OT-CERT

DRAGOS

# Getting started:

## Default Passwords and Internet Connected Devices

**Author:**
Reid Wightman
Dragos Senior Vulnerability Researcher

May 2024

# Legal Disclaimer

OT-CERT (Operational Technology – Cyber Emergency Readiness Team) resources are intended to provide guidance to help under-resourced organizations, those lacking sufficient financial resources or technical expertise, to establish minimum baseline OT cybersecurity protections and do not necessarily meet the usual best practice standards for a mature OT cybersecurity program. Dragos, Inc. does not provide any warranty or guarantee that following the guidance provided by OT-CERT alone will safeguard an organization from all OT cybersecurity threats. Whenever possible organizations should seek additional enhancements to the recommendations provided by OT-CERT resources based on an organization's own cybersecurity risk profile.

# INTRODUCTION

Improving the state of operational technology (OT) cybersecurity can sometimes feel like an overwhelming prospect for resource-constrained organizations. It is so easy to get lost in the details of the myriad of best practices for risk management, incident response, and security controls that it is hard to even know where to get started.

To help organizations get past the analysis paralysis, we encourage OT security champions to start simple. Our philosophy is that industrial cybersecurity teams should take a crawl-walk-run approach to building and maturing their programs. Don't worry about the advanced principles out of the gate. Just get some basics down first.

There are no silver bullets in security. Changing default passwords will not eliminate risk of a device being compromised. It will, however, reduce instances of drive-by compromise. It is an especially important procedure on internet-exposed systems. Understanding what devices fall into this category can be its own unique form of challenge.

In a world that is reliant on contracting services, it is often the case that 'ownership' of industrial equipment, particularly industrial connectivity equipment, is a blurred line. Remote connectivity for systems may depend upon a third-party system or service, may involve remote access as a part of a contract, and may not be included in normal asset lists.

An invisible 'Step 0' in determining what passwords to manage is knowing what *systems* to manage, via an asset inventory that includes not only owned property but rented property.

This Getting Started Guide is intended to help Small and Medium-Sized Businesses (SMBs) approach the development of this vital part of your OT cybersecurity program. Because of our recommended "crawl-walk-run" approach, throughout the document, some items are labeled as

*"Run" Level Advanced Component*.

Don't be intimidated by those more advanced components. In the beginning, just complete what you can and move on; avoid getting bogged down with items that may be far outside your current capabilities.

## TRENDS

In 2023, the number of security vulnerabilities which are "authentication required" increased significantly in the industrial space.

CVSS[1] (Common Vulnerability Scoring System), which is a numerical (0-10) representation of the severity of an information security vulnerability, often does not capture the nuance of these vulnerabilities. Vulnerabilities can often be chained together: default credentials, authentication bypass, or brute force issues can be chained with an authentication-required vulnerability to gain significant access to a device. These chains are not effectively communicated when vulnerabilities are displayed on their own.

A campaign to identify and remove default credentials in your environment will immensely improve your cybersecurity readiness. Eliminating default passwords helps mitigate some of those low-hanging fruit weaknesses that require the least amount of skills required for exploitation. It also helps to prevent drive-by modifications to control systems, which have been observed with increasing frequency since fall of 2023. At the very least, these changes make it so that attackers must brute force their way in, or phish a legitimate user, or some other secondary attack, to achieve their goals.

## DEFAULT PASSWORDS and COMMON PASSWORDS

In the industrial space, several classes of products are found with default credentials:

- PLCs or safety controllers
- Panel PCs or embedded HMIs
- Security appliances such as firewalls
- Network 'backbone' devices such as network switches and gateways

In addition, security credentials come in four common forms:

- Configuration of devices using proprietary protocols, or proprietary overlays of industrial protocols (most often found on PLCs and safety controllers).
- HTTP and SSH services, usually used for basic device configuration such as network settings (found on PLCs, security appliances, and network backbone devices). Particularly old equipment may even expose TELNET instead of SSH.

[1] https://www.sans.org/blog/what-is-cvss/

- VNC services or other 'remote HMI' type services for directly manipulating a controls system without any need to understand the ICS-specific network protocols. Also present on some PLCs with integrated HMI features.
- SNMP services, usually used for monitoring and sometimes for configuration of systems (found on PLCs, security appliances, and network backbone devices).

Default credentials also come in several shapes and forms:

- Simple credentials, such as 'admin/password' or 'admin/admin', more common on legacy equipment.
- Hardcoded credentials, which may either provide remote access or provide methods of performing a factory reset (where default credentials will now be in place).
- Empty credentials, common on VNC systems and HMIs with remote connectivity.
- More complex derived credentials, which may be derived from the device serial number or Ethernet MAC address. These often are found printed on the device identification label which is installed at the factory, and the device reverts to these credentials when a factory reset is performed.
- Truly random default credentials. These are also often found printed on the device identification label.

Differentiating between derived and truly random default credentials can often be a difficult task for end-users. As such, it is best to think of all random-appearing credentials as derived: it may be possible to determine the default credential, even a random-looking default credential, based on information that can be retrieved remotely (MAC address, serial number, etc).

Finally, one last class of credential should be considered: weak or common username+password combinations that are used in typical attacks. These may not be the default passwords for the device but may instead be common passwords used by automated intrusion software. The good news is that the techniques for identifying these share some overlap with the techniques used for identifying even 'Simple' default credentials.

Armed with this knowledge about where to look for default credentials, and what default credentials need to be changed, let us examine the impacts from leaving default credentials in place.

## A NOTE ABOUT CVES

In 2023, Dragos noticed an uptick in vulnerabilities with PR:L or PR:H in their CVSS vector. This means that the vulnerability exists in a device but requires some level of authentication: either low (L) privileges or high/administrative (H) privileges.

It is easy to dismiss these vulnerabilities as less important: after all, if an attacker can log in, particularly with administrator access, then why do they even *need* a vulnerability to do malicious 'stuff'?

As with most security topics, the answer is nuanced. Vulnerabilities, particularly those with PR:H access requirement, often give access to a system, especially an embedded system, in ways that the factory did not intend, such as low-level access to firmware, where it can be difficult or impossible for an end-user to truly remove the access. This level of access can also give an attacker the ability to permanently damage equipment, so that it must be replaced by the owner, as explained in the real case example below.

*Case Example: Fuxnet*

The 'Fuxnet' malware contains a module to continuously write data to a NAND memory chip in a sensor gateway. By repeatedly erasing and rewriting the memory, the memory 'wears out' and no longer holds data. NAND chips can typically be erased 100,000 times (often less) before the memory no longer reliably holds data. This requires low-level access to the device since normal access would not allow such fast overwriting to a single memory address.

This doesn't just apply to ICS-specific equipment. In-the-wild exploitation of equipment from major IT vendors also used a vulnerability with some privilege requirement.

Dragos researchers also identified several interesting flaws in internet-connected gateways in the past, including cellular gateways. For example, in one vendor's equipment, we could take advantage of the default SNMP "read-only" community ('public') to read an 'encrypted' form of a device administrative password. This administrative password could then be used to log in to the device and make configuration changes, export cryptographic keys and certificates, modify network access control lists, and provide direct access to industrial equipment.

Similar vulnerabilities likely exist in a wide variety of products. In the scenario below, an end-user changed the HTTP/SSH remote administration credentials, but by leaving the SNMP credentials in place, they allowed the attacker to retrieve the administrative credentials used to log in to the device, anyway.

*Case Example: Unitronics PLCs*

In late 2023, the threat group Cyber Av3ngers ran a campaign targeting Unitronics controllers. This campaign was fairly simple: connect to the PLC with the Unitronics software, and load the controller with a new logic project that displayed a defacement message. By deleting the original logic, this attack also reset the network adapter settings in the controller, so that affected controllers required physical access to restore them. Most owners replaced the hardware out of concern that it had been damaged. Dragos performed forensic analysis on one controller, which showed that it could be restored to operation.

## AUTHENTICATION BYPASS

As stated, there are no silver bullets in security. Indeed, even changing all the default credentials in a device may sometimes not change the overall security posture of the system. This presents a conundrum to the defender: is it worthwhile to change a credential even when the system may be "insecure by design"?

The answer is, in the humble opinion of the author, "yes". Evidence of recent intrusions against Unitronics PLCs[2], as described above, suggests that the attackers simply use the vendor-provided engineering software to gain access to remote PLCs. These low-skill attackers are still surprisingly effective but can be blocked via a simple credential change – because there is no evidence that the attackers have determined methods of bypassing the protection that is presented by the engineering software.

[2] https://www.cisa.gov/news-events/alerts/2023/11/28/exploitation-unitronics-plcs-used-water-and-wastewater-systems

Some examples of authentication bypass mechanisms:

- System reset for older Micrologix firmware ( https://literature.rockwellautomation.com/idc/groups/literature/documents/rm/1762-rm001_-en-p.pdf , page 53 "Clearing the Controller Memory" )
- Unitronics CVE-2024-1480, retrieval of password via unauthenticated protocol (CVE-2024-1480)
- General Electric UR relay password retrieval and decryption (CVE-2017-7905)

There are many others. Still, use of these vulnerabilities requires an understanding of the device that the attacker may not have and raises the barrier to entry.

## IDENTIFYING DEVICES AND THEIR DEFAULT CREDENTIALS

Step 0 of this section should be done first. The remaining sections may be performed at any time, however, are presented in order of easy to difficult in terms of implementation.

### "STEP 0": ASSET INVENTORY AND CONTRACTOR CONVERSATIONS ("CRAWL" LEVEL)

Obtain a list of all hardware that is key to the functionality of your control systems. Pay special attention to any contractor relationships, where the contractor or vendor requires some level of remote access to equipment. Remote access may come in the form of on-premises VPN appliances, or cellular gateway or other wireless gateways.

Pay special attention to equipment that is on network perimeters: either on your corporate network and facing the internet (e.g. for inbound VPN connections) and especially cellular gateways.

Once the list of remote access equipment, and remotely accessible equipment, is known, move to Vendor Documentation review.

### VENDOR DOCUMENTATION ("CRAWL" LEVEL)

Proactive vendors provide "Security Hardening" style documents which list:

- All network services, what they are used for, and what can be disabled.
- All factory-established accounts with instructions for changing them.

Often these default accounts require changes to both the account, as well as related 'client' software, which may automatically connect to the server and thus must be made aware of the credential change.

Encourage vendors that provide these lists by using their products, or by making such documents a contractual requirement for purchase. If the products are being provided and configured by a third party the specifications and contract language should explicitly state that products should include "Security Hardening" or "Secure Configuration Guidance" and the installer should follow those recommendations to the greatest extent possible.

### USING DEFAULT AND COMMON PASSWORD LISTS ("RUN LEVEL")

The Hydra brute force attack tool, when used with an accompanying default credential list, can be a terrific way to check protocols 2 and 3 (HTTP, SSH and SNMP). Using Hydra and other brute force tools with default credential lists can be useful in determining what equipment has default passwords ("Walk level"). However, it is not suited for checking proprietary or industrial-specific network protocols. For these protocols, no standard brute force tools are available.

Start by using the SCADA Strangelove list with Hydra or other online brute force attack tools: https://github.com/scadastrangelove/SCADAPASS. This list covers many industrial-specific devices including HMIs, PLCs, and industrial-specific network equipment.

See the Appendix for other default credentials lists that can be used by more advanced teams.

Dragos also develops its own brute force attack tools for use by its pen test teams. These tools are often written for proprietary network protocols, specific to one manufacturer or even one specific device line. While not available to the public, understand that tools like this exist – for example a brute force attack tool was a part of PIPEDREAM[3] malware targeting CODESYS PLCs. This is why it is important to set even proprietary systems to use passwords that do not exist in wide password lists.

## REMEDIATING OR PROTECTING

### CHANGING CREDENTIALS ("CRAWL" LEVEL)

The 'obvious' answer. Change not only the default password but, if possible, eliminate common usernames such as 'root', 'admin', 'administrator', 'user'. Look to default credential lists and avoid using usernames that are common, as well as passwords that appear in any common password list.

[3] https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/

### RECOGNIZING INEFFECTIVE PASSWORDS ("WALK-RUN" LEVEL)

Devices which use common industrial network protocols such as Ethernet/IP (TCP/44818), Modbus (TCP/502), or DNP3 (TCP and UDP/20000) are less likely to offer any meaningful protection of these services. The result: changing default credentials on HTTP, SSH, SNMP and other services on devices which natively support these industrial protocols will not offer much protection. The focus for this equipment must be to protect it by other means, such as VPN.

### LOGGING ("WALK-RUN" LEVELS)

Enable device logging and collect the logs in a central location for analysis. Most devices will log authentication attempts. For devices which are internet-facing, this may result in thousands or hundreds of thousands of authentication attempts per day. While sifting through this list may sound tedious, automation can help. Focus on successful authentications: if a remote field site was logged-in to, review who accessed it, and confirm that the access was legitimate. Further automation can then be applied: for example, if a legitimate engineer access the site remotely from the corporate IP space, then future access attempts from that same source can be squelched (but still preserved). Keeping the logs can help determine what happened in the event of a breach, either by an outside or even by a malicious insider.

### NETWORK MONITORING ("RUN" LEVEL)

Plaintext protocols provide an additional method of detecting default credential use. IDS signatures may be written for well-known protocols such as HTTP, FTP, or SNMP.

Run-level: monitor your network for default credentials use. Dragos Platform monitors for attempts to log in with default credentials for a variety of industrial equipment:

- ICS: ABB Default Credentials Login Attempt
- ICS: Digi Default Credentials Login Attempt
- ICS: Emerson Default Credentials Login Attempt
- ICS: Hirschmann Default Credentials Login Attempt
- ICS: Moxa Default Credentials Login Attempt
- ICS: Rockwell Automation Default Credentials Login Attempt
- ICS: Schneider Default Credentials Login Attempt

# INTERNET CONNECTED DEVICES

## INTRODUCTION

Internet-connected devices include:

- Cellular modems
- HMI displays with Remote Connectivity options
- PLCs with integrated HMIs
- Security gateways such as VPN appliances or network firewalls for securing remote access

In addition to the basic remediation steps (changing credentials and enabling logging), which should be done for ALL devices, internet-connected devices require some additional attention.

## FINDING ICS DEVICES THAT FACE THE INTERNET ("WALK" LEVEL)

Internet-connected assets *should* be identified in "Step 0", however realize that there will always be gaps in this process. Perhaps a contractor simply is not aware of some method of remote access that was installed, or a well-meaning engineer added remote connectivity for ease of troubleshooting, without documenting it on official network diagrams. There are many approaches to identifying internet-connected systems, but the basis should include a site walk-through to ensure that network diagrams are up-to-date.

This walkthrough can be followed-up with a check of popular search engines which implement industrial and 'things' protocols. While OT-CERT does not endorse any particular search engine, the Shodan site can be used for identifying industrial assets fairly simply.

A few common example searches are provided below. These examples can reveal devices with exposed industrial network protocols, or which expose common HMI VNC (Virtual Network Computing) screen-sharing services.

Common Shodan searches:
Modbus devices: port:502 "unit id"
Ethernet/IP devices: port:44818 "Product name"
VNC Servers: port:5900 "vnc"
(Note: further restrictions to a VNC search may include industrial or site-specific keywords such as "hmi" or "water" or "pump". Note also that VNC commonly uses ports 5900-5909, so run additional searches with additional port numbers)

Shodan also makes an attempt to geo-locate exposed systems. If the device is exposed from an IP address owned by your company, Shodan will indicate this. If your company does not have a block of IP addresses reserved specifically for it, the device may appear with your internet service provider as the 'owner' of the device.

Note however, many systems exposed - especially via cellular modem - may not be readily identifiable as owned by your organization. One reason: cellular networks are difficult to geolocate. For example, Dragos recently helped an analysis of several HMI systems located in the eastern portion of the United States. These systems were attached to cellular network providers. Shodan identified them as located in Texas and California, despite their actual locations in the US-Eastern time zone.

This is why asset inventory is so important and is considered the primary method of finding equipment. Unless the device has some company-specific label that is observable in search engine results, it can be difficult to point to exactly who owns them.

In several cases, Dragos has reached out to companies where the owner was specifically named, for example in a HMI or PLC project file. However, the owner could not locate the cellular gateway physically after multiple site visits. These can particularly frustrating experiences for all involved.

## PROTECTING INTERNET FACING ICS DEVICES

### ARCHITECTURE RECOMMENDATIONS ("WALK-RUN" LEVEL)

Changing the architecture of an already-deployed control system can be a very difficult process. If architecture considerations are made prior to deployment, this can be considered a "walk"-level remediation. Trying to change the system after-the-fact is very much a "run"-level remediation; however, an unprotected control system with internet connectivity is generally of the highest priority to address. In those cases, help from internal or external IT or OT Security support resources may be required. A project to mitigate a control system architectural weakness would include the implementation of a network firewall or other security device. The security device should be implemented such that it can restrict the flow of both incoming and outgoing network traffic to only what is required and authorized, as well as applying data encryption, integrity checking, logging, and potentially other advanced cybersecurity functions.

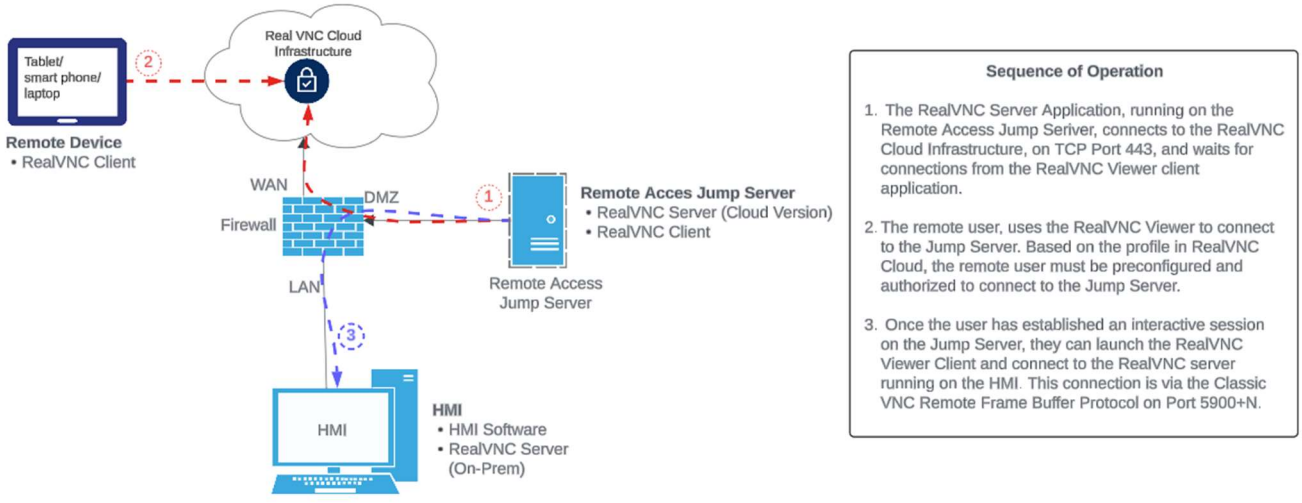
### VNC

Due to the prevalence of VNC deployments, we felt it would be helpful to discuss a secure deployment of VNC using the RealVNC variant.  RealVNC offers a VNC Cloud option that provides

some opportunities to implement architecture changes that enhance the security of the remote access connectivity. The main cybersecurity advantage of the cloud option is that you don't need to open any incoming "allow" rules on your perimeter firewall. All necessary connectivity can be supported with firewalls allowing connectivity from the internal LAN to the RealVNC cloud infrastructure.

In this architecture, the RealVNC server application runs on your asset on your local network and reaches out to the RealVNC cloud infrastructure. Ideally, you should make your firewall egress policy specific enough to allow the RealVNC server asset to communicate with the RealVNC cloud infrastructure, only. RealVNC provides the required documentation for their cloud infrastructure including the associated IP addresses and communications ports on their website.

Because the connection between the VNC client and server is brokered in the cloud infrastructure, you do not need any firewall rules allowing incoming connection to your VNC server.




Within your VNC Cloud profile you configure users, devices, and access groups to control access between users and devices. You should periodically review your organization's RealVNC profile to validate that the accounts and devices present match your organization's business cases.

Additionally, we recommend that you further configure your firewall to limit DNS queries to external resources to only the assets that require internet connectivity, such as the VNC server.

For example, if the only assets in your environment that need to reach out to resources on the internet are your VNC servers, then you can create an asset group for them and only allow that group to send DNS queries. Furthermore, you should choose a reputable DNS server, such as OpenDNS, and configure your firewall to only use those servers.

There is one caveat to mention here. If you only allow your VNC server to communicate to a restricted set of external resources as described above (which is recommended), the VNC Server will give an error because Windows will think it is not connected to the internet (it won't see the Microsoft DNS Servers). To fix that problem, you need to modify the registry setting, as follows:

> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet\EnableActiveProbing to 1

This registry setting disables active probing and resolves the aforementioned error in the VNC from an internet restricted Microsoft Windows Asset.

# CASE EXAMPLES AND THREAT INTEL

## PIPEDREAM

PIPEDREAM used some hardcoded credentials to go after Omron, default/null credentials for CODESYS, as well as credentials specific for Schneider Electric PLCs. While the Omron hardcoded credential cannot be changed, the null credentials and default credentials CAN be changed. Both of these latter issues can be corrected through setting new credentials (or, using certificate-based authentication in the PLCs).

## UNITRONICS/CYBER AV3NGERS CAMPAIGN

In a campaign that began in Fall 2023, the threat group Cyber Av3ngers wiped the configuration and defaced the HMIs on various Unitronics PLCs. A part of the attack is the ability to wipe settings and stop, start, and reboot the PLC using a passcode with a well-known default value.

The attackers in this case appear to simply use the vendor-provided engineering software, and to enter the remote HMI password. From there, the attackers could reset the controller and load new logic into it.

Changing the default password in this case is not a cure-all: Dragos recently disclosed CVE-2024-1480 for example, which identifies a case where the product stores the device password in a "recoverable format" such that an unauthenticated user can recover password in plain text. However, the threat group does not appear to have the skills necessary to use this technique and so changing the default password may still present some benefit to end-users.

### SSH CAMPAIGN

While this paper was being written, Cisco TALOS published an advisory about a SSH brute force campaign apparently targeting security appliances. SSH brute force attempts are nothing new for those that run internet-exposed SSH servers and monitor the logs, but Cisco helpfully documented IP addresses used in this sustained campaign, as well as common usernames and passwords that are attempted.

## ADDRESSING NEW PROJECTS AND EXISTING SYSTEMS

Recognizing that architectures are often expensive or risky to change, legacy assets often present a challenge in risk management to organizations. By working to better understand the systems and the site, operators can incrementally build toward their intended architecture. This architecture can be executed through planned projects or added to existing upgrades or obsolescence projects. Finally, mitigating controls such as visibility within OT systems is one of the best ways to better understand actual communication flows, identify potentially suspicious events or traffic, and become temporary conduits until more active controls can be implemented.

1. The design of new projects with internet exposure should document why the exposure is needed and who requires access. The architecture should be designed so that the remote site can 'phone home' to a central VPN service rather than exposing its own VPN service.
2. Include requirements in your plans and specifications for future projects that stipulate defensible ICS/OT network architectures. Require that all external connections be implemented in a cybersecure manner according to industry recommended practices. Also, make sure to explicitly include cybersecurity testing in your acceptance testing/system commission requirements.
3. Clearly establish which organization is required to harden, maintain, and re-assess the security posture of remote sites.

When working with contractors, especially contractors that provide remote connectivity to systems, gather an asset inventory list of products. Do not assume that the contractor will change default credentials or apply necessary security patches or updates: instead verify that they do so, and include contract language that clearly states who is responsible for maintenance and what remedies exist for failures to comply.

## GENERAL ARCHITECTURE RECOMMENDATIONS

Typical "legacy" architecture for outside-managed equipment is to place a cellular gateway or some other external connection on the equipment to be managed, as shown in the figure below. The cellular gateway then exposes one or more services, usually including a VPN service, or direct access to the industrial protocols, to the internet.

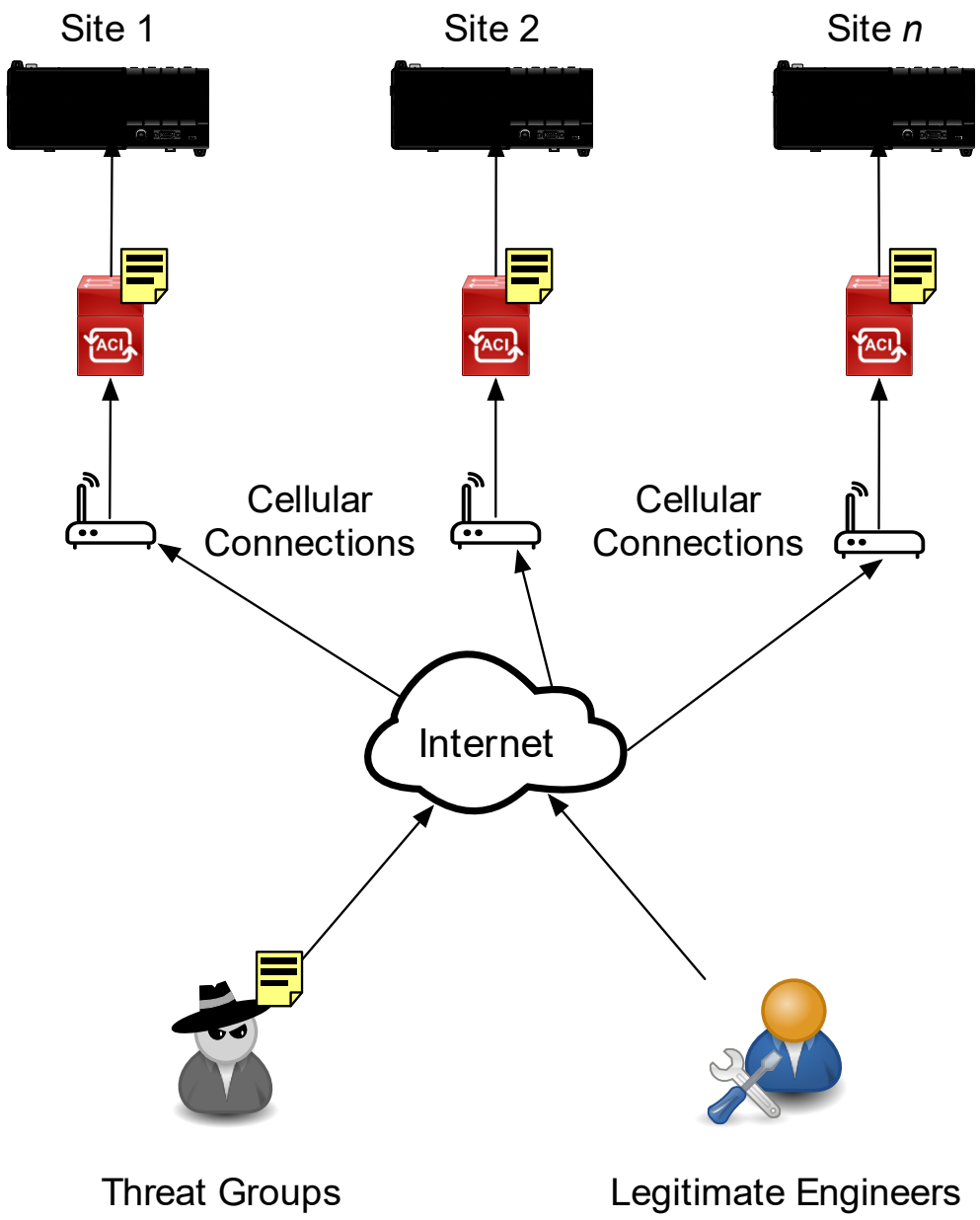



*Figure 1: Typical legacy architecture: service contractor requires access, but leaves services at each site exposed to the internet. The service exposed may be a VPN, but is more often direct access to engineering protocols and HMIs.*

Both of these methods should be avoided. Exposing services to the internet requires maintenance: keeping systems up to date/patched and hardened, dealing with configuration change management, and missing/forgetting to limit access to some service.

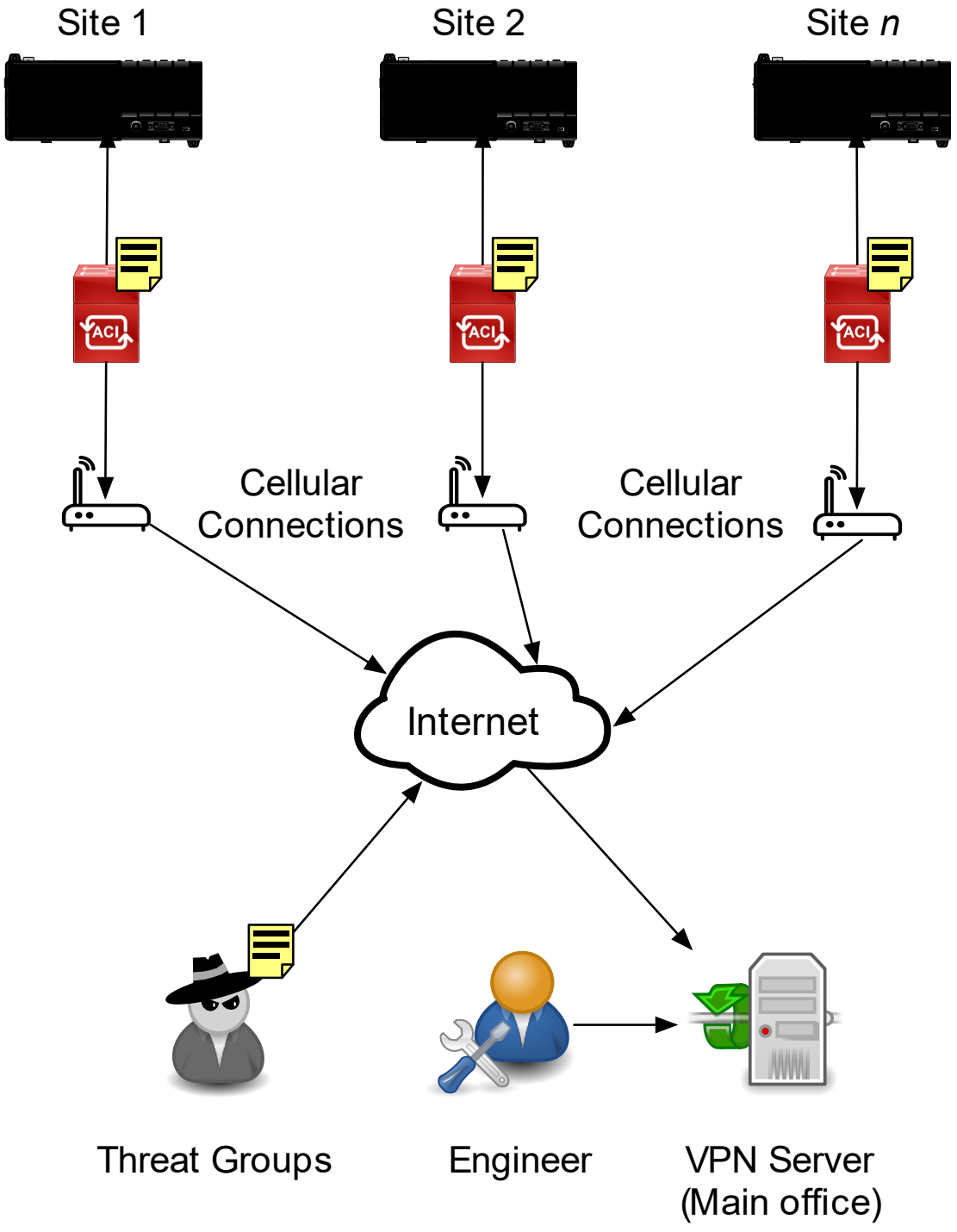



*Figure 2: A better architecture: cellular modems present no attack surface to the internet. Instead, only the main office presents a VPN server, which remote sites connect in to. This connection allows a tunnel to the remote sites.*

Historically, third party vendors rely on the fact that "no one understands ICS protocols" to protect equipment. This was a major contributor to recent Cyber Av3ngers' activity: the internet search engine Shodan incorporated a scanner for the proprietary PCOM network protocol, and indexed Unitronics PLC+HMI systems. The threat group likely used search engines such as Shodan to identify these exposed controllers. Once identified, the threat group used the VisiLogic software itself to connect to, and transfer a new program to, these controllers. That the controllers were left exposed with the default '1111' passcode made exploitation of the devices far easier.

## PROCUREMENT

When procuring products, insist upon documentation from the vendor which includes:

- Listing all default accounts
- Ability to change both usernames and passwords for all accounts
- (alt) Acceptance of JCDC Secure by Design Pledge

# Appendix: DEFAULT CREDENTIALS LIST

Start by using the SCADA Strangelove list with Hydra or other online brute force attack tools as described in the document. This appendix contains other default credentials lists that can be used by more advanced teams.

Mirai botnet source code: https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/scanner.c#L123 .This contains a list of credentials without specifying what actual device is targeted. While it does not target industrial equipment, Mirai may incidentally infect industrial controllers and network equipment which happens to run embedded Linux.

Miscellaneous equipment list:
https://gist.github.com/austinsonger/d70bbc36b88da097f1ce58c9add0c923 . This list specifies the vendor but not the device. It primarily covers IT equipment like network switches, VOIP systems, printers, and PC motherboards.

Miscellaneous equipment list:
https://192-168-1-1ip.mobi/js/parallax.js . This JSON format list shows make/model/protocol. It is mostly for home routers and whatnot, but we sometimes see these devices used in plants.

Cisco Talos SSH Campaign Credential list:
Cisco recently published about a campaign targeting SSH servers:
https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense/221806-password-spray-attacks-impacting-custome.html . Helpfully, they also published a list of offending source IP addresses, usernames, and passwords, that the campaign is trying:
https://github.com/Cisco-Talos/IOCs/blob/main/2024/04/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials.txt .

# RESOURCES AND REFERENCES

SCADA Strangelove password list:
https://github.com/scadastrangelove/SCADAPASS

Mirai botnet source code:
https://github.com/jgamblin/Mirai-Source-Code/blob/master/mirai/bot/scanner.c#L123

Miscellaneous equipment list:
https://gist.github.com/austinsonger/d70bbc36b88da097f1ce58c9add0c923

Miscellaneous equipment list:
https://192-168-1-1ip.mobi/js/parallax.js

Cisco repository of IoCs: IP addresses, usernames, and passwords used in SSH brute force attacks:
https://github.com/Cisco-Talos/IOCs/blob/main/2024/04/large-scale-brute-force-activity-targeting-vpns-ssh-services-with-commonly-used-login-credentials.txt

'Fuxnet' malware:
https://www.securityweek.com/destructive-ics-malware-fuxnet-used-by-ukraine-against-russian-infrastructure/

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.




## Dragos Global Headquarters

1745 Dorsey Rd
Suite R
Hanover, Maryland 21076
(855)-372-4670

www.dragos.com


## Customer Support Requests

https://portal.dragos.com/#/