Cyemptive™
Technologies

PREEMPTIVE CYBERSECURITY

formerly EnZoo

Remote Sensor Protection

cyemptive
cy·emp·tive /ˌsī ˈɛmp tiv/ *adjective*
Serving to preempt, forestall, or prevent computer attack by disabling the enemy.

THE THREAT TO REMOTE SENSORS

Remote sensing devices such as cameras, motion detectors, and other similar sensors are an especially vulnerable part of the cybersecurity landscape. They are both highly tempting targets and difficult to secure. Organizations that rely on these sensors as part of their physical security solution recognize that they can be vulnerable and are looking for solutions.

WHAT ARE REMOTE SENSORS?

In the context of this discussion, we'll be talking about the various remote sensing devices used as part of a physical security infrastructure. These include cameras, motion sensors, radar systems, microphones, intrusion alarms, and similar devices meant to provide remote "eyes and ears" to security professionals.

These devices are remote electronics that send some kind of information back from a remote outpost to a central monitoring facility. That information could be as complex as video and audio, or as simple as an alert. They can be connected via wired or wireless connection, and a given installation may have a few or hundreds of these devices.

Many older sensing devices are connected using dedicated and proprietary networks. However, most current devices use IP networks to communicate. This is the same sort of IP network that millions of other internet connected devices use, which makes setup and programming easy – for both the security professional and those who wish to attack it.

Though many of the solutions presented here are applicable to a wide range of devices in the broader Internet of Things (IoT), this discussion is specifically limited to physical security remote sensing devices. These devices are especially tempting targets for cyber attacks because defeating them can result in unfettered access to highly sensitive areas.

HOW ARE THEY VUNERABLE?

Remote sensors are vulnerable in a variety of ways, both through physical and cyber attacks.

Physical attacks include harm or destruction of the device and are outside the scope of this discussion. It is assumed that some care is taken to avoid access to, or to otherwise physically protect the sensing device.

Cyber attacks are those that use computerized mechanisms to disable or change the devices sensing capabilities. These kinds of attacks are the focus of this discussion.

HOW ARE THEY CYBER ATTACKED?

Remote sensing devices are vulnerable to cyber attack in two primary ways: attack on the device itself and corruption of the data stream back to the monitoring station.

Cyber attacks on the device itself can include a variety of hacks with the intent of disabling the device, or altering the internal programming of the device. These attacks use the network infrastructure itself to access the device, and use that access to disable or alter the device.

Corruption of the data stream is a less obvious and yet more complex attack vector. Instead of disabling the device entirely, the intent of the attack is to change the resulting information. This is less likely to be noticed than a complete failure of a device. This corruption could be as simple as ignoring otherwise alerting events, or as complex as simulating a normal picture from a camera to hide nefarious activity.

REMOTE SENSOR PROTECTION

Given the two primary vulnerabilities there are a variety of ways to protect remote sensing devices. At Cyemptive, we plan to provide a suite of solutions to protect remote devices.

DEVICE PROTECTION

Protecting the device itself from cyber attack is primarily a function of controlling access to the device from the network. By tightly limiting access to the device you can prevent the attacks that occur thorough outside network access.

Remote sensing devices are much like any other network connected device. There are two concerns: the initial attack and subsequent spreading of the attack to others on the network. For example, most malware attacks today start with a single machine that gets infected, and then the peers on the network become infected through machine-to-machine connections.

The Cyemptive Firewall Controller (CFC) is built to prevent just such attacks. It controls, by default, all access to devices and strictly limits the communication in and out of each machine. The CFC also features the patent-pending CyberSlice™ technology that protects the CFC itself from all forms of attack. Together, these limits make it essentially impossible for one device to infect another.

Cyemptive is also developing a subminiature version of the CFC that can be located at each remote sensing device. This Cyemptive Firewall Controller for Remote Devices (CFC-R) will limit access to the device and protect it from attack – at the local level, on the device itself.

With this local version of the firewall the initial attack can be thwarted, and with the controller located in the monitoring station, the machine-to-machine attacks are prevented as well.

DATA STREAM PROTECTION

The other form of cyber attack is the potential for corruption of the data stream from the remote sensor. These attacks occur when the data stream is interrupted and replaced with different information.

The most secure ways to prevent a data stream attack are to use mutually authenticated communication between sender and receiver and to encrypt the information itself.

By using modern cryptographic techniques, it is possible to insure the identity of both the sender and receiver of a communication through a secure "handshake" called mutual authentication. Such communication can detect if it has been interrupted, and can refuse connections from unconfirmed communication partners. The Cyemptive CFC and CFC-R perform this mutual authentication between them. This completely eliminates the possibility of "man in the middle" forms of data stream replacement.

Further, with the appropriate encryption, the corruption of the stream itself is impossible. Even if the attacker could interrupt the stream, they wouldn't be able to interpret it. If they substitute it with their own stream, they wouldn't be able to encrypt it to match the original. The resulting data can even be stored encrypted, and only decrypted by authorized devices for access or display.

The Cyemptive CFC and CFC-R devices are planned to include both of these techniques to fully protect the data stream from the remote sensing devices.

CYEMPTIVE SENSOR PROTECTION PLAN

Cyemptive is taking a four step plan to providing complete remote sensor protection.

STEP 1: NETWORK PROTECTION

The initial step to protect remote sensing devices is to protect the network. Using the Cyemptive Firewall Controller (CFC) at the monitoring station will lock down the network more securely than other competing solutions.

The CFC can protect the devices from intrusions that happen through the monitoring station. The CFC also includes Cyemptive's patent-pending CyberSlice™ technology to protect itself from attack.

STEP 2: DEVICE PROTECTION

The next step is to implement the Cyemptive Firewall Controller for Remote Devices (CFC-R). This is a subminiature version of the CFC located at each remote sensor. The CFC-R will provide strict access control to the devices, further protecting them from attacks.

This combination of local and remote CFCs will secure these devices from both initial attack, and protect them from infecting each other.

STEP 3: STREAM PROTECTION

The next step is to implement data stream protection on the CFC and the CFC-R.

The CFC-R on each device will insure that it is only communicating with the intended CFC and that the stream is uninterrupted. The CFC-R will also encrypt the stream to prevent interpretation and/or replacement of the data stream in transit. Only the appropriate CFC will be able to decrypt the stream.

This protection, including handshakes and stream encryption, will eliminate the potential for data stream corruption.

STEP 4: CYBERSLICE ON THE DEVICE

The final step will be to implement the patent-pending CyberSlice technology in the CFC-R devices. CyberSlice has the ability to protect devices even if the network as somehow been compromised.

This step will further protect these devices from attack and provide the ultimate in remote sensor protection.

UNPARALLELED PROTECTION

The combination of these four steps will result in remote sensing device protection that puts Cyemptive in a class by itself.

Contact a Cyemptive cybersecurity professional today to see how your organization can get the benefits of Cyemptive's remote sensing device protection, and to understand the many other ways Cyemptive can give your network the protection it deserves. Email us at info@cyemptive.com or check out cyemptive.com for more information.

ABOUT CYEMPTIVE

Cyemptive Technologies, Inc. is a cybersecurity software company headquartered in the Seattle area. Originally founded as EnZoo in February 2014, the firm is privately held.

Cyemptive has assembled a world class team of experts in security and enterprise software. The team combines hundreds of years of experience working at companies like Microsoft, Hitachi, and IBM delivering outstanding results for millions of customers worldwide.

For more information, or to have an expert help you secure your network, visit Cyemptive.com or email info@Cyemptive.com.