SECURING
SMART
CITIES

Does CCTV put the public at risk of cyberattack?

How insecure surveillance technology is working against you

Vasili Hioureas

Junior Malware Analyst at Kaspersky Lab

Thomas Kinsey

Senior Engineer at Exigent Systems Inc.

INTRODUCTION

Late one night, a colleague and I decided it would be a good idea to climb up a public fountain in the middle of a city. Suddenly a disembodied voice from the heavens boomed out: "PLEASE GET DOWN FROM THE FOUNTAIN." We were shocked, until we noticed a number of cameras – complete with speakers attached – pointing to us from various lamp-posts in the city. This was the first time we'd ever felt so closely monitored so we decided to take a look at how the systems worked.

It is nothing new that police departments and governments have been surveilling citizens for years with the help of security cameras set up throughout various cities. These days most of us accept this as a fair tradeoff that we are willing to make, sacrificing a measure of privacy in the hope that it will keep us safer from criminals and terrorists. However, we also expect that our private data, in this case video feeds of our public life, will be handled responsibly and securely to ensure that this surveillance does not end up doing more harm than good.

In our recent research, we came across many cities that use wireless technology for their security cameras and infrastructure, rather than the hard-wired setups that were common in the past. This change makes things more cost and time effective for the city authorities.

Unfortunately, the problem is that right now wireless technology is not as secure as it could be. As security-conscious people, we instantly saw that handling data in this manner could potentially be vulnerable to a number of attacks, and so we started looking into whether these systems were implemented in a way that handled our data safely, or whether the data could be easily manipulated for malicious intent.

Although wireless technology itself can be vulnerable, there are still many additional improvements which can be implemented to add a sufficient level of security. Ideally, there should be many levels of security in place, so if a hacker clears one hurdle, he must then face a greater challenge at the next. However that was not the case in this instance.

RESEARCH

Our research started on the physical level: we traveled to various locations around the city, looking at how the hardware was set up, and finding the first sign that the city really had not put enough thought and effort into properly handing their own systems.

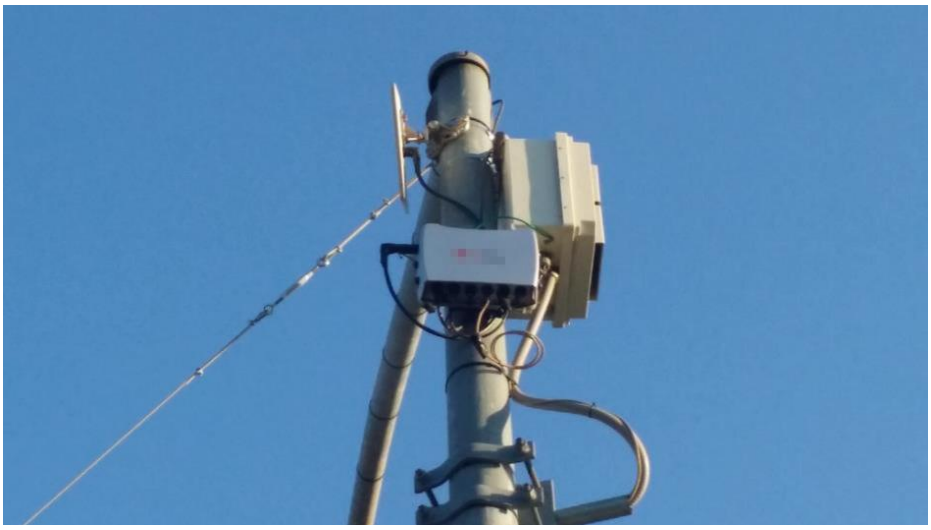

Figure 1: The security system

As the picture shows, the security system was set up in a sloppy way. The units that will be carrying our data have not been masked at all; on some units we could clearly see the name and model of the hardware needed in order to identify the devices and begin the research.

Why it is so important to protect the labeling of the hardware that you use? I will provide an example to help illustrate why this is such a major flaw. When there is a server that needs to be secured, a major factor in preventing it from being exploited is that the server binary is not publicly available. The reason for this is that if a researcher can get his hands on the binary, it can be reverse engineered and studied to find bugs and vulnerabilities. It is rare that a vulnerability can be discovered without being able to look at the code implementing the service. This is why not covering up the device labeling, seemingly a small mistake, actually has a massive effect.

Returning to the camera network: if a hacker was to crack the wireless security of these systems (which only implement your standard WEP or WPA wireless protections), he would at this point only be able to see unknown protocols, headers, and wireless packets with no reference to what system they belong to. In our analysis, we initially had no idea what software was generating these packets, as it is a proprietary system. Without getting our hands on the actual code, it would have been more or less impossible to reverse the protocol they use, which is really the only way to properly examine the network. At this point, our work was cut out for us.

Having obtained the hardware, we realized, despite the fact that the police department's setup was weak, the hardware they chose was actually not the problem at all. The mesh nodes were actually a very complex and well-made solution, and there are modules built into it to secure communications beyond the outlying wireless security. It just needed a sufficiently knowledgeable person to implement this technology and ensure it was properly set up. Unfortunately, having inspected many of the packets, we quickly realized that these encryption modules had not been set up and were not being implemented at all. Clear text data was being sent though the network for any observer who could join. There was no encryption to subvert, so we knew that it would just be a matter of recreating our own version of this software in order to manipulate the data traveling across it.

A quick comparison of how the mesh network works to transport video feeds will help give an understanding of what exactly we learned in order to manipulate the system. In a traditional Wi-Fi network, each device is typically connected to a router that serves as a central point. In order to send one piece of data to another part of the network, you would send it to that address, and it would travel via the router to the connected device. This works well in close proximity, but in order to be able to communicate over a long distance, the camera network used a topology and protocol that we will not name in this article.

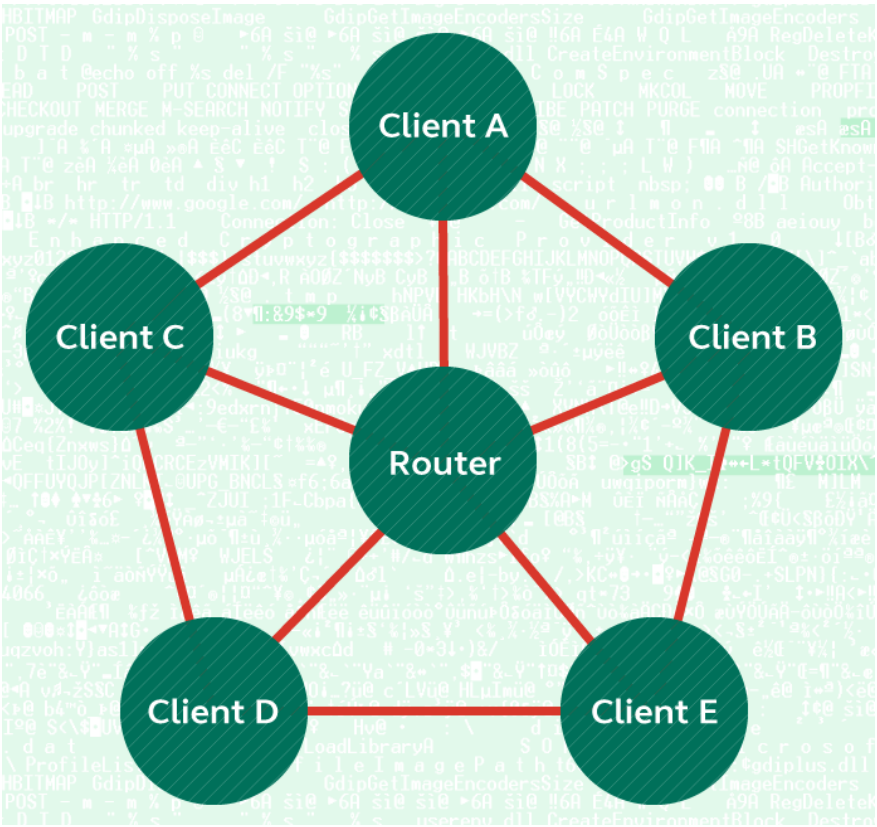

Figure. 2: Traditional topology of a home wireless network. Clients can be any device connected to the Internet.

In general, being on any wireless network – a home wireless network, for example – makes it possible for anyone connected to perform regular man-in-the-middle attacks by using methods such as ARP poisoning. This essentially enables the user to alter any data sent to and from the router.

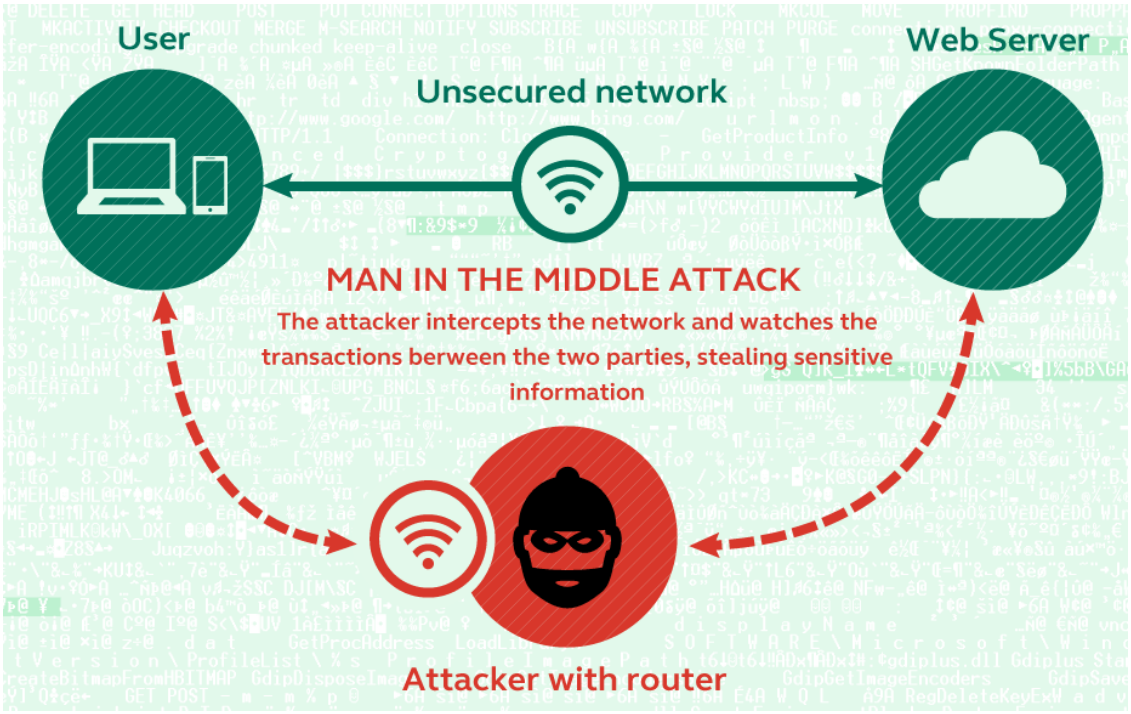

Figure 3: An attacker tells the user he is the router, and tells the router he is the user, thus intercepting traffic to and from the web server

In general, being on any wireless network – a home wireless network, for example – makes it possible for anyone connected to perform regular Man-in-the-Middle attacks by using methods such as ARP poisoning. This essentially enables the user to alter any data sent to and from the router. Because of the nature of the mesh software, however, this standard method would not be very valuable if attempted in the vanilla form. Basically, each node in the mesh network can only have a direct line of sight to a few of the many nodes that exist in the network. In order to send a packet to a device that is not within range, the packet must travel from the origin point, through several other nodes, and eventually reach the destination node. The hardware vendor's system implements a pathfinding algorithm in order to efficiently transport data and to be able to find the most reliable route to destination. The algorithm is very similar to that which is commonly used in video games to determine the path a character will take to get to his destination, avoiding obstructions.

Figure 4: The Pathfinding algorithm find routes for characters to travel based on variables such as difficulty of terrain

The pathfinding algorithm used for the cameras relies on a number of variables, but most important is the signal strength between one node and the next and the number of nodes it travels through in order to reach to the destination.

This is exactly what we took advantage of. By lying to the other nodes, telling them that we had a direct line of site to the simulated police station and would behave as a node by forwarding the packets along, the cameras set up in proximity actually began forwarding their packets directly to us because of the A* implementation. With that set up, a classic Man-in-the-Middle scenario is possible, but now on a very wide range of video feeds. A good analogy here with the RTS game above would be like building a bridge across the lake, so all characters would follow that path, rather than traveling around the shore of the lake.

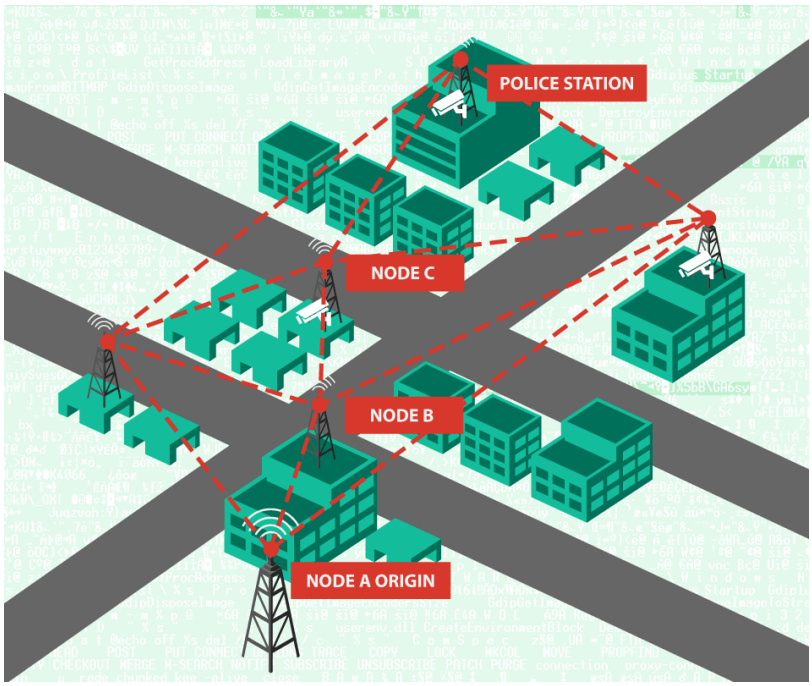

Figure 5: Packet originates from Node A and travels through B to C and finally to Destination Simulated police station). Meanwhile, all other nodes travel through a completely different path and thus cannot be intercepted by listening in at a single location.

SO WHAT ARE THE IMPLICATIONS?

We are not in the business of hacking, we simply wanted to create a proof of concept to demonstrate that this kind of attack is possible, to expose that a vulnerability exists, and ultimately to alert the authorities to a weakness that needs to be fixed. Because of that, our research was done on our own private lab setup, replicating the systems the police had in place, and did not actually harm their network in any way.

As frequently seen in Hollywood movies, if hackers with criminal intent were to take advantage of the problems which we have shown, many dangerous scenarios could unfold. Being able to launch Man-in-the-Middle attacks on the video data is a short step away from replacing real video feeds with pre-recorded footage. In this scenario a cybercriminal gang could lead the police department to believe that a crime is taking place in one area of the city, and wait for the department to dispatch officers there. This would leave a window of opportunity for crime in another region of the city where there are no officers available. This is just one way in which someone could maliciously use these systems to actually assist them in committing crimes much more efficiently than if they were not in place at all. Unfortunately, this is not just a Hollywood scenario. We successfully replicated this functionality in our lab.

We trust the proper authorities to access our private data, but when those authorities do not spend the time and resources necessary to responsibly handle this data we are better off

without this technology at all. Thankfully, after we alerted them to the problem, the cities involved expressed their concern and have since acted to increase security.

The unfortunate truth here is that everything is connected these days, and as new technology is being implemented across the board to modernize older technology, it will inevitably introduce new vulnerabilities. Aside from just the surveillance systems which we analyzed today, there are many more systems which are, and will be, vulnerable to various attacks. The race is on for "the good guys" to test security, before "the bad guys" can use it for malicious intent. Our task is to continue in this effort, to keep the world a safer place.

CONCLUSIONS

The following considerations are necessary to bring a mesh network to a reasonable level of security:

- Although still potentially crack-able, WPA with strong password is a minimum requirement to stop the system from being an easy target.
- Hidden SSID and MAC filtering will also weed out unskilled hackers.
- Make sure all labels on all equipment are concealed and enclosed to deter attackers who do not have insider information.
- Securing video data using Public-key cryptography will make it more or less impossible to manipulate video data.

About authors:

Vasili Hioureas

Junior Malware Analyst at Kaspersky Lab

Vasili Hioureas *initially worked as a software engineer for a number of game development companies and had been independently doing vulnerability research for a number of years before he officially entered the security industry as the lead engineer of an MMO where he wrote exploits for the game servers. He has a wide range of engineering experience having developed everything from audio DSP systems/ language processing algorithms to dynamic texture mapping software.*
In 2013 he joined Kaspersky Lab as a malware analyst with specific interests in APT's and exploits.

Thomas Kinsey

Senior Engineer at Exigent Systems Inc.

Thomas Kinsey has been hacking systems apart since 1999, and working professionally as an an admin/engineer for the last 14 years. His experience from both breaking and reassembling systems (sometimes frantically) serves as a platform for a wide variety of projects. In prep for his past talk at Defcon, Thomas used his skills in reverse engineering to exploit city IT laziness, gaining access to the municipal surveillance video feed in Redlands, CA. Currently he is working at an MSP by day, and creating UAV GNC software/hardware by night.

About Securing Smart Cities

Securing Smart Cities is a not-for-profit global initiative that aims to solve the existing and future cybersecurity problems of smart cities through collaboration and sharing of information between companies, governments, media outlets, other not-for-profit initiatives and individuals across the world.

@SecuringCities

securingsmartcities.org