Politechnika Wrocławska

Wirtualne Środowisko Nauki SJO

Projekt Studium Języków Obcych

Politechniki Wrocławskiej

Język specjalistyczny

Właściwości dokumentu:

Język:	ANGIELSKI
Poziom:	B2
Wydział:	W4
Opracowanie:	mgr Zbigniew Deka

Many security cameras vulnerable to hacking

Businesses and other services dependent upon security solutions have been urged to upgrade their security cameras due to risks that such cameras can be hacked. A big risk arises from malware which leads to leakage of sensitive information from the very same surveillance devices used to protect facilities.

Organizations with internet-connected networks use a host of security software to keep nefarious hackers out of the network. But for even greater security, firms and government entities set up “air-gap” networks, which aren’t physically connected to the Web. To bypass this “air gap,” a hacker needs to embed malware into such a network. This could be accomplished by using a malicious insider, or simply selling a USB with malware loaded on it.

The extent of the concern has been highlighted by Ben-Gurion University (BGU) of the Negev. In a study the researchers have shown how surveillance cameras can be sent covert signals which trigger them to leak sensitive information.

The danger from hacking exists equally for businesses and home security solutions. Moreover, the risks extend beyond cameras to other control and access systems like LED doorbells, which can detect infrared light (IR) that is not visible to the human eye. The method for bypassing security systems has been dubbed "aIR-Jumper". This is because hackers can create bidirectional, optical communication between air-gapped internal networks.

The weaknesses were identified by a team led by Dr. Mordechai Guri. The researcher has shown how IR can be deployed to develop a covert communication channel between malware installed on an internal computer network and a hacker located in close proximity to the site. The infrared channel can be exploited to send commands and to receive response messages.

To transmit sensitive information, the attacker uses the camera’s IR-emitting LEDs, which are typically used for night vision. The researchers showed how malware can control the intensity of the IR to communicate with a remote attacker that can receive signals with a simple camera without detection.

The researchers shot two videos to highlight their technique. One video shows an attacker hundreds of yards away sending infrared signals to a camera. The other video shows the camera infected with malware responding to covert signals by exfiltration data, including passwords. In the same way a potential hacker, standing in a parking lot could obtain information about PIN codes and encryption keys.

Commenting on this Dr. Guri said in a research note: "Security cameras are unique in that they have 'one leg' inside the organization, connected to the internal networks for security purposes, and 'the other leg' outside the organization, aimed specifically at a nearby public space, providing very convenient optical access from various directions and angles. Theoretically, you can send an infrared command to tell a high-security system to simply unlock the gate or front door to your house".

It’s troubling to see how vulnerable networks can be. Hackers have used electromagnetic radiation from the computer screen and audio signals from a spinning hard drive or a fan to generate binary messages and transmit data. In one attack, hackers designed malware that sends signals by blinking the caps-lock light into a camera. If it generates an optical, thermal, acoustic or electromagnetic signal, it can be used to relay information.

Adapted from:

1. http://www.digitaljournal.com/tech-and-science/technology/many-security-cameras-vulnerable-to-hacking/article/505215

2. https://aabgu.org/hackers-via-security-cameras/
3. https://aabgu.org/security-cameras-hacked-using-infrared-light/
4. http://blogs.discovermagazine.com/d-brief/2017/09/21/security-cameras-hackers/#.WnNSYTd75Ea

TASK 1 Read the text and decide if the following sentences are TRUE or FALSE.

1. One of the shortcomings of surveillance cameras is that they can be used to steal information about the facility they are supposed to protect.
2. "Air gap" networks, where computers are disconnected from the Internet, do not allow for remote access to an organization.
3. According to the BGU researchers, signals emitted by an attacker to hack a security camera can be easily detected.
4. The method presented by the researchers will work on both professional and home security systems.
5. The channel between internal networks and remote attackers provides information transfer both ways.
6. Among cameras vulnerable to hacking are those equipped with night vision infrared LEDs.
7. An attacker needs a very clever camera to receive response messages.
8. To initiate communication with the malwared network hackers must know the password.
9. Nearby parking lots and other public spaces should be avoided by attackers if they want to establish successful communication.
10. Even components of computer's cooling system can transmit information.

TASK 2 Match the verbs from the text with the definitions.

1. to urge	a. to withdraw or remove without permission
2. to leak	b. to make something include more things, areas or objects
3. to bypass	c. to contain or implant as an essential part, to insert
4. to trigger	d. to strongly advise, encourage, advocate
5. to extend	e. to make use of
6. to detect	f. to avoid or ignore something e.g. to get it done quicker
7. to relay	g. to cause something to start
8. to exfiltrate	h. to allow e.g. secret information to become generally known
9. to exploit	i. to pass from one person or device to another
10. to embed	j. to discover something, usually using special equipment

TASK 3 **Complete the sentences with the following words and phrases (each can be used only once).**

malicious / vulnerable / internal networks / bidirectional / encryption keys / infrared / surveillance / remote / proximity / malware

1. It’s difficult for security guard to spot any suspicious behaviour because __________ light is invisible to the naked eye.
2. To be able to send and receive data, hackers must establish a _________ communication channel.
3. Some people complain that public _________ cameras can violate privacy and personal rights.
4. Modern smartphones are now as easy to infect with __________ as a traditional PC.
5. Over one-third of critical infrastructure organizations in the UK are _________ to DDoS attacks.
6. This system provides __________ access from anywhere and is easy to administrate.
7. __________ used to secure data must be carefully managed to ensure data remains protected and accessible when needed.
8. Many people believe it’s impossible to hack into _________ within businesses that are not connected to the Web.
9. One of hackers’ favourite methods to trick online shoppers is to make them click on __________ links and attachments.
10. NFC (near-field communication) is a wireless technology where electronic devices in __________ can communicate with each other.