Securing your Supply Chain

THE RFID NETWORK

Some people don't understand how critical it is to secure their supply chain. After all, for most companies, it's not as if lives are put on the line if their competitors get unauthorized access to the supply chain, right?

But securing your supply chain is critical. If you don't, a competitor can exploit weaknesses and steal some of your customers. Just ask yourself, what would happen if one of your competitors were able to access your prices by using one of your customers' systems? They could set their prices lower than yours and grab part of your market.

Companies need to secure their own systems and ensure their trading partners are doing so as well. Before you roll out RFID throughout your supply chain, you need to understand the potential security risks and how to reduce vulnerabilities. After all, your confidential information is only as secure as the weakest link.

In a complete RFID solution, there are multiple layers, and each layer needs to be secured individually. The secured layers work together to further secure the entire system. Let's examine the layers.

At the top, you can find the server-layer that stores the supply chain data. Most companies already have these systems in place, and they're fairly well locked down. If you're using the new servers on the block that are part of the EPC Information Services (EPCIS) to link consumers to companies, make sure to properly secure

them as well. The object name server (ONS) part of the EPCIS sits on the Internet and may provide product information to consumers.

Your trading partners, which can include retailers, third-party logistics companies and transportation companies, may need to access the ONS for additional, non-consumer-related information, such as authorized dealerships and service history. Both users and servers should be using SSL certificates for authentication purposes. If you're not familiar with SSL certificates, it's an Internet standard that helps ensure you are who you say you are. (For more information on EPCIS, please see An Introduction to EPCIS *[1]*.)

The next layer is the RFID reader layer. RFID readers are network devices and, like all other devices on your corporate network, they need to be secured. Substitute the word "reader" for "router," and you get the idea. Would you want an unsecured wireless router on your network?

Readers provide critical information about corporate assets. Companies need to ensure that the readers on the network really are theirs and not "rogue readers," which are unauthorized readers connected to their corporate network or that exist within their facilities. These may be physical devices or even software reader emulators that report false information. Virtual readers could simulate the behavior of a physical reader and add false information to your network. The primary solution is to use embedded certificates on reader devices the same way that servers use SSL certificates.

The lowest layer is the RFID tags. Beware of a couple of possible weak spots that may be exploited by your enemies. The first is the RF conversation between tag and reader. The conversations between reader and tag may occur via open or secure conversations. Most of the passive and active RFID tags on the market today do not communicate through secured conversations. That means a listening device within range tuned to the proper frequency can record the conversation between tags and readers. All of the signal information would have to deciphered, which would be extremely complex in environments with numerous readers and tags.

Although this scenario is not likely, it is a serious concern for some and must be addressed. Gen II tags have a 32-bit access password. If this password is set, then the reader must have the valid password before the tag engages in a secured data exchange. This password also prevents unauthorized people from scanning an area to see what products are there. For example, someone may scan the tagged contents of a wooden trailer to see if it's worth breaking into.

It's also important to restrict unauthorized access to tag memory on applied tags. You don't want someone to reprogram your RFID tags after they've been applied. Some of the most secure RFID tags on the market meet the ISO 14443 standard. The tag memory contents may be divided up into segments. Each segment can require a different password to access. Gen II tag contents may be locked. The lock command allows a reader to lock individual passwords or individual memory banks. For manufacturers that want to ensure certain information remains on the tag for the life of the product, a perma-lock feature makes it impossible to alter the

contents.

How Secured Layers Work Together

Once secured, all of these parts work together: A serialized RFID tag on products makes every item unique. An authenticated user accessing an authenticated server permits the user to retrieve information to the specific product in hand. Date of manufacture, expiration date, product instructions, etc. all can be retrieved from the manufacturer's EPCIS server. This process nearly eliminates the possibility of tag forgery and counterfeit products. The manufacturer's EPCIS server can even tell you if you're purchasing a product from the company authorized to sell it to you.

Here's how these security measures can improve business. Manufacturers that resell through only authorized dealers are very concerned about their products showing up on the gray market. This occurs when an authorized dealer purchases higher quantities than they really need in order to obtain greater discounts. The surplus product is then resold to non-authorized retailers.

People we spoke to at one company were distressed because they had no way to know how pallets of their high-end, contractor-grade power drills turned up at a local club store. There was no agreement in place with the club store, and the units were being sold at prices lower than their authorized dealers. With serialized RFID tags, the manufacturer can purchase one of the drills from the club store and trace the unit to the dealer that first purchased it. The manufacturer can then ask questions about how the product found its way to the unauthorized retailer.

For more information, please visit www.rfidwizards.com *[2].*

Copyright 2011; RFIDwizards.com; All Rights Reserved

Source URL (retrieved on *03/12/2014 - 5:26pm*):
http://www.chem.info/articles/2011/07/securing-your-supply-chain

Links:
[1] http://rfid.net/basics/147-the-internet-of-things-an-introduction-to-epcis
[2] http://www.rfidwizards.com/