Operant White Paper:

Mitigating Cyber Vulnerabilities by Architecture

Introduction

How big is my attack surface? 7? 53? Can a number even represent it? While these are simple questions, there are seldom simple answers. In this paper we will look at this topic, and how Operant Network's OPN Connect™ is designed to reduce the attack surface of Operational Technology (OT) networks.

Why is OPN Connect Different?

While this paper focuses on the topic of security, it is worth taking a brief look at why OPN Connect is different, and why that matters.

OPN Connect is designed specifically for industrial environments where it is critical to protect data and be certain that parties communicating are authenticated to be who they say they are.

Unlike typical TCP/IP architectures which are based around point-to-point links, OPN Connect is data-centric rather than connection-focused. As illustrated in **Figure 1**, a typical TCP/IP connection is composed of a series of hops, and each hop can be imagined as a pipe which is typically protected by VPNs and firewalls. In this way the journey is protected, but the data itself is not. This provides security but is complex to administer and open to misconfiguration during setup and over time. If an intruder is somehow able to break into the TCP/IP pipe they can alter any and all data, potentially targeting and compromising multiple pieces of equipment and applications at the site.

In contrast, an OPN Connect communication involves every data packet being individually encrypted, authenticated, immutable and with access controls at a packet level, even when added as an overlay to an existing TCP/IP network.

One advantage of this is that packets can take any route through a network and still be secure. Indeed, many routes can be taken in parallel, and

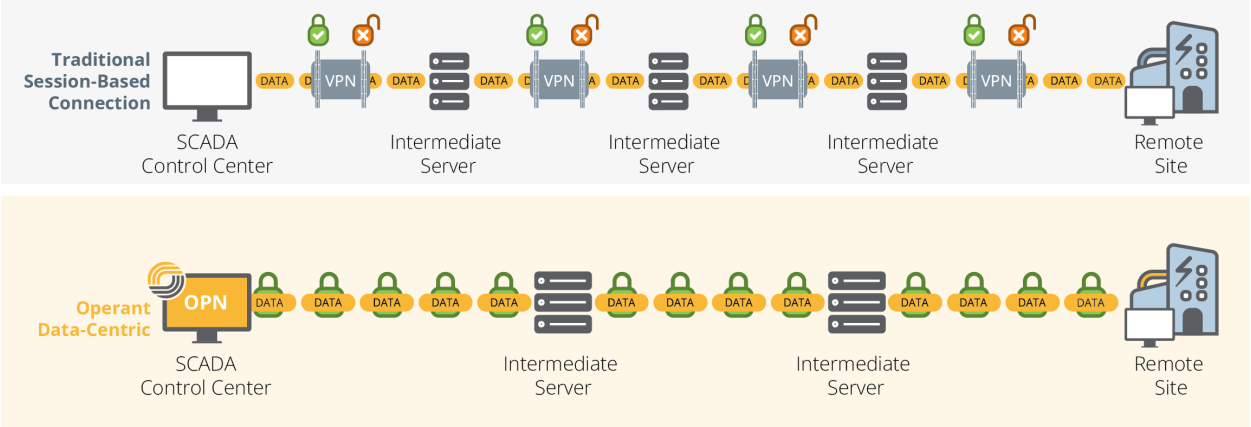


Figure 1: Comparison of a typical TCP/IP network employing VPNs and firewalls for security between a control room and remote generation site (upper) with OPN Connect's approach of securing and authenticating every packet individually (lower).

the network elegantly accommodates this; only the fastest packet reaches the destination, making redundant paths trivial and seamless, aiding resiliency. Data can be passed securely over any physical link that can pass bits, cellular, fiber are handled equally and smoothly.

Encryption is end-to-end, such that intermediate independent of type, such that wired, wireless, hops between and through servers are unable to access data. Indeed, only nodes with appropriate certificates can read data, inherently excluding any outside parties including Operant. No external party administers the network, and no third-party cloud overlay applies security. Identities are tied back to a single root of trust, and secured with hardware, cloud or virtual TPMs (Trusted Platform Modules).

Table 1: Summary of standard security protocols employed by OPN Connect.

Publication / Packet	Publication Signing	Publication Encryption	Response Publication Signing	Response Publication Encryption	Comments
Command	EdDSA Client software-based private key	AEAD-256	EdDSA Gateway software-based private signing key	AEAD-256	Full end-end security for command and return Data pubs. Pub signing entity determines access control privileges. Signing key and certificate updated every day and verified with TPM (hardware, virtual or cloud-based) private key.
Transport	AEAD-256 authentication	AEAD-256	AEAD-256 authentication	AEAD-256	Each transport link is AEAD-256 encrypted with separate key giving authentication and to hide the pub headers.
AEAD key (updated hourly)	EdDSA Server software instance private key	EdDSA public key from certificate collection	-	-	AEAD-256 content key encrypted in turn with each public key in certificate collection for distribution. Separate AEAD keys for end-end and transport link encryption and authentication.
X.509 Certificate	-	-	-	-	Certificate is signed by root certificate authority (CA) and is public.
Signing Certificate	EdDSA TPM-based private signing key	-	-	-	Software signing key used for speed with public certificate signed by TPM private key having the X.509 certificate.
CRL	-	-	-	-	Forthcoming.

OPN Connect packets can flow through existing TCP/IP networks, including VPNs and firewalls that are already setup, both making implementation easy and providing defense-in-depth such that any holes in existing security can be plugged by the OPN Connect packets.

A key attribute in securing OT networks is segmentation, the idea that sub-dividing nodes into smaller groups can restrict movement of attackers within a network. With this model in mind, OPN Connect can be thought of as nano-segmentation, with every data packet isolated from every other. Security is both comprehensive, but also modular and based upon industry norms (see **Table 1**) which can be updated as cryptographic algorithms improve.

Having taken an extremely brief tour of the technology, the discussion will now move on to the topic of attack surface.

What is an Attack Surface and Why Does it Matter?

NIST defines attack surface[1] as: "The set of points on the boundary of a system, a system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, component, or environment."

Various attempts have been made to rigorously quantify the attack surface with an absolute metric, however this is challenging. There are so many different possible attack vulnerabilities, and their importance varies for each specific business use case. So perhaps a better way is to use the principles of Attack Surface Analysis and just compare the relative safety of two security approaches for a particular business use case.

Here we consider industrial Operational Technology (OT) applications, such as energy systems, in detail. For the comparison, cyber-attack resistance for a traditional IP-based approach with TLS, VPN, and other security overlays, compared with adding the OPN Connect publish/subscribe (pub/sub) security framework overlay.

Key aspects of the Attack Surface Analysis include:

- Delineation of business-critical functions that must be protected.
- Limiting access to the system. Approaches include role-based access controls; layered defenses; controlled software supply chain risks; physical intrusion controls; disabled inactive accounts; isolated business critical data; and social engineering mitigation.
- Identification of all data paths in the system and secure them with digital signing for authentication, authorization, and integrity together with encryption for confidentiality.
- Securing of all private keys and data storage caches.
- Reducing the amount of critical code that executes.

More recently, in NIST SP 800-207[2], the similar but more refined concepts of zero trust are described to further improve cyber-security: Control and secure all data flows regardless of network location; consider every user or industrial asset as a resource; enforce least-privilege access for each data access; and Transparent privilege policy.

Maintaining consistent efforts to reduce the attack surface and apply zero trust principles to Critical Infrastructure energy systems has essential national security implications as they are targeted by sophisticated nation-state actors.

1https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

2https://csrc.nist.gov/publications/detail/sp/800-207/final

Security Aspects of OPN Connect Pub/Sub for Industrial OT Energy Systems

In a simple diagram of an energy system OPN Connect network (**Figure 2**), seven resource entities are shown.

Each can publish named data publications to securely transport information. The admin employs a highly secure system and publishes compiled trust rules to all entities. These specify precisely which energy generators can supply generation production data publications to each control center (Utility and Wind Supplier). Only the utility is allowed to see the solar data.

For resiliency, multiple servers relay the publications, but only relay data publications are allowed by the trust rules. All publications are signed by private keys that are securely stored in a TPM of some kind in each entity. Corresponding public key certificates signed by the admin are published to all entities for signature validation.

For confidentiality all publications are AEAD encrypted. This security is end-to-end: Only entities authorized by the rules can publish, relay, subscribe to, or decrypt a publication. In addition, the OPN Connect publication name is hashed and double AEAD encrypted during each transport hop, thus transport traffic between the entities cannot be snooped to determine flow patterns.

The use of multiple servers and multiple transport paths creates a resilient distributed system that can cope with natural disasters such as hurricanes or fires, as well as cyber-attacks, which can disable servers or transport paths. In addition, remote generation sites can publish data once over limited bandwidth cellular connections and distribute it to multiple control centers or storage locations on or through servers as allowed by the granular trust rules. The data is always encrypted, even when at rest in storage. Such flexibility and resiliency are not possible with a basic point-to-point IP connection alone.

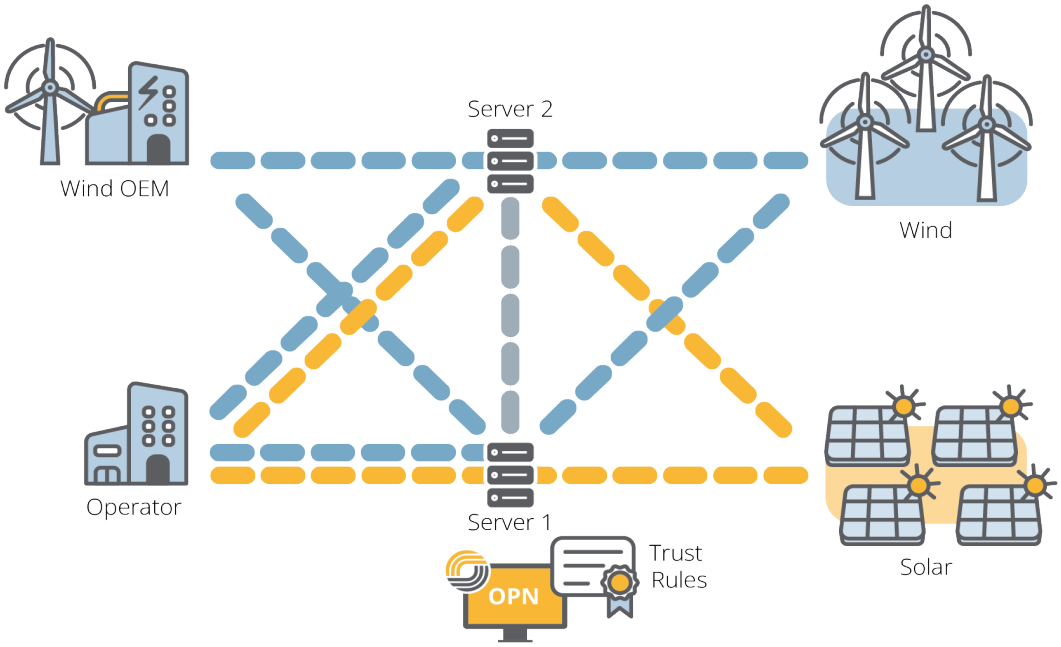
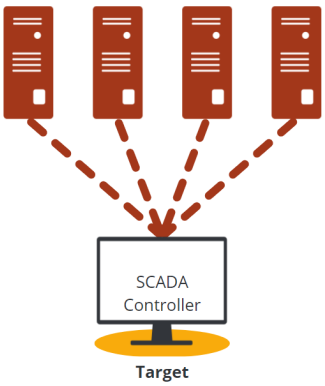


Figure 2: A simple OPN Connect power generation network example. Here the Owner/Operator is able to see data from both generation assets, while the wind turbine vendor is prevented from receiving data from the solar site by the trust rules which are enforced at all OPN Connect nodes in the network.

Additional comparisons of Attack Surface vulnerabilities between OPN Connect and TCP/IP networks without OPN Connect are considered in the following sections.

1. Denial of Service

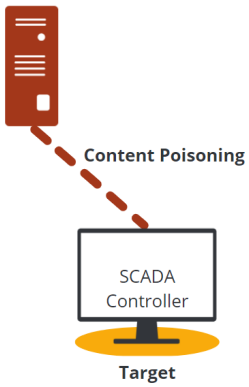
In IP networks an entity IP address can be determined through DNS services or by analyzing traffic patterns. Sending repeated requests to this address can block other access (a DoS attack). Sometimes multiple sources coordinate to simultaneously access the same address (DDoS attack).



OPN Connect authenticates all Protocol Data Unit (PDU) data packets with AEAD so they are immediately rejected by all entitles outside that OPN Connect network since they lack the key. Entity firewall rules can restrict IP access to that entity to only those other nearby OPN Connect entity IP addresses in the network, and these upstream entities also reject any out-of-network traffic. Resilient OPN Connect network paths can also maintain data flow despite the possible DoS compromise of a single node.

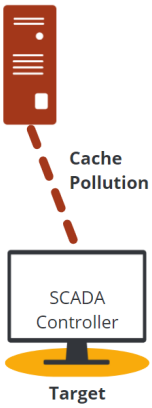
2. Content Poisoning

A rogue actor can attempt to publish fraudulent data into the publication collection. However, all publications are signed with an asymmetric private key securely held in the TPM of each authorized entity. Trust rules restrict the entities (with corresponding private signing keys) that are allowed to sign each publication. In addition, the transport packet PDU that carries the publication is independently signed with the AEAD symmetric key. Both keys are required to forge a new fraudulent publication or modify an existing publication, and only publications that adhere to the security rules and keys are accepted.



3. Cache Pollution

In traditional networks proxy data caches can be attacked, attempting to overflow the intermediate cache with fraudulent data. In OPN Connect each entity caches the full collection of publications it subscribes to, with each signed to guarantee it is an authentic copy. Attempting to publish multiple fraudulent publications to overwhelm the collection is prevented since fraudulent publications are immediately dropped and not cached.

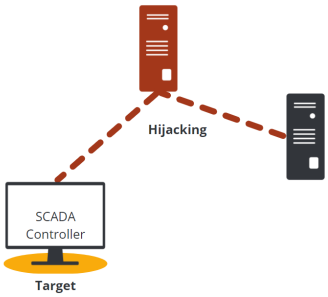


All PDU data packets that are relayed to multiple entities through the OPN Connect network are AEAD authenticated so that they cannot be altered in intermediate relaying nodes. Hence, any OPN Connect packets making up a publication at multiple locations in the network are cryptographically identical and cannot be altered for cache poisoning. Trust rules limit which entities can publish into the collection and unauthorized publication, forwarding and subscription are blocked. Fraudulent publications cannot be introduced into the collection cache since they are not authorized.

4. Name Hijacking

In traditional IP networks DNS attacks through phishing or DNS server compromise can route data to rogue entities. An analogy in an OPN Connect network is to publish OPN Connect data to an incorrectly named collection. However, in OPN Connect zero trust rules guarantee that a publication can only be published by; relayed through; and subscribed to by authorized entities, and only for the valid publication name. Signed publication and PDU names cannot be altered.

5. Route Hijacking



In traditional IP networks false routes can be advertised to misroute packets through a router. In OPN Connect each entity in the network is named and trust rules govern, using zero trust, whether that entity can publish, relay to another specified entity, or subscribe for each named publication. False routes are cryptographically prohibited by zero trust. Publication distribution is name-based and not routing table based. Signed publication names and trust rules cannot be altered, and relay entities do not have the signing keys.

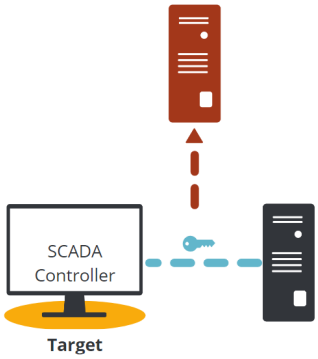
6. Application Hijacking

If an application encrypts its publications, which is typical, the distribution of the encryption keys can lead to compromise if performed carelessly. In OPN Connect generally all publications and transport PDU are encrypted, and the keys are distributed in a consistent manner. The AEAD symmetric key generator entity creates the AEAD key hourly and then separately encrypts it with the asymmetric public key for each entity in the collection group. The public keys are obtained from the certificates which are published to all members in the group. The subscribing entity decrypts their version of the encrypted AEAD key using their private key in the TPM. Trust rules govern which entities can publish and subscribe to signed key distribution publications. Thus, the key distribution is handled securely in a consistent way as part of the OPN Connect transport.

7. Private Key Compromise

All authorization in a cryptographically secured system is tied back to the private keys that sign the packets and publications. In traditional IP systems these may be secured by shared or default passwords or stored on disk where they can be discovered. In the Operant OPN Connect system, private keys are stored in each entity in a TPM. This type of security constitutes a "who-you-are" security mechanism.

In addition, two-factor password protection can be added to secure access to devices that host the TPM, this is "what you know" or in the case of a multi-factor authenticator "what you have". The asymmetric private key in the TPM is used to decrypt distributed symmetric AEAD transient keys (that have a 1-hour lifetime) residing in memory. These are securely published to all entities for publication and packet encryption and authentication. AEAD-256 keys are very secure (requiring much more than 1 hour and more transmitted data to cryptographically compromise) and attempting to extract them from a compromised device's memory is of limited utility since they are frequently updated.



If a processor OS or the OPN Connect binary is compromised locally on the machine, then access to the keys could result in compromise of the application and the entity authentication. This is always a risk and can be reduced with traditional methods of multi-factor entity logins, physical controls of OT network equipment, signed OPN Connect application binaries, and secured boot and memory partitions in a Trusted Execution Environment

in the processor.

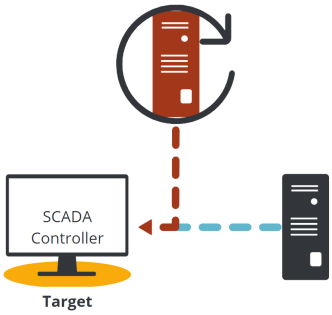
Zero trust rules also limit what a single compromised entity can do according to the detailed permissions.

8. Man-in-the-Middle Attack

In a network, if an attacker can connect in-line in the middle of a network they can intercept data, forward, drop or modify packets as desired. In an OPN Connect network packets are end-to-end signed and encrypted so that they cannot be viewed or modified. In addition, intermediate links double encrypt each transport PDU with AEAD to provide authentication and to obscure header information. Thus, without both AEAD keys the intercepted packet cannot be decrypted or modified. In addition, without the asymmetric publication signing key the intercepted publication can still not be modified or re-sent, since each signed publication includes a nonce and is thus unique and immutable. Finally, firewall rules and trust rule permissions only allow authorized connections in the middle of the network to other validated and authorized entities.

9. Replay Attack

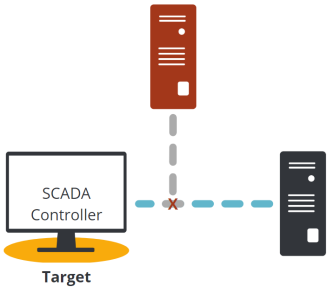
In a replay attack the adversary captures signed packets and replays them in an organized manner to compromise the network operation. In an OPN Connect network each publication is signed and encrypted so the packet content is not viewable by an adversary and cannot be altered.



In addition, each publication has a nonce that it is unique. If an attempt is made to republish into a collection, the repeat publication is dropped since it is already in the collection. Changing the nonce in the signed publication is not possible without the appropriate trust rule permissions and the corresponding private key for signing. Similarly, each transmission data packet is AEAD encrypted and authenticated including a header with a nonce. Replayed transmission packets are summarily rejected as duplicates.

10. Anonymity or Censorship Attack

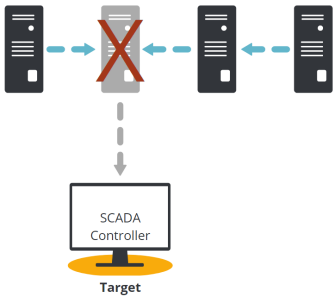
An attacker sniffs commands and return data traffic and then selectively drops or censors chosen content anonymously. In OPN Connect each publication is encrypted, and each transport data packet is doubly encrypted obscuring the header. It is impossible to sniff the content of the transport packets or publications without the corresponding AEAD encryption keys.



Also, multiple network paths relay packets from the publisher to the subscriber. Censoring packets or publications at one node will likely not block publication collection synchronization over parallel resilient paths. A dropped packet will continue to retry and synchronize the collection and there is a notification if synchronization is unsuccessful.

11. Black Hole Attack

An intermediate relay entity node or connection path is disabled due to cyber-attack or other equipment failure. In a point-to-point secured network all end-to-end communication will cease. In OPN Connect a resilient network can be designed with multiple relay nodes in diverse geographic regions and cloud environments, using communication over multiple media types such as fiber or cellular. Publications are secured end-to-end and during each transport hop are synchronized across all the intermediate nodes to the end connections. In this way, if any single path through transport media or relay entities remains operational the resilient OPN Connect mesh will retain robust functionality.

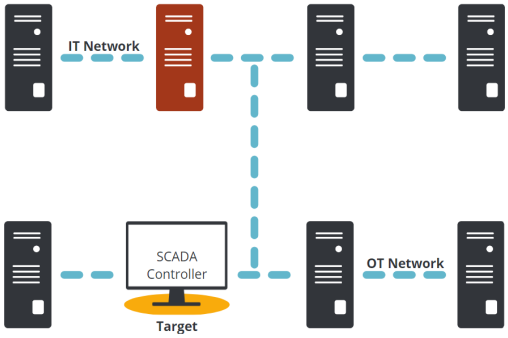


12. IT Compromise of Operational Private Network (OPN)

An IT network which is shared with all the other IT functions including email, web browsers, and social networks has many additional attack vectors such as phishing emails, and DNS attacks with altered URLs in web browsers. If OT systems share the IT infrastructure, many common attacks, such as ransomware, originate in the IT system. An OPN Connect operational private network is completely separate from the IT network with unique keys and authorizations including a separate OT root of trust, even if it passes through and over the IT network. The OT network cannot be attacked by common means, greatly reducing the attack surface.

13. Shared IP Transport Compromise

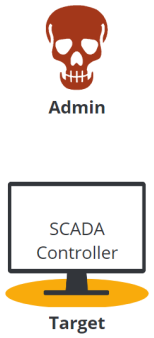
Segmentation of OT networks is used to limit the exposure of Critical Infrastructure to port scanning and password attacks. This has been used for energy systems through: dedicated private fiber lines, VPN access through public networks, firewalls and SD- WAN. However, in distributed energy systems with thousands of sparsely located assets it is not cost-effective to secure all these connections. Often all paths are not configured robustly leaving cyber-security holes and increasing the attack surface.



In OPN Connect every entity has a unique key and role-based certificate authorized through the zero trust rules. Every publication data packet is end-to-end signed and encrypted and validated back to a locally stored root of trust. Each transport hop is double- encrypted to obscure the OPN Connect publication header. Multiple end-devices, connections, and servers, together with parallel resilient network paths can be supported in the cost- effective shared transport infrastructure, without raising the complexity or broadening the attack surface.

14. Unauthorized Role Access Attack

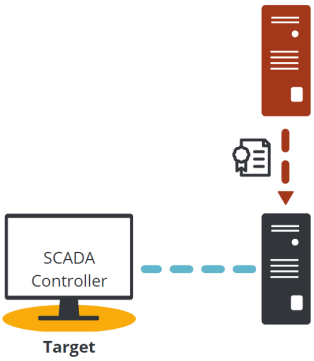
IP systems implement access control through application-level controls. Zero trust is approximated by micro-segmentation which adds numerous firewalls and complexity. Insider threats remain since full control remains for each segmented island of assets.



In OPN Connect each publication in the collection has granular data-level permissions that are secured in signed trust rules that are published to all entities for enforcement. Role-based access is checked each time a publication is published, relayed through a node or subscribed to. The publishing, subscribing, and relaying entities must possess the appropriate private keys to pass the packet along with the corresponding granular Attribute-Based Access Control (ABAC) permissions in the signed trust rules. All validations are through a trust chain that traces back to the shared OPN OT network root of trust. The trust rules are compiled to a compact binary and are checked for mathematical completeness and consistency using Langsec security principles.

15. DNS Server Attack

DNS servers are used for conventional TLS security and the resulting 3rd party CA certificates are subject to DNS spoofing and DNS service compromise. Some 3rd party CA certificates like those for IEEE 2030.5 energy systems cannot be revoked. OPN Connect uses an internal root of trust that is shared at installation with all entities. The corresponding root private key is securely controlled by the OT network high-level administrator. Role- based certificates are issued by an internal OPN Connect CA that can also generate granular data publication-level trust rules. OPN Connect certificates are revocable back to an OT CRL (Certificate Revocation List) or authorized Whitelist server to eliminate known attackers.

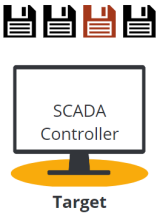


16. Cryptographic Algorithm Attacks

In most IP traffic there is no encryption or signature unless TLS is used. Different crypto algorithms are employed for the various TLS standards, with varying levels of security. OPN Connect uses the Libsodium open source, cross platform crypto library, a well-respected library. AEAD 256-bit symmetric encryption keys with hourly key updates and distribution are used to encrypt Publications, and to separately encrypt and authenticate the transport Protocol Data Unit (PDU). EdDSA 256-bit asymmetric signing of publications with strength equivalent to ~ 3000-bit RSA is used. All publications are signed and encrypted and all PDUs are encrypted by default, providing a consistent level of security. The configuration and choice of the algorithms used is flexible and can be easily updated as cryptographic requirements change in the future. Quantum resistant algorithms can be used if needed.

17. Insider Attacks, Proprietary Code and Supply Chain

Complex IP software applications with numerous interacting code blocks increase the attack surface exponentially, given all the possible interactions between the components. Not only does each unique block present vulnerabilities, but the interactions between these blocks also add intrusion points. Code blocks can have insider threats, supply chain defects, or security holes. Many IP security applications are proprietary 3rd party code and cannot be verified.



OPN Connect is based on a network-level security paradigm in which all packets are secured, authenticated and authorized as part of the transport. This network-level code is open source so that it can be verified by trusted auditors, national labs, or cyber-security groups, using white and black hat teams. All OPN Connect executables are version controlled and signed once verified so they cannot be altered. Supply chain risk is minimized in these critical security functions using trusted libraries.

OPN Connect security follows the principles of KISS (Keep It Simple). Since the key security code is isolated to the network layer, it is compact and relatively simple to understand and verify.

Exploits & Mitigations Summary

Having looked at some common attack types, a summary is given in **Table 2**, below.

Table 2: Summary of exploit types and OPN Connect mitigations.

Exploit	Corresponding IP Vulnerability	Summary Description	OPN Connect Mitigation
1. Denial of Service	Denial of Service (DoS) or Distributed Denial of Service (DDoS)	Generate massive data traffic to overwhelm nodes in the network	Firewall rules allow only authorized node IP access. Unsigned packets rejected. Duplicate publications dropped. Only trust rule-authorized traffic is relayed.
2. Content Poisoning	False Data Injection	Router or data producer is compromised and publishes fraudulent data publications	All transport packets signed. Publications signed and router does not have the key. If the data producer key is compromised then trust rules limit which publications can be generated. Application security controls limit likelihood of a compromised producer.
3. Cache Pollution	Proxy cache pollution	Generate large numbers of publications that must be added to collections resulting in overflow	Publications are signed. Invalid publications are not added to collections. Packets are signed. Invalid packets are dropped. Trust rules govern allowed publishers, dropping others.
4. Name Hijacking	DNS hijacking	Capture publication names and explore manipulating them	Publication names are encrypted in transport PDU and cannot be sniffed. Trust rules govern explicit publication names that each entity can add to the collection. All publications and PDUs are signed so the names cannot be altered.
5. Route Hijacking	False route advertisements	Cause misrouting of publications to fraudulent destinations through a compromised relay entity.	Publication distribution depends only on the publication name and the relay trust rules. Subscription is impossible without an authorized rule and entity name and key. Trust rules and publication names are signed and cannot be changed. A relay entity does not have the keys.
6. Application Hijacking	Key exchange	Capture encrypted data. Gain access to keys through improper key distribution by the application.	Publications and PDU are double encrypted with AEAD. Symmetric AEAD keys are encrypted with the asymmetric public keys of each subscriber individually, and signed by the key publisher's private key prior to distribution through publication. Trust rules govern which entities can publish and subscribe to the key publication.

7. Private Key Compromise	Private key exploit	Through the application or Operating System (OS) the private key is extracted and used to sign a fraudulent publication, or decrypt encryption keys.	Private keys are stored in a TPM and never extracted. A Trusted Execution Environment (TEE) can be used to limit access to the TPM and to authenticate the application binary to avoid corruption. Two-factor application access control for TPM cryptographic functions.
8. Man-in-the-middle	Man-in-the-middle	Access is gained to an intermediate entity relay node and packets in transit are intercepted. These packets are selectively dropped, relayed inappropriately, or modified.	All transport packets authenticated and encrypted with AEAD. Publications are double-encrypted and asymmetrically signed and relay entities do not have these keys. Relay trust rules limit which routes can be relayed to and firewall rules specify only valid IP addresses for authorized entities.
9. Replay	Replay	Packets or publications are intercepted and replayed in an organized manner to alter network operation.	Each publication is signed with a nonce. Duplicate publications are rejected. Similarly, each PDU packet is AEAD authenticated with a nonce and duplicate transport packets are dropped.
10. Anonymity and Censorship	Anonymity and Censorship	Man-in-the middle captures command request and then censors (drops) the corresponding reply data packet anonymously	Packet and publication encryption blocks initial capture. Response data publication encryption makes it difficult to identify publications to drop. Multiple return data paths must all be blocked. Return data publication collections will synchronize and retry, so if the publication is dropped, there is a notification to the publisher.
11. Black Hole	VPN server failure	An intermediate relay server or TCP connection fails due to a cyber-attack or other cause and the publication cannot be transported	Resilient relay servers and TCP interconnections allow collections in all functioning entities to synchronize all publications even if isolated entities or connections fail. Unlike point-to-point TLS connections, OPN Connect is end-to-end secure over multiple resilient paths.
12. IT Compromise of OT	Phishing, DNS attacks, altered URLs	If an OT network is interconnected with the IT network attacks through phishing emails or DNS can impact the OT network	Using a local root of trust and verifying all PDU transport data packet and publications to this locally stored root of trust isolates the OT network from common IT vulnerabilities.
13. Shared IP transport	Port scanning, password attacks	IP port attacks in shared low- cost infrastructure impact OT systems. Physical isolation and dedicated fiber lines are too limited and not cost-effective.	Securing each transport data packet and publication by signing and validating back to a locally stored root of trust does not depend on the security of the data pipe, but instead directly secures each data packet sent over any resilient cost-effective transport that can transfer bits. All data is double-encrypted for confidentiality.

14. Unauthorized Role Access	Network segmentation failure	Granular role-based access is required to secure critical OT functions while allowing general access for other cases. Micro-segmentation with firewalls is cumbersome and can be breached.	Granular role-based trust rules are securely distributed to all entities and define which publications can be published, relayed, or subscribed to for each entity and role. All aspects of the access control are signed and validated back to the locally stored root of trust.
15. DNS Server Attack	DNS server compromise. DNS name hijacking	Keys from web-based DNS server and CA are compromised introducing vulnerabilities	A local root of trust and CA certificates isolates the OT system from systematic web-based CA issues.
16. Cryptographic Algorithm	Insecure cryptography	Some crypto algorithms are poorly implemented, or insecure versions are used.	Operant OPN uses open source vetted Libsodium crypto library. Algorithms are easily updated and can support Quantum-secure algorithms in the future as needed.
17. Insider. Proprietary Code	Supply chain vulnerabilities. Black box code. Back doors.	Application layer security cannot be verified. Insider back doors. Inconsistent application of security methods.	Transport layer OPN Connect security is open source and contained so it is verifiable by third parties. Executables are signed to verified versions. Transport level security is concise and simple so that it is applied consistently.

Finishing Up

OT networks run most of the world's most critical infrastructure and make some of the juiciest targets for bad actors. Cyber- security continues to be a battle, and one usually requiring many layers of defense-in-depth. This paper has toured a variety of possible attack vectors and how OPN Connect is architected from the ground up to minimize the attack surface. This allows it to be deployed as a transport in its own right, or as an overly to an existing conventional network. This further increases security and defends systems against mis-configurations and vulnerabilities that may creep in over time. In so doing, it provides an easy way to substantially move a system towards zero trust with minimal overhead.

OPN Connect has been extensively validated by third parties, and currently securely connects over 10 GW of generation capacity in the United States. In 2021 the US Department of Energy published the Solar Futures Study report[3], calling Operant's technology 'potentially game changing' in the category of cyber-security solutions required to transition the US electric grid to distributed renewables while also protecting national security.

For a more in-depth discussion of our solution and its security, contact us

[3] https://www.energy.gov/sites/default/files/2021-09/Solar%20Futures%20Study.pdf

Operant Networks, Inc.
1500 Valley House Dr
Suite 210, Office 151
Rohnert Park, CA 94928
contact@operantnetworks.com