



Boundless Security Systems, Inc.

sharper images with better access and easier installation

WHITE PAPER

Covert Wireless Video Surveillance using Network Cameras and a Cellular Internet Service Provider with Static IP Addresses is in Jeopardy of Cyber Attacks

Steve Morton, CEO, CTO; Boundless Security Systems, Inc.; July 17, 2006

Executive Summary

Covert video surveillance operations using network cameras and cellular Internet Service Providers with static IP addresses are gaining popularity because they're easy to deploy. However, such simple, wireless video surveillance systems not only suffer performance limitations and have limited geographic areas where they can be used, but can easily be compromised or even brought down by Cyber attacks.

This White Paper details the problems, and how Boundless, using a cellular ISP with dynamic public IP addresses, avoids them, and provides superior Cyber security and video performance, including the ability to economically handle far larger video surveillance operations.

Rationale for Using Static IP Addresses with Network Cameras

There's a simple reason why a covert agency would require a cellular Internet Service Provider with static IP addresses for use with the agency's network cameras. It's a software problem. It's because the use of static IP addresses is the only way the agency can provide any Cyber security, limited as it is, of their covert video surveillance operations using network cameras.

There's nothing inherently wrong with the cellular service itself that is provided by any particular carrier. In fact, cellular services have superior security compared to Wi-Fi networks. The problem is an agency's requirement for static public IP addresses for its network cameras.

A covert agency's requirement for static IP addresses is their Achilles' heel. Based primarily on that key requirement, combined with in-depth knowledge of communications systems, IP-video surveillance and Cyber security, it is possible to deduce not only the likely limits of an agency's video surveillance system, but also how to compromise or bring it down by Cyber attacks.

For information on Boundless' extensive expertise in this complex area, please see the 14-page White Paper, *Fundamental Problems in Current Digital Video Security Systems*, that was released in Sept 2004 in response to the 9-11 Commission Report. It's available on this link:

http://www.BoundlessS.com/documents/Boundless_White_Paper_Fundamental_Problems_in_Current_Systems_and_Boundless_Solution.pdf

I particularly call your attention to item 5, **Poor Cyber Security of the Video System**, in that White Paper, to which I've added some additional material below.

Limitations of Network Cameras with Cellular Communications

Network cameras, regardless of vendor, are designed for use on high speed, wired local area networks with a large amount of spare capacity, not a relatively slow speed, cellular link with highly variable capacity and whose capacity is easily entirely used by video.

While it is expedient to use network cameras and cellular communications with static IP addresses to remotely access live images from those cameras, one faces several serious problems with that approach. I will explain the problems, and how Boundless and a cellular ISP with dynamic IP addresses can:

- 1) avoid Cyber security problems,
- 2) provide superior video performance,
- 3) increase the number of cameras at each location,
- 4) increase the number of locations where the system can be used, and
- 5) perform surveillance more efficiently and thus save labor and increase the number of covert operations that can economically be performed simultaneously.

I will base my analysis of network cameras on products from Axis Communications of Sweden. Axis has the largest market share of network cameras according to the Frost & Sullivan market research firm. I will also assume that, to restrict remote access to video from the cameras, the web server within each network camera is password-protected and using the latest firmware.

1) Vulnerability of network cameras using a Cellular ISP with static IP addresses to Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks

Many network camera vendors offer a DDNS, dynamic domain name service, for use with their network cameras. This service enables a network camera to be connected to the Internet using a dynamic IP address. Each network camera requires its own dynamic IP address, thus one cellular link supports only one network camera. The DDNS service avoids the need to have a public, i.e., accessible on the Internet, static IP address for each camera.

However, any DDNS service has a database that has the dynamic IP address to access every camera. This requirement, especially from a foreign company, since most network camera vendors are foreign, is surely an unacceptable security risk to any covert agency. An agency can avoid this problem by using a static public IP address with every camera. Unfortunately, the use of static IP addresses solves some problems while creating Cyber-security problems.

In addition, the wireless modem that connects a network camera to a cellular network with static public IP addresses is also a security risk, due again to the use of a static IP address.

Using a static IP address makes any web site especially vulnerable to DoS and DDoS attacks. While there are four billion public static IP addresses in the world, only a relatively small group is assigned to a given cellular Internet Service Provider, and only a fraction of that group is

available for static IP addresses. Thus the choice of which static IP addresses are used by the covert agency's surveillance cameras is relatively small and could easily be found and attacked.

One need not have a static public IP address to have to endure Cyber attacks. Our experience with the use of dynamic public IP addresses with our ultra low bandwidth, **Multi-Stream Video Servers** that are exposed directly to the Internet is that each one receives about 10,000 malicious probes per month. These probes are of no consequence due to the high level of cyber security we provide in our equipment, in part because we do not operate HTTP and FTP servers, which are readily identifiable to Cyber attackers. The use of dynamic IP addresses is in fact a great asset in combating Cyber terrorists because the target, i.e., the IP address, keeps changing. In fact, the dynamic IP addresses provided by a cellular ISP change far more frequently than the dynamic IP addresses on the cable modem connections, giving even more protection.

Note: Boundless has a patent-pending technology called **Stealth Web Site** that goes even further in providing Cyber security, but I will not discuss it here.

Unfortunately for a covert agency, network cameras rely upon their internal web servers to communicate images and are thus far more detectable and vulnerable to Cyber terrorists. Again, it's not necessary for a Cyber terrorist to block the covert agency's use of video surveillance, or even to view the video, but merely to compromise the agency's efforts, a far easier task.

I believe that, with modest effort, it would be possible for a Cyber terrorist to determine the static IP addresses used by the covert agency for its network cameras. Even if the network cameras were password-protected, and the password had not been compromised, the network cameras could be rendered useless merely by the terrorists' repeatedly trying to login to them. The problem is that the bandwidth of a cellular communications channel is so low compared to that of a wired LAN that network cameras are designed for, excessive uplink and downlink traffic could be created by Cyber terrorists. Access to the video by the Cyber terrorists would not be required to compromise the covert agency's operation. *The operation could be compromised simply by the terrorists' blocking the covert agency's access to the video by hogging the limited cellular bandwidth by creating useless traffic.* It's 1,000 times easier to carry out a Denial of Service attack against a 100 Kbps cellular link than a 100 Mbps optical link.

In addition to bandwidth hogging, there are the usual Cyber terrorists' methods of blocking access, such as the Ping of Death, but any attacks are far easier due to the relatively low cellular bandwidth. In this case, it's the cellular communications channel, not the web server's CPU, that is most easily overloaded. However, low performance RISC processors are used in most network cameras, and they must perform many tasks including image acquisition from the image sensor, color space conversion, video compression, file system management, IP encapsulation, web server operation, and network communications. Thus any unwanted burden on the communications aspects of the network camera takes away its capacity for handling video.

2) Video compression constraints of network cameras using Cellular ISP

3G cellular communications speeds, even with EV-DO, regardless of carrier, are very slow compared to wired networks, vary with time, and vary widely from one location to another.

Cellular operation inside a building is often far inferior to outdoors due to the electromagnetic shielding and reflections provided within the building. Thus a covert agency's ability to deploy network cameras (I emphasize network cameras) via any cellular network is very limited.

As a result of these wireless communications problems, it's unlikely that video streaming with either UDP/IP or TCP/IP, and relatively efficient MPEG-4 compression from a network camera can be performed reliably using a cellular uplink. The network camera is most likely using relatively inefficient JPEG compression. (Motion JPEG offers little improvement over JPEG, since each frame is still compressed independently of other frames, rather than taking advantage, as does MPEG-4, of removing redundancy between frames.) A given JPEG image with TCP/IP will eventually be communicated perfectly if its communications do not take so long that the camera overwrites the image in its own memory before transmission of the image is completed. To avoid having broken images (a single image made from parts of several images), the camera's firmware must lock a given image once an external application opens it for sending. Unfortunately, this critical parameter is rarely specified by network camera vendors.

For frame rate calculations via a cellular network, I'll use Axis' figures of 30 KB to 40 KB per 640x480 frame. However, this file size for a single image represents compression of 40:1 to 30:1 -- so high that compression artifacts are likely to be excessive. Compression of 15:1 to 20:1 give better images but doubles the already-slow transmission times and halves the frame rates. Ignoring transmission protocols, which reduce the payload by about 10 to 15% and thus degrade performance further, the use of 40:1 to 30:1 compression and a wireless uplink of 50 Kbps gives only one frame every 5 to 6 seconds. An uplink of 100 Kbps gives only one frame every 2.5 to 3 seconds. At these low frame rates, one has only a series of snapshots, not video, and it's when images from only a single camera are carried by a given cellular wireless link.

Since recording is not done in most network cameras, the only way video from network cameras can be recorded is to send live video from the camera to a distant recording device via the wireless channel. If the data link only supports low data rates and thus low frame rates, e.g., one frame every several seconds, a great deal of activity will be missed in the recording. One should have frames per second, not seconds per frame. A person can easily walk past a doorway in one-half second, so a frame rate of at least several frames per second is required to see the person.

If MPEG-4, which is used in Boundless' system, could be used with network cameras with cellular links instead of JPEG, then the amount of data required per frame could be reduced by a factor of 3 to 5 or more depending on the amount of motion. The reason is that static, or minimally varying scenes require very little data with optimally configured MPEG-4, but require an endless series of nearly identical frames with JPEG. With the redundancy removal of MPEG-4, and thus its higher compression for comparable image quality than JPEG, a corresponding increase in frame rate can be obtained for a given amount of communications bandwidth.

Another problem occurs when multiple users connect to a given network camera at the same time for common viewing. Axis allows as many as 20 simultaneous users per camera. Ignoring the additional load on the camera's CPU for communications, which further degrades the camera's ability to handle video, the frame rate drops in proportion to the number of users due to

wireless bandwidth limitations. Thus with a 50 Kbps uplink and two users, the frame rate would drop from one frame every 5 to 6 seconds to one frame every 10 to 12 seconds.

The frame rate could be increased for a given amount of bandwidth by using images with lower resolution or higher amounts of compression, but image quality would suffer. However, low to medium resolution, with its reduced data rates, is ideal for situation assessment and monitoring, but is inadequate for forensics, which needs the highest resolution the camera provides, and the highest clarity (least amount of compression).

Boundless' Ultra Low Bandwidth, Digital Video Surveillance System

Boundless has developed a fully distributed, ultra low bandwidth, IP-based, multi-stream, digital video surveillance system that avoids these problems. Boundless' fully distributed, ultra low bandwidth, multi-stream technology is explained in several one-page drawings that are available on Boundless' web site.

Links to the drawings are:

http://www.BoundlessS.com/documents/Boundless_Wireless_Mobile_Video_Surveillance.pdf – mobile and portable use in vehicles, briefcases...

http://www.BoundlessS.com/documents/Boundless_Hybrid_DVR_NVR_Wireless_Video_Surveillance_System.pdf – distributed storage and Boundless' **Broadcast Servers** to send video streams to many users without burdening wireless uplinks

http://www.BoundlessS.com/documents/Boundless_Comparison_IP_Wireless_Video_Surveillance.pdf – comparison of conventional, bandwidth-intensive IP-video network cameras to Boundless' ultra low bandwidth, fully distributed system

http://www.BoundlessS.com/documents/Boundless_Skyconnect_Iridium_Video_Surveillance.pdf – Boundless' system for covert use with automated detection of events (user selectable motion in 128 zones), and Live Alerts. Replace the “Iridium” network by a faster, cellular network, and the Iridium modems by one or more, 3G cellular modems.

Some of Boundless' benefits to covert video surveillance applications via cellular networks are:

- 1) Boundless' ultra low bandwidth system operates where other systems can't because other systems require much higher wireless bandwidth, which isn't widely available
- 2) Boundless decouples the quality of live images from the quality of recorded images by recording sharp images local to the cameras, independent of the quality of live video, if any
- 3) Boundless continuously records images in its **Multi-Stream Video Servers**, local to the cameras, even when the wireless connection to the Internet is off, broken, slow or erratic
- 4) Boundless' system provides live and recorded images with multiple resolutions, frame rates, compression parameters and data rates simultaneously to meet competing imaging needs for situation assessment, monitoring and investigations / forensics

5) Boundless' system quickly and automatically re-establishes video communication despite dropouts in cellular signals with not only moving vehicles where video that was captured remotely is being viewed, both also with moving vehicles where video is being captured

6) Boundless enables the user to create streaming content in cell phone, Pocket PC, Standard Definition and High Definition (opt) resolutions and corresponding data rates using live and recorded video sources from the *Boundless Security System™*

7) Boundless' system is designed for the highest levels of Cyber security for highly sensitive covert operations

8) Boundless uses dynamic IP addresses to protect system operation from Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks, which can cripple conventional systems that only use static IP addresses

9) Boundless enables customers to operate their own secure, DDNS service using a Boundless *Name Server* in their own facility, rather than requiring the use of a vendor-owned and operated DDNS service that compromises knowledge of the IP addresses being used

10) Boundless' four-camera, *Multi-Stream Video Servers* optionally autonomously create encrypted VPN tunnels to Boundless' *Broadcast Servers* on the Internet as another level of Cyber security, making them invisible to malicious Cyber probes and enabling a single public IP address to handle as many as 192,000 cameras simultaneously

11) Boundless enables video surveillance sites using both static and dynamic IP addresses to be identified by name rather than IP addresses

12) Boundless records and quickly searches (one can search hours in seconds) recorded video for motion, with the selection of parameters for motion to be searched for being made after the video has already been recorded

13) Boundless' *Multi-Stream Video Servers* automatically detect user-selectable motion events and send notification of the events to remote users so they don't have to constantly monitor live video, making video surveillance with large numbers practical

14) Boundless optionally broadcasts live and recorded video to stationary and mobile forces with only a single load on the wireless uplink, using a variety of formats

15) Boundless provides simple, plug-and-play, end-to-end operation with little or no assistance needed from IT departments

Conclusion

A covert agency's video surveillance operations using network cameras and a cellular ISP with static IP addresses are at grave risk. Cyber terrorists can easily compromise, and shut down, the covert agency's video surveillance operations merely by overloading the wireless link. The use of Boundless' ultra low bandwidth, multi-stream, fully distributed, digital video surveillance system with Cyber invisibility and a cellular ISP with dynamic IP addresses avoids these problems. In addition, Boundless also provides superior video performance, both live and recorded video, multiple cameras at each site, and intelligent motion search and automated notification upon event, improving operational efficiency and enabling more, and more extensive, video surveillance operations to be carried out economically.