network video
Seamless Intelligence

Internet of Things and the risks of vulnerabilities

Date : 27th July 2017

The Background to IoT

- The “Internet of Things” (IoT) covers all IP addressable appliances
- Ranges from home appliances and control, such as heating, lighting control, and even internet connected fridges and kettles.
- Many are based on embedded Linux and common code structures
- Frequently not considered ‘critical’ and so not protected – after all how much damage can someone do with your kettle?
- Each IoT item however is potentially a relatively powerful processor – 1000’s times more powerful than the computers that took man to the moon!
- IP cameras and other security devices amongst the most prolific types of IoT.

network video
Seamless Intelligence

IoT Vulnerability

What is an IoT vulnerability and what does it mean?

- A remote attacker, directly or indirectly can execute commands or add code to an IoT device.
- That code can then spread the malicious code to other devices.
- These devices can then be activated to either harvest confidential information, or attack other systems, either altering their operation or potentially disabling them, short term or permanently
- Attack frequently targeted at other devices, rather than the device that has been compromised

network video
Seamless Intelligence

Is it a real threat?

- When concerns were first raised in the late 2000's the risk was dismissed by many as far fetched, and "Hollywood Fiction"
- September 2016 was one of the first major cyber attacks, affecting major commercial organisations such as Amazon, Netflix, Dyn and more.
- IP cameras were a significant element of the "Cyberbot" network
- During the last 12 months, vulnerabilities have been identified in many IP cameras from a wide range of manufacturers.

Recent Vulnerabilities

- There have been many reports of vulnerabilities in Chinese manufactured cameras including major players such as Hikvision and Dahua.
- They are not alone however – and many apparently western manufacturers OEM cameras from Far East sources.
- In July 2017, a significant vulnerability was identified in a leading western manufacturer, Axis, but of much greater concern it has been identified as being shared by many ONVIF compatible cameras from a wide range of both western and Far East manufacturers.

Common Vulnerabilities

- Vulnerabilities typically take one of three forms
  - Simple command execution

    Gaining access to a device that either has no access credentials set, or are obvious common default values such as ‘default’ or ‘password’. Any OS command can be executed, potentially including installing new software.
  - ‘Stack Overflow’

    Injection of malicious code, and as a result complete control of the device can be achieved.
  - Raising of Privileges

    Changing / adding the security level of a given user credential, such that complete OS ‘root’ command privileges can be gained, allowing complete control.

What is a ‘stack overflow’ ?

- ‘Stack Overflow’ based attack

  This is typically achieved by sending an unusually long command or submission to the unit.

  This submission ‘corrupts’ the internal memory structure and allows the injection of malicious code.

  When accessing subroutines, data is stored in a memory area called the ‘stack’. This includes information about where the subroutine should pass control back to when finished. This can be altered if there are no checks on data submitted overrunning the maximum limit – and then overwriting the ‘stack’ with new parameters - including next code to execute. As a result complete control of the device can be achieved.

  This type of attack has been addressed very frequently in Windows security updates, often referring to “control being achieved by a remote user”.

network video
Seamless Intelligence

Why can't the vulnerabilities be found and fixed?

- It has been estimated that an undiscovered vulnerability will occur in 1 in 1,000 to 1 in 50,000 lines of code depending on the skill of the developer and control systems.
- An embedded OS such as Linux will have around 50 million lines of code.
- A typical IP camera application and associated libraries will have far more than 2 million lines of code.
- gSoap, a library recently exposed as containing a 'stack overflow' vulnerability, has 150,000 lines of code.
- Whoever the developer, and whoever the manufacturer, it is likely that vulnerabilities exist now, and remain to be discovered.

How to Mitigate

- In response to the recent gSoap vulnerability named ‘Devil’s Ivy’, identified by Senrio Labs, the report included the following recommendations and conclusions :

  1. Keep physical security devices off of the public internet….. Devices like security cameras should be connected to a private network, which will make exploitation much more difficult

  2. Defend IoT devices as much as possible. If you can place a firewall or other defensive mechanism in front of an IoT device, or utilize Network Address Translation (NAT), you can reduce their exposure and improve the likelihood of detecting threats against them.

  …….

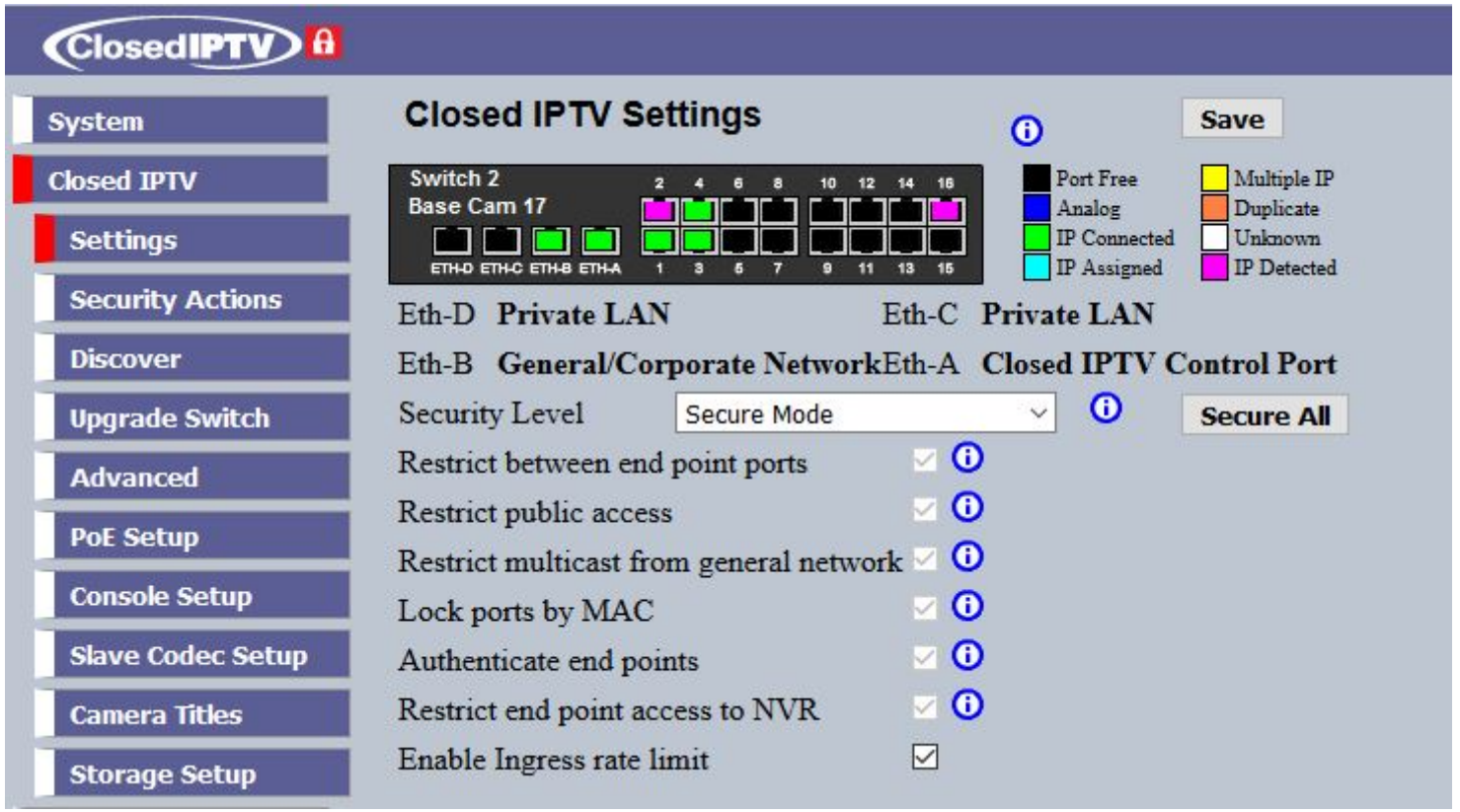
  While forums like ONVIF serve a useful purpose when it comes to issues of cost, efficiency, and interoperability, it is important to remember that code reuse is vulnerability reuse. The significance of this principle in the physical security device industry should be self-evident.

How does DM product help to protect against Cyber Attacks?

- Closed IP TV introduced in 2010 provides an additional ‘hardened’ management layer, that automatically applies a number of additional security layers.
- DM products do not support generic protocols such as ONVIF and PSIA, as this has always been felt to expose unnecessary risks, as now proven.
- The NetVu Connected protocols not only reduce the ‘attack surface’ presented they also provide many rich features that simple generic web streaming protocols core to solutions such as ONVIF and PSIA cannot support.
- RTOS / Hybrid OS to limit the ‘attack surface’ exposed.

Closed IPTV Setup

Closed IPTV Configuration Setup



network video
Seamless Intelligence

Key Features

- Restrict between end point ports

  Each endpoint port is blocked from communicating with any other endpoint ports. This would immediately defend one device from being attacked or compromised by another.

- Restrict public access

  A number of independent VLANS (Virtual LANs) are created to segregate secure endpoints from the general network and potentially the storage network

- Restrict multicast from general network

  Prevent any discovery or other broadcast information from passing beyond the closed network.

- Lock ports by MAC

  All devices are specifically identified on the network and IP addresses automatically allocated. Once the system is set secure, each port is configured with a MAC address restriction to solely the discovered devices.

network video
Seamless Intelligence

- Authenticate end points

  An individual security key is applied which is validated as part of any IP Camera communications, further verifying that the correct device is connected, so preventing unauthorised access even if the MAC and IP address of a valid device have been cloned.

- Restrict end point access to NVR

  Only allows communications to be established from the master control units (Gateway, NVR, DVR etc) to the IP Camera – so no attack could be launched by an affected camera upon the central infrastructure, as it is unable to initiate an inbound connection.

network video
Seamless Intelligence

- Enable Ingress rate limit

  Limits the maximum data rate and number of packets that can be sent by a specific port. Even if a port were compromised, this would significantly limit any attempted ‘Denial of Service’ form of attack.

- Single IP Address Gateway

  Only very specific communications allowed via the Gateway, such that no generic access is granted to the endpoints. This means that typical routes for a cyber attack to be performed don’t exist between the general network and the enpoints.

RTOS / Hybrid OS

- If a vulnerability exists, often can only be leveraged through generic OS functions and entry points
- DM products previously all RTOS (Real Time Operating System) based.
- However with increased complexity of latest DSP's etc, it is not typically viable for 'bare metal' RTOS designs.
- Hybrid hardened RTOS / OS solution allows complex device driver support from the OS, but with a minimum of generic OS services only, excluding generic command line shell and many other 'open services' which are more subject to exploit.
- All required services provided by the core application, running in an RTOS like mode, significantly reduces the 'attack surface'

Key Recommendations

- Avoid generic open standard solutions and reuse of popular libraries, exposing common vulnerabilities.
- Segregate the IP camera network, and only provide access by well defined Gateways that only forward specific services.
- Use IP camera technology based on RTOS / Hybrid OS architecture such as NetVu Connected.
- Avoid generically addressed traditional VMS architectures, and replace with automatically managed hardened network management layers, such as Closed IPTV