seclāb

Electronic Air Gap by Seclab

THE BEST WAY TO PROTECT YOUR OT NETWORK

WHITE PAPER • 2020

The Problem

In most industrial or transportation organizations, there is no dispute that the Operational Technology (OT) network needs to be "locked down" to a much greater degree than the IT network. This is partly because uptime is of critical importance for OT systems, and also because OT systems tend to be older and more "fragile". Small anomalies that wouldn't faze an IT system can bring an OT system to its knees.

However, it seems the users who call for greater security for the OT network are the same ones that clamor for more access to OT systems – from the IT network, of course. Engineers and other IT network users all need to get data from, and make adjustments to, OT systems. They would like nothing better than to eliminate a SIl separation between the two networks – provided, of course, that at the same time you lock down the OT network better than Fort Knox. How can you help these people do their jobs, without compromising security on the OT network?

Of course, the security technology that most organizations deploy first is firewalls. At first, they may seem like the perfect solution. All you have to do is make sure you close off all access to the OT network except what is absolutely needed. What can possibly go wrong if you do that?

Here's what can go wrong:

1. Firewalls networks run software, and like any other software, it can be hacked.
2. Configuration errors seem to be more the rule than the exception.
3. Firewall technicians are under constant pressure not to do anything that might result in an important power user not being able to finish a critical project because he or she couldn't reach the system they needed to reach.
4. Vendors always want as much access as possible for their systems – big, wide-open port ranges, etc. Your firewall begins to look like the Swiss cheese you had on your sandwich at lunch.

However, you probably heard a long time ago that there is a better way to protect your OT environment – data diodes. Data diode vendors can truthfully say that they protect against any and all attacks from your IT into your OT network. They can say this because a data diode doesn't let in any traffic at all. It's hard to beat that level of protection, isn't it?

But what does it cost? And by this we mean the productivity cost, as users who are used to real-time, bi-directional interaction with OT systems - using protocols like Modbus – suddenly realize they will need to physically go up to the systems they're used to using from their IT network desktop or laptop in order to accomplish the same result. And if they're out of
town and need to do this, well….good luck!

When these users complain to you, you of course patiently point out to them that what they're asking for is impossible: There is no way that you can provide real-time bi-directional communications sessions from outside the OT network, at the same time that you provide the highest level of security against any and all attacks from the IT network into the OT network. What they're asking for is like squaring the circle or inventing a perpetual motion machine; it simply can't be done.

Or can it? Have you considered the possibility that you could protect your OT network against all network attacks to the same degree as data diodes do – yet at the same time enable full bi-directional communications with almost all systems on the OT network? Could this be possible?

The Solution

We can assure you it is possible; moreover, we can assure you there are lots of users of this technology now in Europe. The technology is called Electronic Air Gap, and the product is called Secure Xchange™. **The robustness of our solution has been proven by our customers using the most sophisticated test systems, including those used by NATO.**

Secure Xchange allows you to give your users full bi-directional communications between systems on the IT and OT networks, while at the same time providing the same total protection against network-layer attacks that the data diode vendors provide.

Secure Xchange Network™
By Seclab

How do we do this? If you're familiar with the seven-layer OSI model, you may know that the great majority of cyberattacks are propagated through layers 3 and 4, the Network and Transport layers respectively. Attacks like Stuxnet, Black Energy, Wannacry, NotPetya, CrashOverride, etc. all rely on these two layers to spread themselves. No matter how devastating their "payloads" are, without having access to the Network and Transport layers, these attacks simply can't cause damage.

Secure Xchange is built on an important technology called Secure Transport. There are three separate processes going on in Secure Transport. They are implemented on three separate circuit boards within the Secure Xchange device.

1. In the first process, each IP packet coming from the IT network is stripped of layers 1 through 4. This leaves only the "payload": layers 5 (Presentation) and 7 (Application).
2. The second process passes the payload through to the third process, without any layer 1-4 information.
3. In the third process, layers 1-4 are rebuilt – without any malicious code that may have been in them originally. Layers 5 and 7 from the original packet are added to the rebuilt layers 1-4; the entire packet is passed on to the OT network.

Because Secure Transport destroys then recreates the entire layers 1-4 of every IP packet, Secure Xchange makes it physically impossible for any Network or Transport-layer attack to pass into the OT network. At the same time, Secure Transport allows layers 5 and 7 of each packet to pass through unimpeded, so there is no change at all to the payload of the packet. This means that engineers won't need to change how they use the applications, databases and protocols on the OT network – because they will still be using them in their full native capabilities. However, the OT network will now have the highest level of protection against network cyberattacks.

Besides blocking network cyberattacks, there is another important benefit of using Secure Xchange to protect your OT network: With Secure Xchange "in front of" your OT network, any potential attackers who may have penetrated your IT network and are performing reconnaissance will never be able to "see" any information about your OT network; in fact, the entire network will be invisible to network scanning tools. What you can't see, you can't attack!

Protecting Against Application-Layer Attacks

The vast majority of cyberattacks are conducted through the Network and Transport layers of the IP protocol (layers 3 and 4, respectively); these will all be blocked by the Secure Transport technology described above. However, there are some attacks that utilize the Application layer (layer 7). How can these be blocked? You can do this in Secure Xchange using two methods.

The first method is Direction Control. Even though Secure Xchange allows secure bi-directional communications between the IT and OT networks, you can still control the network from which a communication has to be initiated, for any particular protocol, database or application. For example, if you want to limit all Modbus sessions to being initiated from the OT side, you can do that. Once the session has been initiated, it will be truly bi-directional, but having Direction Control is a powerful tool to prevent attacks into your OT network that originate in your IT network.

In cases where using Direction Control isn't possible, the second method utilized by some Secure Xchange customers is to implement an Application-layer firewall in line with their Secure Xchange device. The Application-layer firewall can be configured to block known attacks on the particular applications, databases and protocols found on your OT network.

Which Applications Work?

If you are familiar with data diode solutions, you know that the big question when implementing one of these is: "Will we be able to use the applications, databases and protocols on the OT network after we have implemented the data diode? And if so, how will we be able to do it?" This is because, with all access from the IT to the OT network completely cut off, there are literally zero applications, databases or protocols on the OT network that will be directly accessible from the IT network, since they all require interactive access to work in their native mode.

When a data diode is in place, for any application, database or protocol to be accessible to IT users, there needs to be some special application to make it possible. For example, a database on the OT network can be replicated to the IT network, making it accessible there. Replication works fairly well with databases, since there shouldn't normally be a need to write to an OT database from the IT network. However, for most other applications, and especially for protocols like Modbus, it is impossible to "replicate" them; the user will need to directly attach to the OT network in order to use one of these.

These concerns don't apply with Secure Xchange. Because Secure Xchange passes layer 5 and 7 information from each packet directly onto the OT network (while destroying and then rebuilding layers 1-4), almost all applications, databases and protocols will work securely without any change, or without having to deploy a special replication application. In the very few cases where there could be a problem, Seclab will work with the customer to resolve it; the few issues that have been discovered so far have been quickly resolved.

SECLAB_

WWW.SECLAB-SECURITY.COM