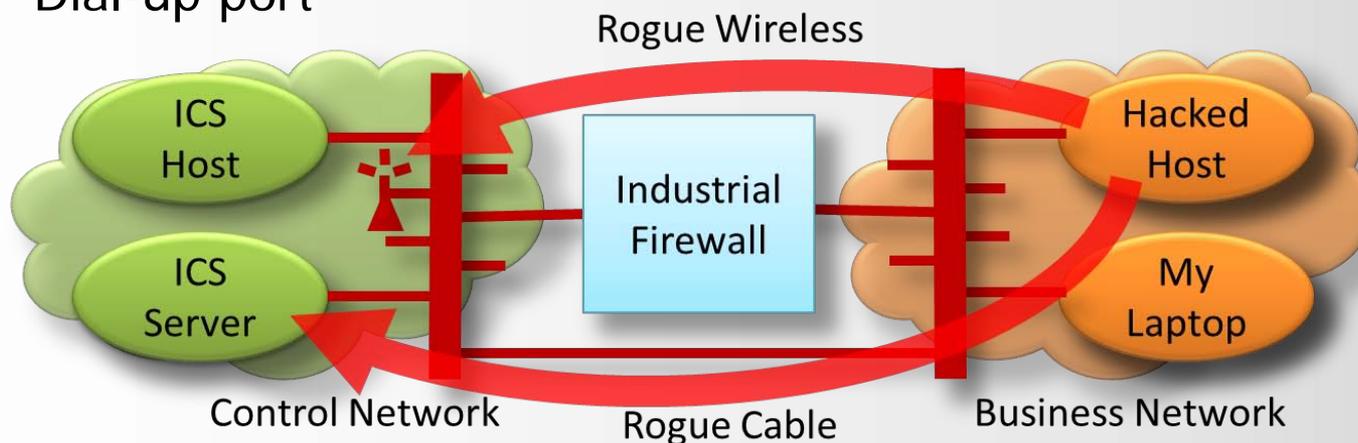


2-FACT
ENC
<b>RULES</b>
HIDS
NIDS
SECUPD
UGW



## #11 Bypass Network Security Perimeter

- Complex network architectures – path from business network to ICS network through only routers exists, but is not obvious
- Rogue wireless access points
- Rogue cables – well meaning technicians eliminate “single point of failure” in firewall
- ICS network extends outside of physical security perimeter
- Dial-up port



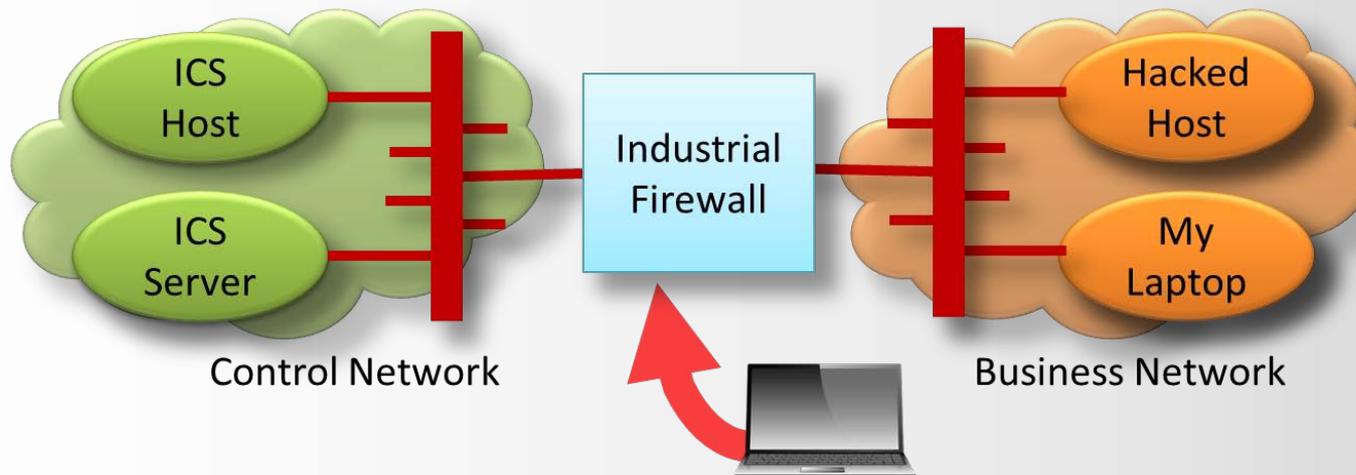
2-FACT
ENC
<b>RULES</b>
HIDS
NIDS
SECUPD
<b>UGW</b>





## #12 Physical Access to Firewall

- If you can touch it, you can compromise it
- Reset to factory defaults
- Log in to local serial port, change settings with CLI
- Re-arrange wiring



2-FACT
ENC
RULES
HIDS
NIDS
SECUPD
UGW



## #13 Sneakernet

- Removable media, especially USB sticks, carried past physical / cyber security perimeter
- Entire laptops, workstations and servers carried past physical / cyber security perimeter



2-FACT
ENC
RULES
HIDS
NIDS
SECUPD
UGW





---

# Demo



## Keeping Score

Graphic	Score	Impact
	2	Would have prevented / detected the attack
	1	Would prevent / detect some variants of the attack
	0	Would not have prevented / detected the attack

Score	Abbrev	Compensating Measure
<b>10</b>	2-FACT	2-Factor authentication
<b>10</b>	ENC	Encryption
<b>6</b>	RULES	Better firewall rules
<b>11</b>	HIDS	Host intrusion detection / prevention system / SIEM
<b>11</b>	NIDS	Network intrusion detection / prevention system / SIEM
<b>10</b>	SECUPD	Security updates / patch program
<b>20</b>	<b>UGW</b>	<b>Unidirectional security gateway</b>





## Waterfall Security Solutions

---

- Headquarters in Israel, sales and operations office in the USA
- Hundreds of sites deployed in all critical infrastructure sectors
- Frost & Sullivan: Entrepreneurial Company of the Year Award for ICS network security
- Pike Research: Waterfall is key player in the cyber security market
- Strategic partnership agreements / cooperation with: OSIsoft, GE, Siemens, and many other major industrial vendors

*Market leader for server replication  
in industrial environments*





## Firewalls Are Not Enough

- Firewalls are porous
- Given the “elephants in the room,” perimeter protection will always be disproportionately important:
  - 100,000 vulnerabilities
  - Plain-text device communications
  - Dissonance between ECC and IT’s “constant change” patch programs
  - Long life-cycles for physical equipment

*All ICS security professionals should be familiar with Unidirectional Security Gateways as an alternative to firewalls*

2-FACT
ENC
RULES
HIDS
NIDS
SECUPD
UGW

