Reading Mission Control Data out of Predator Drone video feeds By Kingcope

Introduction

There have been recent reports [1] of insurgents intercepting unencrypted U.S. Predator drone video feeds in Iraq and Afghanistan. The predator drone video feeds were sent in some cases from the predator drones without any encryption technology so the insurgents were in a rather simple situation to intercept the video feeds and save them to hard disks and share them among each other. WSJ [1] states that a software called “SkyGrabber” was used to read the video feeds. The intention of this software is to read images and videos off the air by using satellite antennas.

After doing some research on the issue we found that in the predator video feeds aside from image data there is also mission control data carried inside the satellite signal to the ground control stations. It is theoretically possible to read off this mission control data both in the intercepted video feed and saved video data on harddisks.

Technology used by the drones

There is a control and command link to communicate from a control station to the drone. Further there is a data link that sends mission control data and video feeds back to the ground control station. Here one has to distinguish between line-of-sight communication paths and beyond line-of-sight communication paths. The operation of the line-of-sight link is limited to approx. 81-138 miles. This operating range can be extended by for example using mobile ground control stations, which are locally deployed. Line-of-sight links are critical for takeoffs and landings of the drone. These links utilize a C-Band communication path. Beyond line-of-sight communication links operate in the Ku-Band satellite frequency. This allows the UAV (Unmanned Arial Vehicle) to cover approx. 1500 miles of communication capability.

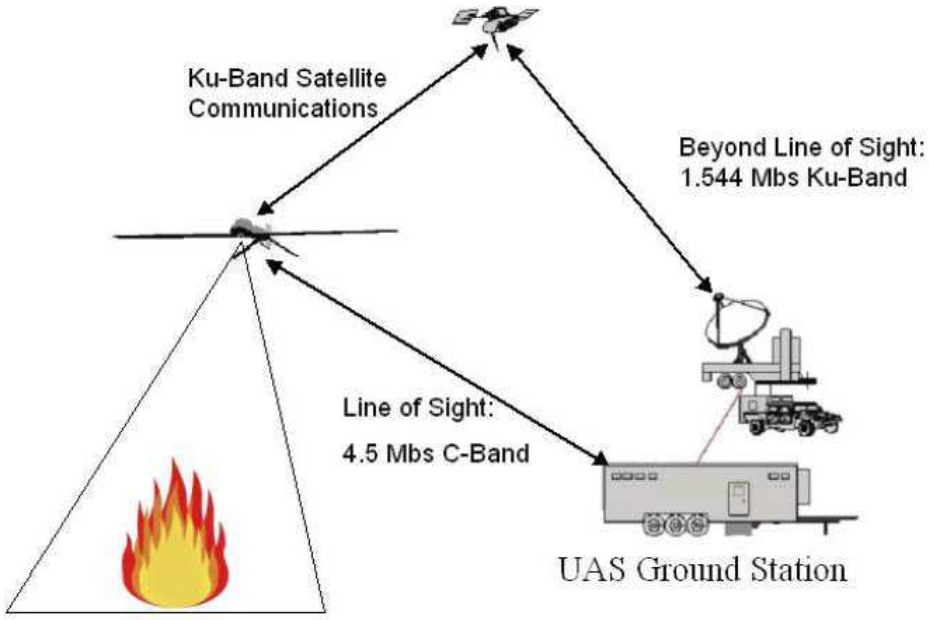


Figure: C-Band and Ku-Band Communication

So this explains somewhat why the insurgents were able to intercept the Predator video feeds when they were sent unencrypted to the ground station. The only thing needed is a C-Band or Ku-Band antenna which can read traffic. Sending traffic to a satellite for example is not needed in this case.

The drones normally use MPEG-TS (MPEG Transport Stream) to send video and data to the ground station. Motions Imagery Standards Board (MISB) [2] has developed several standards on how to embed the control data into MPEG streams.

16-byte UL	Name	Data Type or References	Allowed Values or References	Maximum or Default Length (Bytes)	Required/ Optional/ Context
06 0E 2B 34 01 01 01 03 02 08 02 01 00 00 00 00	Security Classification	ISO 7 bit Enumerated Text	TOP SECRET// SECRET// CONFIDENTIAL// RESTRICTED// UNCLASSIFIED//	14	Required
06 0E 2B 34 01 01 01 03 07 01 20 01 02 07 00 00	Classifying Country and Releasing Instructions Country Coding Method	ISO 7 bit Enumerated Text	ISO-3166 Two Letter ISO-3166 Three Letter ISO-3166 Numeric FIPS 10-4 Two Letter FIPS 10-4 Four Letter 1059 Two Letter 1059 Three Letter 1059 Numeric FIPS 10-4 Mixed ISO 3166 Mixed STANAG 1059 Mixed Other	21 (40 max)	Required
06 0E 2B 34 01 01 01 03 07 01 20 01 02 08 00 00	Classifying Country	Enumerated Text from the appropriate standard preceded by '//'	FIPS 10-4 ISO-3166 STANAG 1059	6	Required
06 0E 2B 34 01 01 01 01 0E 01 02 03 02 00 00 00	Security-SCI/SHI Information	ISO 7 bit	Security Ref 2.1.1	40	Context
06 0E 2B 34 01 01 01 03 02 08 02 02 00 00 00 00	Caveats	Free Text	Security Ref 2.1.2	20 (32 max)	Context
06 0E 2B 34 01 01 01 03 07 01 20 01 02 09 00 00	Releasing Instructions	ISO 7 bit Free Text	Security Ref 2.1.1 Refs 2.1.11, 2.1.12, 2.1.13	40	Context
06 0E 2B 34 01 01 01 03 02 08 02 03 00 00 00 00	Classified By	ISO 7 bit Free Text	Security Refs 2.1.2, 2.2.11	40	Context

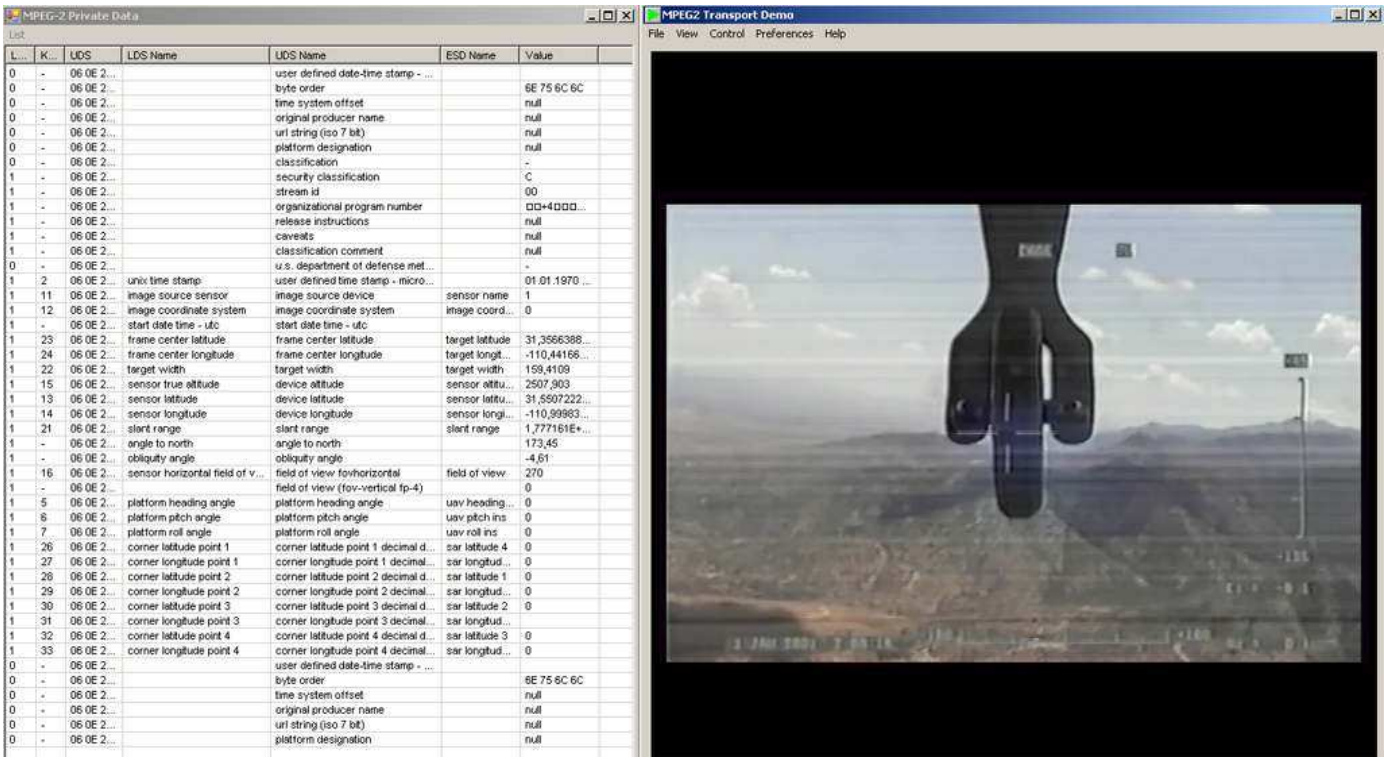
Figure: Excerpt of metadata sent with the MPEG Transport Stream taken off a public MISB Standard document

An important note is that our research shows that most if not all metadata inside the MPEG Stream is for its own not encrypted if the MPEG Stream itself is not encrypted.

How to read the control data with publicly available tools

During our research we found a suitable tool to read the mission control data off the air video feeds and also off saved video feeds. The tool is programmed by LEADTOOLS [3] and is capable of reading KLV metadata out of MPEG-TS. Inside the LEADTOOLS Multimedia SDK package a programmer finds source code and binaries of the needed tool.

The following screenshot shows the tool in action. The loaded file is a saved MPEG-TS UAV video with private metadata embedded.



L...	K...	UDS	LDS Name	UDS Name	ESD Name	Value
0	-	06 0E 2...		user defined date-time stamp - ...		
0	-	06 0E 2...		byte order		6E 75 6C 6C
0	-	06 0E 2...		time system offset		null
0	-	06 0E 2...		original producer name		null
0	-	06 0E 2...		url string (iso 7 bit)		null
0	-	06 0E 2...		platform designation		null
0	-	06 0E 2...		classification		-
1	-	06 0E 2...		security classification		C
1	-	06 0E 2...		stream id		00
1	-	06 0E 2...		organizational program number		□□+□□□...
1	-	06 0E 2...		release instructions		null
1	-	06 0E 2...		caveats		null
1	-	06 0E 2...		classification comment		null
0	-	06 0E 2...		u.s. department of defense met...		-
1	2	06 0E 2...	unix time stamp	user defined time stamp - micro...		01.01.1970 ...
1	11	06 0E 2...	image source sensor	image source device	sensor name	1
1	12	06 0E 2...	image coordinate system	image coordinate system	image coord...	0
1	-	06 0E 2...	start date time - utc	start date time - utc		
1	23	06 0E 2...	frame center latitude	frame center latitude	target latitude	31,3566388...
1	24	06 0E 2...	frame center longitude	frame center longitude	target longit...	-110,44166...
1	22	06 0E 2...	target width	target width	target width	159,4109
1	15	06 0E 2...	sensor true altitude	device altitude	sensor altitu...	2507,903
1	13	06 0E 2...	sensor latitude	device latitude	sensor latitu...	31,5507222...
1	14	06 0E 2...	sensor longitude	device longitude	sensor longi...	-110,99983...
1	21	06 0E 2...	slant range	slant range	slant range	1,777161E+...
1	-	06 0E 2...	angle to north	angle to north		173,45
1	-	06 0E 2...	obliquity angle	obliquity angle		-4,61
1	16	06 0E 2...	sensor horizontal field of v...	field of view fovhorizontal	field of view	270
1	-	06 0E 2...		field of view (fov-vertical fp-4)		0
1	5	06 0E 2...	platform heading angle	platform heading angle	uav heading...	0
1	6	06 0E 2...	platform pitch angle	platform pitch angle	uav pitch ins	0
1	7	06 0E 2...	platform roll angle	platform roll angle	uav roll ins	0
1	26	06 0E 2...	corner latitude point 1	corner latitude point 1 decimal d...	sar latitude 4	0
1	27	06 0E 2...	corner longitude point 1	corner longitude point 1 decimal...	sar longitud...	0
1	28	06 0E 2...	corner latitude point 2	corner latitude point 2 decimal d...	sar latitude 1	0
1	29	06 0E 2...	corner longitude point 2	corner longitude point 2 decimal...	sar longitud...	0
1	30	06 0E 2...	corner latitude point 3	corner latitude point 3 decimal d...	sar latitude 2	0
1	31	06 0E 2...	corner longitude point 3	corner longitude point 3 decimal...	sar longitud...	
1	32	06 0E 2...	corner latitude point 4	corner latitude point 4 decimal d...	sar latitude 3	0
1	33	06 0E 2...	corner longitude point 4	corner longitude point 4 decimal...	sar longitud...	0
0	-	06 0E 2...		user defined date-time stamp - ...		
0	-	06 0E 2...		byte order		6E 75 6C 6C
0	-	06 0E 2...		time system offset		null
0	-	06 0E 2...		original producer name		null
0	-	06 0E 2...		url string (iso 7 bit)		null
0	-	06 0E 2...		platform designation		null

References

[1] Insurgents Hack U.S. Drones, Wall Street Journal
http://online.wsj.com/article/SB126102247889095011.html
[2] MISB, http://www.gwg.nga.mil/misb/stdpubs.html
[3] LEADTOOLS, http://leadtools.com/SDK/Multimedia/mpeg2-transport-stream.htm