Secure Video Surveillance

Camera Shy

Unless your surveillance cameras are wired directly to a video board, they are notoriously insecure. We show you how to keep your cameras from being compromised. *By Kurt Seifried*

In issue 121, Marcel Gagné covered the basics of building a video surveillance system using Linux and Kmotion [1]. But, to build a really secure, scalable (with dozens or hundreds of cameras) system that can't be compromised easily by attackers, you'll need to do more. For starters, you'll probably need to ditch Kmotion and look at ZoneMinder instead, and you'll need to be very careful about the cameras you use.

Wired, Wireless, and IP

One of the biggest mistakes people make when they buy cameras for a surveillance system is selecting wireless cameras. Now, I see the advantages: They are really easy to install, and a power source usually is easily accessible. Also, running network cable can be a real pain – each cable that needs to be run to a camera can cost a hundred dollars or more. But, wireless cameras also have two tiny problems: They can be monitored (so people can see what you're seeing), and they are trivial to jam.

Most wireless cameras come in two flavors now: X10 and 802.11 (WiFi). The X10 cameras have very little security in most cases, and the video signal often is not encrypted. A good rule of thumb is: If the camera costs less than a few hundred bucks, the signal is likely not encrypted. Most WiFi-based cameras, however, now support WPA2, but your system is only as secure as your network passwords, so make sure they aren't easily guessed.

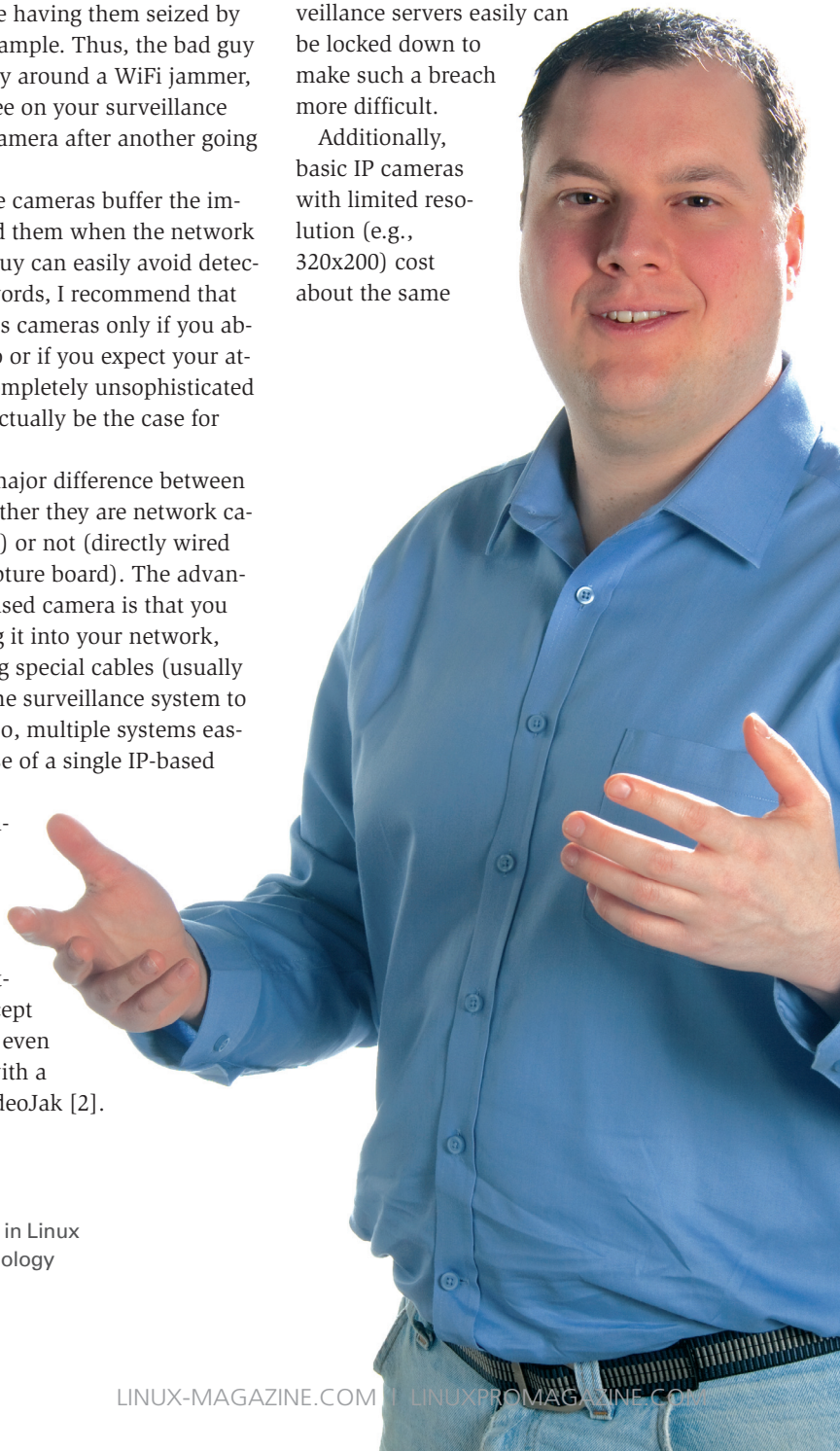
The jamming issue, on the other hand, is basically impossible to fix. You can buy a portable WiFi jammer for US$ 40 from a site like DealExtreme. And, although these devices often are illegal (because they interfere with wireless networks, oddly enough), I've never heard of anyone having them seized by customs, for example. Thus, the bad guy can simply carry around a WiFi jammer, and all you'll see on your surveillance system is one camera after another going offline.

So, unless the cameras buffer the images and resend them when the network is up, the bad guy can easily avoid detection. In other words, I recommend that you use wireless cameras only if you absolutely have to or if you expect your attackers to be completely unsophisticated (which might actually be the case for most of us).

The second major difference between cameras is whether they are network capable (IP based) or not (directly wired into a video capture board). The advantage of an IP-based camera is that you can simply plug it into your network, without running special cables (usually coaxial) from the surveillance system to the camera. Also, multiple systems easily can make use of a single IP-based camera.

The disadvantage to an IP-based camera is that an attacker with access to your network can intercept and monitor or even modify video with a tool such as VideoJak [2]. Non-IP-based cameras with a direct line to the surveillance system mean that attackers will have to compromise the surveillance server directly to get at the video information. Also, most video surveillance servers easily can be locked down to make such a breach more difficult.

Additionally, basic IP cameras with limited resolution (e.g., 320x200) cost about the same



KURT SEIFRIED

Kurt Seifried is an Information Security Consultant specializing in Linux and networks since 1996. He often wonders how it is that technology works on a large scale but often fails on a small scale.

as “dumb” but much higher quality wired cameras.

Live Video Modification

In films, the bad guys often break into a video surveillance system, record a loop of video with no events (i.e., an empty hallway or a bank vault with the jewels still inside), and feed that loop back to the system while they make off with the loot (only to have the video loop fail at some point, resulting in a really good chase sequence). Although this scenario is still possible, the technology is a lot more sophisticated. Until recently, you could usually assume that live video was a pretty good representation of the truth, but with modern technology, you can modify video in real time.

I recommend you pause here and check out the video at LiveLeak [3]. If you haven’t watched it yet, I’ll spoil it for you. Using a computer to modify the video signal, you can simply circle an object, and, presto, it disappears from the video feed. The craziest part of the video is when they “remove” an object on a counter in front of a mirror – you can still see the object in the mirror.

The technique used is quite simple and clever. The computer basically reduces the resolution of the object and its surroundings, then increases it, using video from around the object to recreate the space the object occupied. This technique works especially well on flat surfaces, such as a painted wall.

The kicker is that you can modify the video and feed it back out in less than 40ms. Assuming a standard 30 frames or so per second of video, this time period represents a two-frame delay, which very few systems will notice (network latency and jitter alone can easily account for 40ms). Even the use of cameras with secure digital signing probably won’t help much, because such systems are often flawed [4].

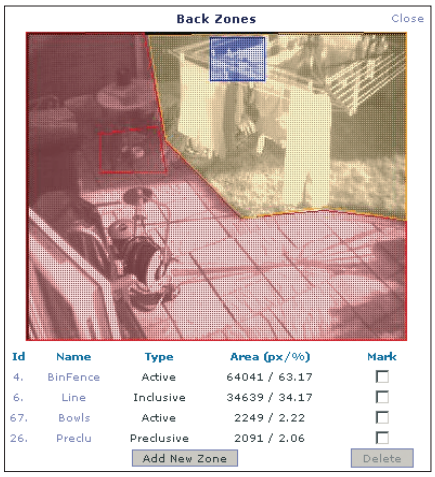


Figure 1: An example of zones in ZoneMinder surveillance. (Reprinted with permission from Philip Coombes)

In other words, unless you can prove that the video stream from the camera to the recording device is secure, you must be wary of trusting video evidence. Fortunately, again, most people caught doing bad things on video are not that sophisticated.

A ZoneMinder Primer

First, use cameras that are wired directly to a capture board running on a Linux server. ZoneMinder (Figure 1) [5] ships with most major distributions, so installation won’t be a problem. Configuration, however, might an issue because getting the settings right for your cameras can be tricky. I suggest using

```
xawtv -hwscan
```

to detect all local cameras [6].

Second, spend some quality time with the web interface and put in all your cameras. Then, you can decide whether you want to capture all video (set the camera to function *Monitor*) or only video when motion is detected (choose *Modetect*). Also, you can configure alerts in case motion is detected. ZoneMinder has a great interface for navigating historical events for one or more cameras. For all the details on ZoneMinder setup, visit the wiki [7], which includes distribution-specific guides.

Motion Detection and CPU Usage

One problem with using motion detection, however, is the amount of CPU time that you’re going to consume, especially if you have many cameras. One solution is to get a video capture board that does on-board motion detection, presenting the computer with pre-filtered footage. Unfortunately, such cards are not widely available. However, bluecherry [8], which sells a host of video capture cards guaranteed to work with ZoneMinder and provides open source drivers for their own boards, does have such a card coming to market soon. I tested a beta version, and it works pretty well, especially if you’re using a computer with limited CPU power or cooling issues.

Future of Surveillance

The future is here – which is both good, because some of the technology is very cool, and bad, because some is definitely open to abuse. New high-end systems not only detect motion but also analyze behavior (e.g., identifying people who are fighting, jumping over a turnstile in a subway station, or breaking into a car). Face and gait recognition are also becoming popular. These systems allow you to alert security automatically, for example, when people who have been banned show up on the premises.

In an Orwellian twist, some new camera systems can physically track individuals and identify and track groups of people, so you don’t need to hire someone to follow people, you can just let the computer do it. If this technology becomes widely deployed, who knows? Maybe large-brimmed hats will come back into fashion. ■■■

INFO

[1] “Webcams” by Marcel Gagné, *Linux Magazine*, December 2010, pp. 30-36

[2] VideoJak: *http://videojak.sourceforge.net/*

[3] LiveLeak: *http://www.liveleak.com/view?i=639_1288445821*

[4] Canon OSK-E3 is proved useless: *http://www.elcomsoft.com/canon.html?r1=pr&r2=canon*

[5] ZoneMinder: *http://www.zoneminder.com/*

[6] xawtv: *http://linux.bytesex.org/xawtv/*

[7] ZoneMinder main documentation: *http://www.zoneminder.com/wiki/index.php/Documentation*

[8] bluecherry: *http://bluecherry.net/*