

Keeping the Hacker/Attacker off the Factory Floor/Network, by Cris DeWitt, CISSP

As access to manufacturing data extends deeper into the manufacturing environment, countermeasures must be implemented to preserve or improve information security within the walls of the factory. The malicious activities of a few or the oblivious activities of many jeopardize the productivity of the organization and as such, a “defense in depth” approach must be implemented. Like an onion.

The majority of vulnerabilities are made possible by a small number of services running on the host operating system. Recently, the acceptance of “remote access” to manufacturing floor tools and data opens up many of these vulnerabilities. For example, when an OEM is allowed remote access into the client manufacturing network, what security policies apply? What can run/not run? Do we adhere to the policies of the OEM or the policies of the manufacturer? Is the host allowed on the network without antivirus controls? What stops this host from connecting if there aren’t any antivirus controls? The core of the onion is vulnerable!

Sound scary? How about this factoid – I know a security practitioner that has a “collection” of approximately 700 known trojan programs, but only about 300 are detected by the mainstream antivirus software providers! (Couldn’t he collect coins or butterflies?). The point is that if commercial antivirus/antimalware software is missing over half of a known list of malware, how can you protect your factory?

Without a defense in depth strategy, your network and its data might be compromised. By trying to improve the factory efficiencies (via remote access or equivalent), we might be doing more harm than good – unless we understand and implement some simple security practices.

Defense in depth

A defense in depth strategy is like an onion – an onion grows many layers of material to protect the core. The lifeblood of the factory consists of sensitive/critical systems and must be protected in a similar manner. An effective security practice is to develop protection mechanisms in layers. An attacker has to figure out how to compromise each layer. Too many layers and the attacker will go elsewhere. Remember, you have to try to protect everything, but the attacker only has to subvert a few controls. Attackers are like lightning – they choose the path of least resistance.

Ok, what to do?

First, identify who will support your security mission in terms of funding and evangelism and make them part of your team. You must have a benefactor and they should be high enough in the corporate food chain to place the security effort on the “critical” agenda. A factory manager is good, but the CFO would be ideal.

Policies

Review your policies and see if they are actually enforced. What? No policies? Get some – start with a decent Use Policy and quickly go to a Password Policy that implements “strong” passwords. Sure it’s tough to keep up with them and who wants to tell the CEO his 4 character, birthday of his dog isn’t enough? Password cracking and brute-forcing are simple measures for an attacker. Computers have enhanced the attacker’s capability to a high degree.

Training

Train your users. Few people like to be told to do something without understanding the “why” of the task. A training and awareness program is the best money spent in security. Like the recent slogan for the U.S. Army – an Army of One, caters to the power of many empowered, trained individuals fighting for the same cause. Enlist the corporation - awareness is curative.

Identify Critical Manufacturing Systems

Next, identify your critical systems. A good place to start is identifying the systems that “print the money”. That is, the systems that are the most valuable to the manufacturing operation. Have you ever been in the factory when a critical system is down? The one where the operators stand around waiting for the “system” to come back up? That’s a critical system! In



semiconductor manufacturing, the manufacturing execution system (MES) controls recipes, work in progress, and manufacturing scheduling... The MES is the “heart” of the factory . Without access to the MES, other systems die.

Hardening

While hardening your critical systems by implementing vendor patches, shutting down unnecessary ports/services, take a look at what systems they interact with and how – message busses, accounting feeds, remote access...all must be comprehended and at many layers. Hardening isn’t a one-time event. Be prepared to patch, patch the patches and patch the patch patches! It’s easy to tell someone to “turn off services that are unnecessary”, but don’t underestimate this task. It’s hard work and time consuming to know what services are necessary. Shutting off the wrong port or service can shut the factory down! Lastly, add security elements to your test plans.

Encryption, Authentication

Encrypt communications! With the current computing horsepower, it’s not too much of a performance hit to encrypt communications. Key/certificate exchange is very robust and the current de facto standard for encryption (AES) is stout enough for the U.S. government to approve. From a coding standpoint, all communications should authenticate with any other host or service. And while you’re at it, get your certificates from a trusted authority. We recently performed a penetration test on a “secure” system, and in the first hour of testing faked a certificate that allowed us to see critical information in clear text. All of the tools used in this particular attack were widely available, for free, on the Internet!

Watch the border

Most papers on network security start with the perimeter devices like border routers, firewalls, etc. However, the manufacturing network should be designed from the inside out (remember the onion). The critical systems mostly rely on internally accessible services (today) so spend your time on the internal infrastructure first, and then branch outward. As the factory evolves into a more highly integrated “printer driver” for products, the border will need more attention. Just look at the adoption rate for web services and you’ll see what I mean. While you are building compartmentalized networks (by supplier for example), implementing role-base authentication and similar enterprise infrastructure. Be sure to come up with a log monitoring solution as well. The ability to peer into the logs of many devices is an excellent way to detect an attack or identify broad themes of insecurity.

Trust but verify

It’s not prudent to trust that what you have designed and built is actually secure just because you say so. Periodic testing by a third party will verify the risk you are assuming. Testing can be the validation of a specification (your network security policy, design, supplier specs...), an industry standard (as is the case with Device Net, ISO17799 or SEMI standards) or of a regulation (Sarbanes-Oxley, SEC 17a, NASD...)

Be prepared, to budget for periodic testing over the long haul. Penetration and vulnerability testing every 6 months is typical for manufacturing environments. The good news is that the tools used in this arena are becoming more robust and competitive pressures are causing the prices of this service to fall. We use a tool for a portion of our testing that automatically performs an entire attack. This allows our specialists to spend the bulk of their time on the complicated targets (like an advanced process control scenario) while automating the task of identifying “easy” targets and reporting remediation steps.

Social engineering testing is worthwhile in facilities where policy compliance is low or turnover is high. Social engineering test results are usually the most enlightening and the remediation costs are low.

And in conclusion

Manufacturing networks are different than an e-business or retail business network. There are intellectual property sharing issues (but you gotta do it!), production uptime requirements that are 24x7 and a slew of very different hosts running the operation. To secure these networks, a “manufacturing” approach to everything from policies, to training, to the network design, to the protocol usage, to the access controls, to testing... is essential.

Not sure where this fits, but...



It's sometimes difficult to understand what is happening on a single host at the network layer (and below). Sniffers require some setup time and assuredly some serious knowledge about packet structure. Some new tools are available that pop-up a warning when ports are scanned or applications are trying to communicate with hosts outside the host network. Most warnings are benign, but with advancing capabilities of trojans in particular, these "flags" might alert the system owner to malicious activity. I highly recommend the use of these tools, especially in the R&D environments. That way, when your copy-exact strategy is deployed, you'll lessen the risk of exposure to these threats.

About the author:

Mr. DeWitt is a 15 year veteran of the semiconductor manufacturing industry. He has architected the networks of several world-class manufacturing facilities and is the former Divisional CIO of a publicly traded manufacturing company. Mr. DeWitt currently is the CSO of In-Depth Security - experts in security, IT deployment, and training. His current interests are in compliance issues, discrete industry standards, and agile implementation techniques.

Cris DeWitt,
CSO, In-Depth Security
www.indepthsec.com