Taking a First Step

Cyber Security on Video Surveillance Systems

A Razberi Whitepaper

April 12, 2015

Executive Summary

Securing the network used for video cameras is an increasingly important system design consideration, especially if you recognize just how often hackers seem to be infiltrating network systems of big and small businesses alike.

It's a looming issue that seriously affects the security industry.

Unfortunately for most installers, addressing this issue often requires a detailed understanding of network operation and a labor intensive process to fully address the potential problem.

Why CCTV can be the open door for a hacker

In late 2013, Target confirmed their credit card systems were hacked. Up to 40 million credit card accounts were compromised and personal data for 70 million customers was stolen.

Not only did Target take a hit in consumer confidence, but they also had to pay $148 million, *after* insurance, for the cost of the hack in the second quarter of 2014.[1]

As it turns out, hackers gained access through a connection to the network used by a third party HVAC contractor for an electronic billing system. Using that interface, the hackers were able to download malicious software to all of Target's point of sale registers and capture consumer credit card information.

The Target break-in is a reminder of the potential cost and consequences of hackers getting behind your firewall and on to the corporate network. While the Target POS network should never have been accessible from an HVAC system, this incident makes it clear that even a sophisticated company with significant network security in place, can make mistakes.

One layer of security is simply not enough.

In the world of network video and network security, we are often playing with fire and may not even realize it. When we place cameras both inside and outside of a building, we know that unplugging any of those cameras and plugging in a laptop should not allow ANY sort of connection to the network. And yet, it is also well known that the vast majority of the time, those LAN connections will allow communications to the camera network and often directly to the corporate network.

[1] Tom Gara, 'An Expensive Hack Attack: Target's $148 Million Breach', *Wall Street Journal*, (published online 05 Aug 2014) <http://blogs.wsj.com/corporate-intelligence/2014/08/05/an-expensive-hack-attack-targets-148-million-breach>accessed 07 Apr 2015.

In fact, connecting a rogue wireless access point between a camera and the network will often allow full access to anyone close enough to the building to do a WiFi connection, and yet not interfere with the camera's normal operation.

While there are hundreds of things a sharp IT guy can do to tighten the security on the camera connections, the truth is that a constant waterfall of urgent items in our professional lives often causes these sort of preventative measures to fall off the to-do list. Even initially well protected and isolated "camera only" networks can suffer security holes brought about by unintended connections that bridge to the main corporate network.

As the installers of CCTV cameras, our industry has a lot to lose if the next big "Target" break-in is facilitated by an IP camera connection.

Blaming the consequences on a network administrator's failure to secure the network is not likely to prevent the inevitable prohibition of network cameras that will likely result from risk averse video users.

What can we do?

Insisting on a system design that includes a virtual or physical dedicated camera network is a good place to start, but it's not a total solution by itself. As security system designers and installers, we need to include additional layers of security -- layers that we can add ourselves easily and economically.

There are technologies, such as 802.1x, which provide secure connections to client cameras. Unfortunately, this technology requires a significant labor investment to create digital certificates for each camera, load them individually to the cameras, configure the switch, and install and configure a special server to control permissions. This labor intensive procedure may be appropriate on a very large system, but it may not be affordable on small or medium size systems.

There is a technology built in to most switches called MAC address binding or Port Security. By configuring the cameras MAC address into the switch, each port on the switch will be limited to connecting only to the authorized camera. All other connections will be refused.

This adds considerably to the difficulty of hacking this port with a laptop since the MAC address must be known, but it also adds a maintenance workload since all of those camera MAC addresses need to be manually gathered and entered. They also need to be disabled for maintenance, and changed if a camera is replaced.

There has to be an easier way

At Razberi, we're convinced that if security is difficult and labor intensive to implement, the majority of people will not go through the effort to make it a priority.

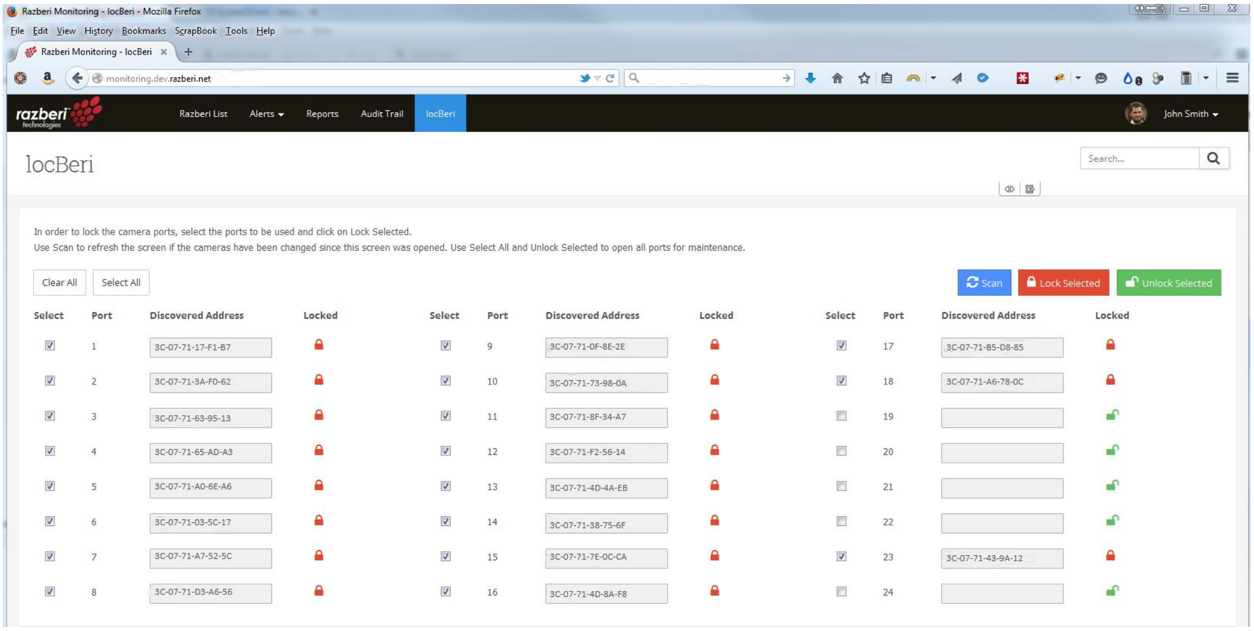
Simple is the answer.

That's why we've introduced a way to lock the ports on a switch with the push of a single button.

Our LocBeri feature scans the attached cameras and then automatically configures the switch so only those cameras work on those ports.

Need to do maintenance or change a camera?

One button push will unlock all of the ports, then simply relock when you're done.


Razberi Monitoring - locBeri - Mozilla Firefox
File Edit View History Bookmarks ScrapBook Tools Help
Razberi Monitoring - locBeri
monitoring.dev.razberi.net
razberi technologies
Razberi List
Alerts
Reports
Audit Trail
locBeri
John Smith
Search...

locBeri

In order to lock the camera ports, select the ports to be used and click on Lock Selected.
Use Scan to refresh the screen if the cameras have been changed since this screen was opened. Use Select All and Unlock Selected to open all ports for maintenance.

Clear All
Select All
Scan
Lock Selected
Unlock Selected

Select	Port	Discovered Address	Locked	Select	Port	Discovered Address	Locked	Select	Port	Discovered Address	Locked
☑	1	3C-07-71-17-F1-B7	🔒	☑	9	3C-07-71-0F-8E-2E	🔒	☑	17	3C-07-71-B5-D8-85	🔒
☑	2	3C-07-71-3A-F0-62	🔒	☑	10	3C-07-71-73-98-0A	🔒	☑	18	3C-07-71-A6-78-0C	🔒
☑	3	3C-07-71-63-95-13	🔒	☑	11	3C-07-71-8F-34-A7	🔒	□	19		🔓
☑	4	3C-07-71-65-AD-A3	🔒	☑	12	3C-07-71-F2-56-14	🔒	□	20		🔓
☑	5	3C-07-71-A0-6E-A6	🔒	☑	13	3C-07-71-4D-4A-EB	🔒	□	21		🔓
☑	6	3C-07-71-03-5C-17	🔒	☑	14	3C-07-71-38-75-6F	🔒	□	22		🔓
☑	7	3C-07-71-A7-52-5C	🔒	☑	15	3C-07-71-7E-0C-CA	🔒	☑	23	3C-07-71-43-9A-12	🔒
☑	8	3C-07-71-D3-A6-56	🔒	☑	16	3C-07-71-4D-8A-F8	🔒	□	24		🔓

One Screen... One Click... Done.

Conclusion

Good security starts with small simple steps in the right direction. That’s why razberi™ has added LocBeri as a standard new feature on all of our appliances. LocBeri allows you to add to the security of your IP video installation with the ease of a simple button push. Cameras and switch ports are bound together in a way that makes it much harder to use the port for anything other than the intended camera.

Simple to activate and easy to maintain, LocBeri makes your video installations more secure without the pain of previous complex solutions.

For more information, visit us at: http://www.razberi.net/locberi

About Razberi Technologies

Razberi Technologies is a developer and manufacturer of network video solutions for professional video surveillance and security applications. The company is an innovator in providing ground-breaking solutions designed for simplicity and ease-of-use. Razberi Technologies offers a full range of plug-and-play network recorders designed for use with VMS software from a wide variety of industry leading developers. The company’s flagship product is the patented razberi™ ServerSwitch™ that combines the functions of a network video recorder and Ethernet Smart Switch into a single compact appliance. Razberi Technologies is a privately-held corporation based in Farmers Branch, Texas, a part of the Dallas / Fort Worth metroplex.

Razberi Technologies Inc.
13755 Hutton Dr, Suite 500
Farmers Branch, Texas 75234

phone: 469-828-3380