waterfall

13 Ways to Break OT “Secure” Remote Access

And the questions we should be asking our SRA vendors

Andrew Ginter, VP Industrial Security
Waterfall Security

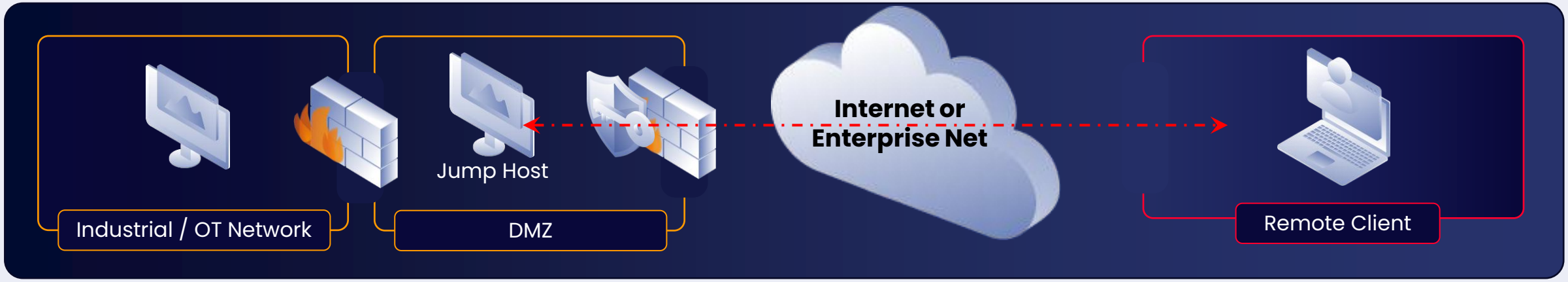
Roll Your Own – VPN, Jump Host, Firewall, DMZ

These products exist – but you can roll your own too – deploy a VPN in your DMZ, put some jump hosts there, configure firewalls

Remote Client – can be RDP, VNC, or vendor's remote client

VPNs may be nested – run DMZ TLS VPN inside corporate IPSEC VPN – gain access to IT first, then activate through to IT/OT DMZ

Deny by default – IT/OT & DMZ firewall best practice – deny all incoming ***and*** outgoing, allow specific IP pairs (except VPNs)



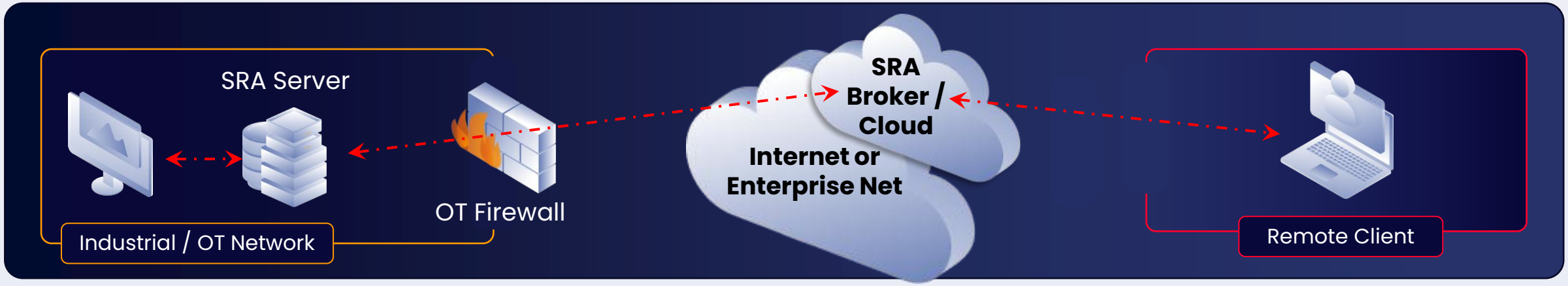
Rendezvous / Broker Style – "Modern" OT SRA

OT Server – serves as jump host – calls out to broker through firewall – "completely secure" – because no inbound connections through firewall

Broker – in IT network or in cloud – client & server rendezvous in broker – much like Teams & Zoom

Client – very often a web browser – "thin client"

"No firewall changes needed" – assumes all OT outbound connections to IT and to Internet are allowed – ***not best practice!***



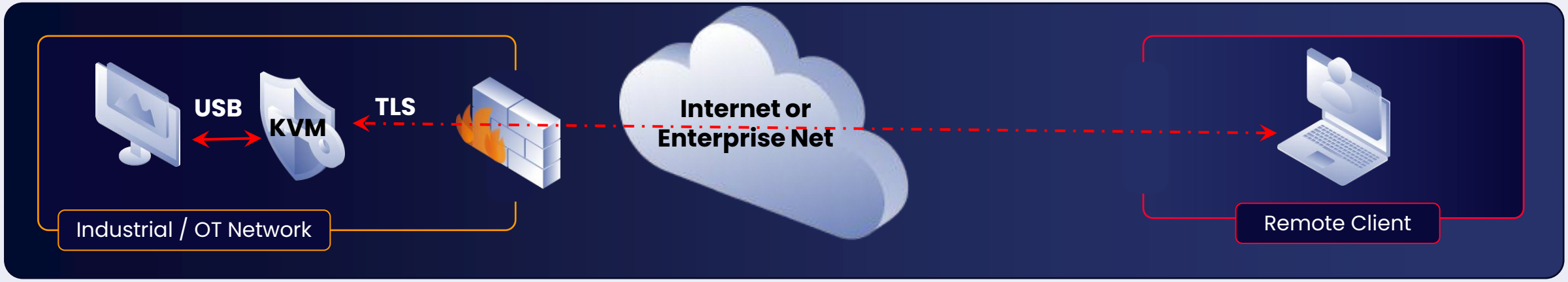
TLS Keyboard / Video / Mouse (KVM)

KVM – historically PS2 / VGA cabling – one keyboard, mouse & screen shared between multiple servers in a rack

TLS KVM – modern KVM has TLS / IP user interface, USB video, kb & mouse

TLS KVM SRA – has of course all the usual SRA features – MFA, multi-user, fine-grained permissions, etc.

Deployment options – Internet -> USB, or traditional Internet -> VPN -> IT network or DMZ -> USB



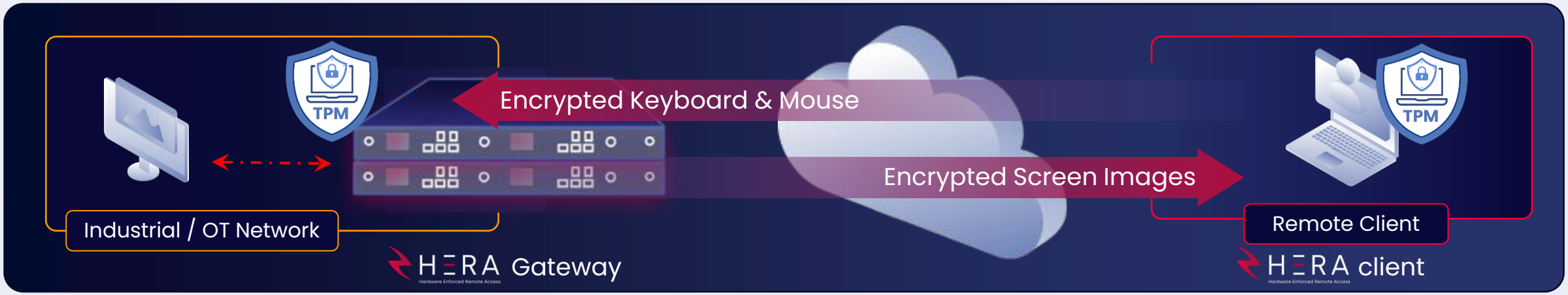
Hardware-Enforced Remote Access (HERA)

Two unidirectional gateways – under the hood – one sends encrypted screen images out and the other encrypted keystroke & mouse info in

Hardware filtering – to permit only the encrypted HERA protocol to pass into the OT side of the HERA device

End-to-end encryption – and authentication – from the remote client to the OT side of the device – the Internet-exposed CPUs do not participate

TPM – hardware-enforced identity on both client and gateway (OT) side



IT-Grade vs. Engineering Grade

Engineering-grade protection – eg: overpressure relief valve – no CPU – essentially “unhackable”

Remember Tacoma Narrows? Bridge tore itself apart in a stiff breeze: harmonic frequencies

Imagine that bridge – stabilized by hydraulic dampers - redundant power & control computers

How happy would you be – knowing the design engineer “hoped” any attack is detected in time?

How happy would you be – knowing the design engineer “hoped” that if detected, we could scramble incident response fast enough?

Lots of SRA includes IDS – hope?

Does your system provide engineering-grade protection, or “hope”?

waterfall

#1 Steal Credentials & Log In

Shoulder surf – watch as someone else logs in

Phishing – "IT requires you to click here to test the strength of your password" – "good job – very secure password"

Guessing – vendor default password for the SRA system? Most common password on the Internet (1234567)?

Breach another system – how many people use the same password on Facebook as the SRA system? Has Facebook been breached & the passwords published on the Internet?

Does your system use multi-factor authentication (MFA)?

… and all the other "usual" protections – session timeout, password length/complexity, password change requirements, strong encryption, etc.

VPN	KVM	RZV	HERA
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
9	9	9	9
10	10	10	10
11	11	11	11
12	12	12	12
13	13	13	13
14	14	14	14

#2 Exploit Legacy Crypto / MFA?

Lots of software is backwards compatible – this is a problem with security, especially with cryptographic and MFA protocols

Attacker – intercepts communications and changes the (plain text) crypto protocol request, or impersonates an old system logging in and exploits the protocol

Remote Access Is Convenience – generally not essential to continuous, safe, correct operations. Upgrade to the latest version. Turn off old protocols. Train the helpdesk how to walk complainants through upgrading their client.

Does your system support weak / obsolete encryption, MFA or other protocols?

VPN	KVM	RZV	HERA
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
9	9	9	9
10	10	10	10
11	11	11	11
12	12	12	12
13	13	13	13
14	14	14	14

waterfall

#3 Malware Jumps Through a VPN

Most SRA solutions support M2M and H2M – machine-to-machine (M2M) lets remote HMIs use Modbus & OPC to reach OT PLCs and OPC servers. Human-to-machine (H2M) transmits only keyboard & mouse

You might trust me – should you trust my laptop? Most VPNs provide access to the entire remote network, just like a physical Ethernet cable does

Malware jumps – across new M2M network connections, especially when there are many dozens of XP systems running on the newly-connected network

Does your system support only H2M?
Or M2M as well?

waterfall

#4 File Transfer

Malware lives in files – executable files, PDF files, Word files – any file with a sufficiently complex structure

Most SRA supports file transfer – and cutting/pasting files from the remote client machine into the OT network

Built in AV is supposed to detect malware – but malware evolves very quickly – no AV can guarantee 100% detection – remember "hope"?

Even some (not all) KVM SRA solutions – support file transfer – they let USB's on the remote client mount on OT assets as if the USB was local

Does your system support file transfer and/or file cut-and-pasting?

VPN	KVM	RZV	HERA
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
9	9	9	9
10	10	10	10
11	11	11	11
12	12	12	12
13	13	13	13
14	14	14	14

#5 Compromise Active Directory / Management Tools

People imagine Active Directory is a security tool – in fact it is a management tool for identity & permissions – a management tool that urgently needs to be secured

Practically all SRA – feature Active Directory integration, and central IT-hosted (IT-exposed) management tools for users, identity & permissions

SRA management tools – are also single points of compromise, and urgently need to be secured

Breach the management tools – and you can add your own user and change your new or old users' passwords, MFA credentials and/or permissions

Can a compromised Active Directory or SRA management tool add users, change SRA user or MFA credentials, or change SRA user permissions?

VPN	KVM	RZV	HERA
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
9	9	9	9
10	10	10	10
11	11	11	11
12	12	12	12
13	13	13	13
14	14	14	14

waterfall

#6 Man-In-The-Middle

Defeat the crypto and you can take over sessions – this is true for all SRA tools

So intercept the communications – eg: configure your laptop as a Wi-Fi access point with an SID of “Free_Airport_WiFi” – and tether to your cell phone with a USB cable – people will connect, you can sniff

Impersonate the SRA encryption certificate – web browsers and other apps will complain. A large fraction of users will override the complaints and force the connection anyways – through your fake access point. Now hijack the sessions.

Many browsers – support such overrides – because web sites regularly fumble their certificate update processes

Can users override certificate mismatch warnings issued by the SRA client?

waterfall

#7 Exploit SRA Vulnerabilities and Zero-Days

The SRA vendor publishes a security update – the bad guys AI reverse engineers the vulnerability, crafts an exploit and launches attacks against Internet-exposed SRA servers and cloud servers. Or find & exploit a zero-day.

The compromised servers allow access – rendezvous-style SRA can be forced to rendezvous, attackers simply pivot through compromised VPNs, compromised KVM devices do the attacker's bidding connectivity-wise

HERA is the exception – TPM compromise is very difficult, and the HERA authentication system is end-to-end – compromised "middle" CPUs cannot allow access

What is the worst that can happen if a zero-day vulnerability is exploited in your SRA server / broker / cloud?

…and auto-update both your SRA servers and clients.

VPN	KVM	RZV	HERA
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
9	9	9	9
10	10	10	10
11	11	11	11
12	12	12	12
13	13	13	13
14	14	14	14

waterfall

#8 Exploit Multi-Factor Zero Days

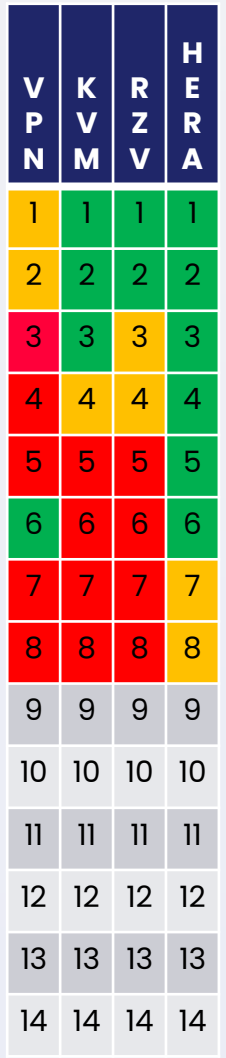
The MFA vendor publishes a security update – the bad guys AI reverse engineers the vulnerability and crafts an exploit. Or finds and develops an exploit for an MFA zero-day.

The attackers have long since phished credentials – now they can attack and compromise the MFA infrastructure with the exploit and the phished credentials

HERA has two multi-factors – conventional software and the client + gateway TPM hardware

What is the worst that can happen if a zero-day vulnerability is exploited in your MFA system?

…and auto-update your MFA systems, devices, and apps.



waterfall

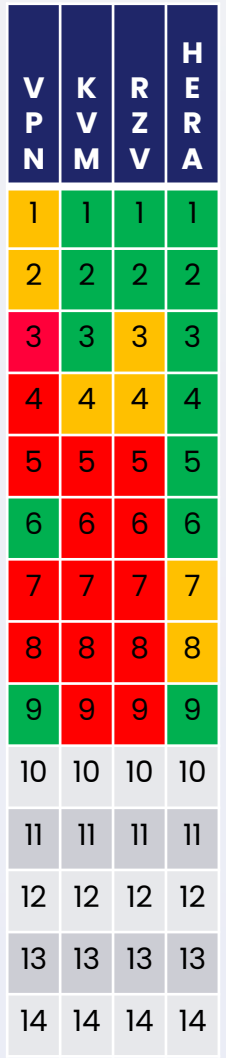
#9 Steal Browser Cookies – Hijack Browser SRA Sessions

Web browser SRA clients are supported – nearly all KVM and rendezvous / broker-style SRA boast about how they support web browser “thin clients”

Browser-based SRA sessions are tracked using cookies – steal the cookies and you can take over the sessions – from a machine in China, or North Korea

94 billion cookies were stolen in 2025 – and posted on the dark web – 20% of those posts were for one kind or another web browser session (eg: banking) – sessions active sessions at the time of the theft / post.

Can you hijack an SRA session by stealing the SRA browser’s session cookie?



waterfall

#10 Ignore SRA – Break In By Targeting The Firewall

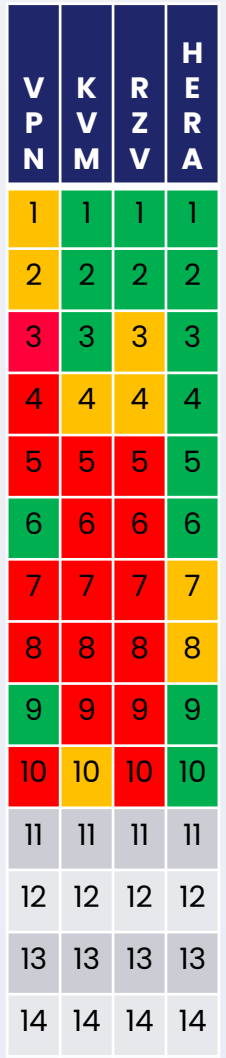
See Waterfall's recorded webinar – *13 Ways To Break A Firewall* – Google "13 Ways To Break A Firewall site:waterfall-security.com"

Most SRA use a firewall – essentially all VPN/jump host systems, broker/rendezvous-style systems, and most KVM systems

Possible to do firewall-less KVM – but most people don't

HERA – frequently deployed in firewall-less mode – HERA is a hardened security device

Does your system use a firewall?



#11 Rogue SRA Solutions

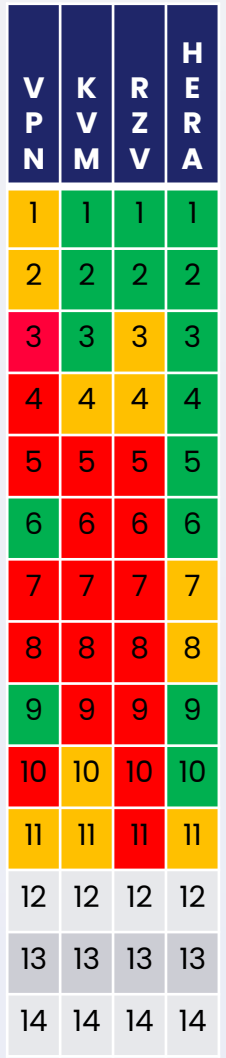
Well-meaning technicians – set up a persistent ssh connection to their home Linux server, with reverse ports tunneled

Cheap "completely secure" – consumer SRA solutions are deployed, again by well-meaning technicians, without consulting engineering, IT or whoever controls the IT/OT firewall

Vendors set up cell-modem connectivity – so they can "manage and support" their equipment at the site

Does your system assume deny-by-default?
If so, how can you deploy the system without changing firewall rules?

…no SRA solution can prevent cell-modems, but we should never be suggesting anything but deny-by-default in OT firewalls



waterfall

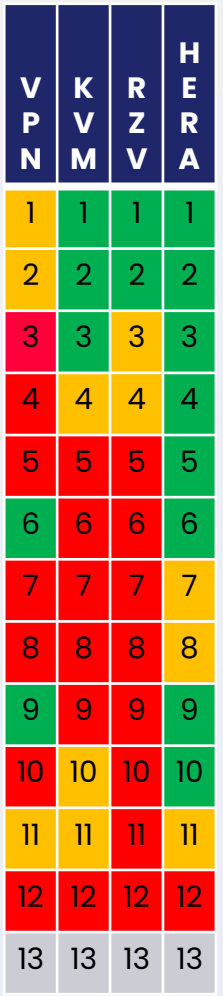
#12 Social Engineer The Help Desk

Research your victim – or phish them for details & credentials

Call the help desk – weave a convincing tale of woe: my cell phone with my authenticator on it was stolen! Or died! I lost my dongle – quick invalidate it and get me a new one!

Help desk helps you – to log back into “your” account

Question for your help desk:
How do you know I’m me?
Does anyone regularly test you with this kind of attack?



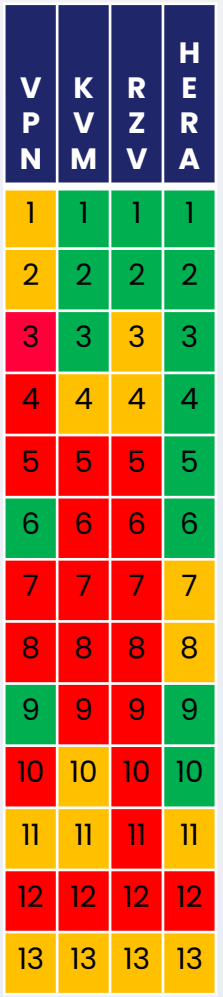
#13 Break The Crypto

Most OT SRA uses multiple cryptographic protocols – break the math of the crypto / randomness of the nonces and you can impersonate the SRA server without any warning messages and hijack sessions

Quantum – is the big thing everyone talks about

Is your crypto quantum-proof?

Can you change out your crypto algorithms easily?



VPN	KVM	RZV	HERA
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
9	9	9	9
10	10	10	10
11	11	11	11
12	12	12	12
13	13	13	13

What We Learn

First law of OT security – nothing is secure – every solution has residual risk

Some OT SRA solutions – are materially stronger than others

Some OT SRA vendors – are assuming, suggesting and failing to point out really bad firewall configurations

Attack	VPN	KVM	RZV	HERA
Steal credentials & log in	1	1	1	1
Exploit legacy crypto / MFA	2	2	2	2
Malware jumps through a VPN	3	3	3	3
File transfer	4	4	4	4
Compromise AD & mgmt. tools	5	5	5	5
Man-in-the-middle	6	6	6	6
Exploit SRA zero days	7	7	7	7
Exploit MFA zero days	8	8	8	8
Steal cookies, hijack sessions	9	9	9	9
Ignore SRA – break the firewall	10	10	10	10
Rogue SRA solutions	11	11	11	11
Social-engineer the helpdesk	12	12	12	12
Break the crypto	13	13	13	13

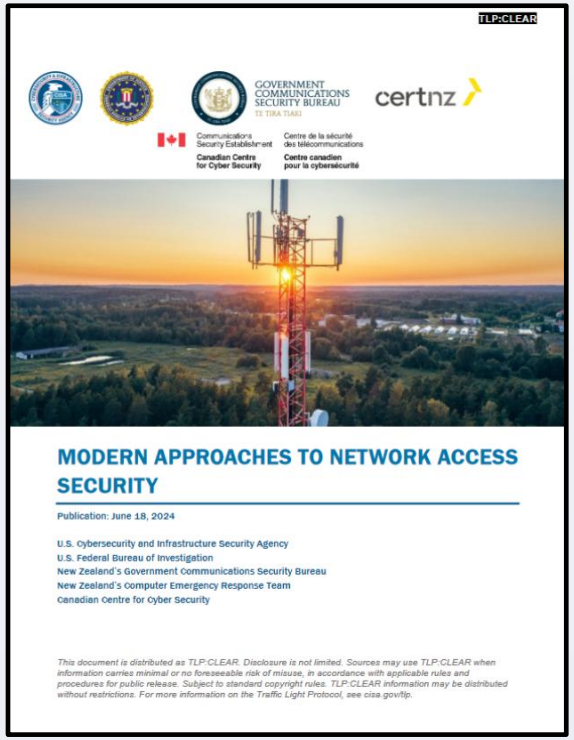
Hardware-enforced security is materially stronger than software-only

Modern Approaches to Network Access Security

Cross-agency advice – mostly targeted to IT, but has a section on OT

For IT networks – half your users are in the cloud working remotely – use the cloud to protect those "cloud workers"

For higher-consequence OT systems – use hardware-enforced unidirectional remote access



Modern Approaches To Network Access Security

Secure Connectivity Principles For Operational Technology

Cross-agency advice – nine authorities from seven countries

Look really hard – at any data *entering* your OT systems from outside – especially SRA – these are all cyber-sabotage opportunities

Use hardware-enforced unidirectional – stronger than software

Use hardware filtering – more trustworthy than software-only filtering

waterfall

Questions To Ask OT SRA Vendors

Does your system provide engineering-grade protection, or “hope”?	What is the worst that can happen if a z-day vuln is exploited in SRA svr, broker or cloud?
Does your system use multi-factor authentication (MFA)?	What is the worst that can happen if a z-day vuln is exploited in your MFA system?
Does your system support weak / obsolete encryption, MFA or other protocols	Can you hijack an SRA session by stealing the SRA browser’s session cookie?
Does your system support only H2M? Or M2M as well?	Does your system use a firewall?
Does your system support file transfer and/or file cut-and-pasting?	Does your system assume deny-by-default? If so, how can you deploy the system without changing firewall rules?
Can a compromised AD or SRA mgmt tool add users, change creds or permissions?	Question for your help desk: How do you know I’m me?
Can users override certificate mismatch warnings issued by the SRA client?	Is your crypto quantum-proof?

Hardware-enforced remote access has a materially smaller attack surface than software remote access (SRA)