Micro Local™ Cameras – Best Practices

By Dan Desjardins – Director/Owner Videstra LLC
With contribution from Michael Funk – Corporate Director of Information Technologies Quincy Media Inc.

With an investment in one or more Micro Local cameras (Skycams, WxCams, etc) there are going to be some high expectations from viewers and station management. Adding reliability and security to these cameras doesn't have to be complicated. There are a few things you can do to make sure your teams get everything they expect from your investment by following a few suggestions we will present in a series of articles called:

Best Practices - Camera Installation/Camera Security

Work with your IT Department

A big thanks to Michael Funk, Corporate Director of IT at Quincy Media for his contributions to this whitepaper. Michael runs a tight ship overseeing network security for the 16 Quincy media stations as well as its corporate offices and print operations and many of QMI best practices are reflected here.

I can't stress this enough. Attempting to work around (or against the advice of) your IT department to enable *or bypass* security creates risk and will often result in:

- Loss of trust
- Loss of security
- Loss of employment

Network security is a *non-optional* element of today's IT infrastructure. Attacks on networks occur *hourly* – in fact, it's guaranteed your network is under attack as you are reading this article. The only reason it's failing is because your IT department has safeguarded it!

Many Ways Cameras are Connected

Your cameras may be connected in one of a few ways

- From within your corporate network
- VIA VPN over the public Internet
- As a device located directly on a public IP Address

If a camera lives *inside* your firewall, then all necessary security is likely in-place and managed by your IT department. This article is not targeted for cameras inside your corporate firewall.
The same is true for cameras accessed via VPN as that is essentially the same as them being inside your corporate network – again being managed by your IT department.

Cameras Outside the Corporate Firewall

Cameras located directly on the Internet at public IP Addresses are where you MUST make sure you have set up enough security protocols to keep them out of the hands of bad actors.
Here's how…

Install a Router

While you *can* connect a camera directly to your ISP modem, we don't recommend it. When connected directly to the modem the cameras IP address becomes the public facing IP address. There is no firewall. Instead we strongly suggest you put a small business router (such as the Cisco RV340) between the modem and camera. You can find extensive information about this in our previous white paper: Camera Installation and Deployment. In addition to providing a firewall, a router lets you do much more.

- IP Filtering
- Dynamic DNS (if the remote site does not have a fixed IP Address)
- Enable basic firewall security measures against a wide variety of attacks
- Safely implement ICMP for pinging – or turn off pinging entirely for "stealth mode"

At less than $300, the additional expense and equipment are not an issue if you follow our recommended best practices in the above white paper. Many of the security suggestions that follow may depend upon having a router managing your camera.

Camera Are Not Set and Forget Devices

With both budget constraints and limited personnel, it would be nice if cameras were set-and-forget devices. They are not. While there is no need to babysit them – you should make it a point to check for firmware updates around once per quarter. You should check with Videstra (or other vendor if you are not using Videstra to manage your Micro Local cameras) before doing updates. It's worth noting that most camera firmware updates are for security reasons and *rarely* change established functionality. Michael Funk puts it this way: *"[Cameras] Like all IoT devices, need love, care, and attention."*

It's About the Payload

Bad actors who try to access your cameras typically want one or more of the following things:

- To turn your camera's Operating System into a DoS (Denial of Service) slave
- To add your camera to their add-supported web site
- To harvest information about your logon/activity to gain access to your, or other networks
- Much like vandals who spray paint walls and bridges – bad actors will often do damage *just for fun and recognition from fellow miscreants*

What the hacker wants is called his/her *payload*. The good news: for Micro Local cameras the payload is typically small – and therefore we don't see wholesale attacks. Cameras are typically isolated devices, separated from the networks they serve, with little to offer in terms of a real payload. That being said – the fact that you use one or more of them every day in your broadcast means passwords, usernames, etc. are flying back and forth over a generally *insecure* http protocol.

HTTP is Intrinsically Insecure

Almost all cameras use http access to log-on and manage their features. The familiar http (no 's') method of accessing a web page never has been secure. Today, nearly all web pages use https (which is secure). What's the difference? When you log on to a device that uses http, your username and password are sent as plain text over the Internet. Any hacker could capture it in real-time. The https protocol encrypts this information and makes it nearly impossible to access.

Many cameras do not support https. That is a sad reality, but there are other ways to secure these cameras. Videstra supports https on many cameras – including Axis, Sony, Truen and Bolin. Be aware that implementing https requires the installation of a certificate – which you can generate *for free* at https://letsencrypt.org/

Don't Make the Hackers Job Easy

Cameras use several protocols. The most common ones will be:

- http for Management and API Access (HLS video is on the same port as http)
- rtsp for h.264/h.265 streaming video access
- ftp for certain utilities (these are only supported by Axis cameras)
- srt Secure Reliable Transport

Each of these uses a network port and each has a default port. For http it is port 80, for rtsp it is port 554 and for FTP it is port 21. If you utilize srt (secure reliable transport) there is no default port – you choose one. You do not have to use default ports!

In fact, default ports are where all hackers begin their exploits. Moving these ports is a good idea. Here is what I typically recommend:

http/hls	**42080**
rtsp	**42554**
ftp	**42021**
srt	**42800 (only if srt is used)**

Simply add 42000 to the default ports. You can use any number you like, but I recommend it be consistent across all protocols. This means hackers will have to go through the process of probing every port on your system to find open ones. Once they find them it will not be clear which protocols are supported. As a matter of course, hackers are not typically even looking for *cameras* and in fact typically have no idea what class of device is on the other end of an open port. Moving away from default ports simply makes hacking significantly more difficult.

Open Ports

The above-mentioned ports *must be open for incoming traffic*. This is the only way to make connections *to* the camera(s). If you have *any* ports open, you are making an attack vector available to hackers. This is essentially a welcome mat for bad actors. At the very least, heed the advice above and do not use default ports.

Most IT managers loath open ports – and simply will not allow them on their corporate networks. It's less of an issue when the cameras are on a public IP address – located well outside corporate fences. That doesn't mean they are not a target though – and it is quite likely someone, somewhere, will try to hack your camera(s).

Passwords

One important step is to use secure passwords. Your call letters, your channel number (e.g. WLPO55) are simply not good choices. I am not a fan of those randomly generated passwords that are impossible to remember but they should be strong enough to make it difficult to discover by trial-and-error. Here is a good article on how you can generate good passwords that are not insanely difficult to remember…

IP Filtering

This is the big one – and is possibly the single most powerful way to secure any device you place on the Internet.

IP Filtering is a simple way to tell a device what IP Addresses it will accept connections *from*. Whenever a connection request is made to a device the requestor must provide an IP Address to where any communications will be sent. It doesn't do any good to 'spoof' a connection address because the spoofed address doesn't belong to the spoofer – and thus communication cannot be established.

IP Filtering can be set up directly on Axis cameras, or on a router that you place at the remote site.

We recommend setting it up on a router.

An IP filter is a list IP address *from which* connections will be permitted. Although IP Filtering can usually be set to either Accept or Deny mode – we are talking strictly about "Accept" mode.

Think of an IP Filter like a big… hairy… ugly… bouncer. If you're not on his list – you will be denied entry. So – what IP Address do you allow? You must set the filter to allow the IP Address from which any legitimate request will be made. You may put several IP Addresses in the list. We suggest you put several that includes your main public facing IP Address and one or two "buddy" addresses.

Your main public facing IP Address can be determined by going to Google and entering 'What's my IP Address' after which you should double check with your IT department. If you put the wrong IP Address into the IP Filter you will need to go on-site to reset the equipment to factory defaults and start all over.

Buddy addresses are secondary and tertiary addresses from places you know to be safe. Make sure these are indeed *fixed* IP Addresses. If you put an IP Address in that is subject to change – that's going to be a problem – eventually.

Summary

It's likely one or more of your cameras will be located on public IP Addresses. This means someone, somewhere, without good intentions will try to access it. Installing a firewall is the first step and enabling IP Filtering is the second step to keep them out of harm's way.