Edith Cowan University
Research Online

Australian Information Warfare and Security Conference

Security Research Institute Conferences

2006

Tags at War: A Review of the United States Department of Defence RFID Tag Data Standard

Uros Urosevic
Edith Cowan University

Christopher Bolan
Edith Cowan University

Originally published in the Proceedings of 7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/isw/21

Tags at War: A Review of the United States Department of Defence RFID Tag Data Standard

Uros Urosevic
Christopher Bolan
School of Computer and Information Science
Edith Cowan University

Abstract

The U.S. Department of Defence have mandated the use of RFID technology in their procurement and supply systems. To enable compatibility across civilian contractors and suppliers and military systems the US DOD RF-Tag Data Format 2.0 specification has been implemented. This paper outlines the features of this standard and the possible security implications of its adoption.

Keywords

Radio Frequency Identification, JDTAV, Data Format

INTRODUCTION

In the evolution of Radio Frequency Identification (RFID) technology, the 2005 mandate of the United States Department of Defence in 2005 to include RFID Tags as part of its inventory and supply chain is widely seen as an important milestone (Bolan, 2005; EETimes, 2004). From the 1st of October 2005 all newly acquired tangible items sold to the US military must contain a compliant RFID tag and by the 31st of December 2010 every tangible legacy item owned or used by the US military will be retrofitted with a compliant Tag (Wynne, 2003). As the total spending budget for the DoD was over $US 417.5 billion for the 2005 financial year the adoption of the ISO standards will provide a strong impetus for others to follow the same standards (EETimes, 2004).

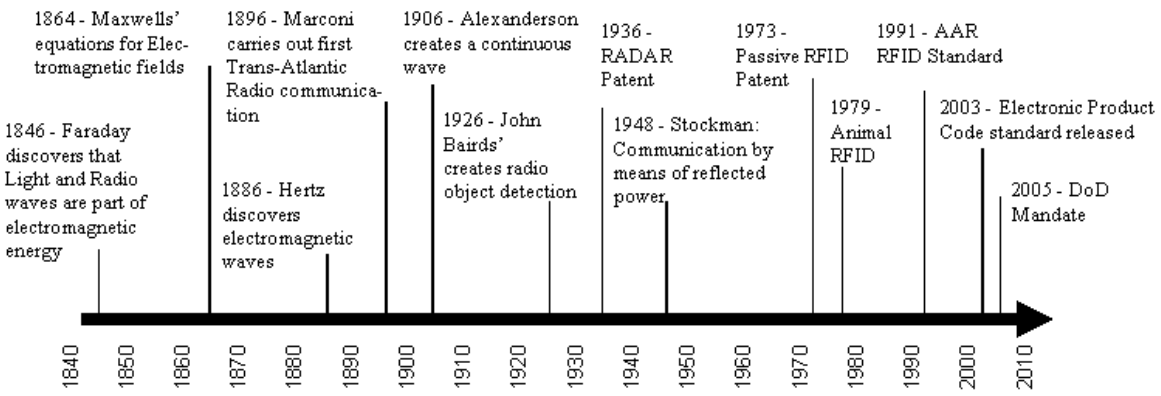

Figure 1. Timeline of RFID related history (Bolan, 2005)

The content/storage requirements of RFID Tags used by the US DoD are specified in a new RF-Tag data standard, RF-Tag Data Format 2.0 (AIT, 2005) that supersedes the previous Joint Defence Total Asset Visibility (JDTAV) format. The goal of the standard is to provide a format for storing, accessing and transferring information, to increase efficiency through quicker access to useful manifest data. The RF-Tag Data Format 2.0 pertains to three different RF-Tag's consisting of the 128K Byte SealTag, 128K 410R Tag and the TAV/ITV 412

tags. Each of the RF-Tag's have in-built memory consisting of cache-like standard memory and extended memory storing vital shipment and item related information (AIT, 2005).

SEALTAG & 410R TAGS

Both the SealTag & 410R tags have a standard non-volatile memory of 128 to 256 bytes. The standard memory section of the tag is used for tag identification and as a type of 'cache' to facilitate information transfer during tag interrogation. A summary of the standard memory is given in figure 2 below.

Address	Length	Stored Data	Data Value	Description
0-14	15	Tag ID, model	Pre-defined fixed value	Fixed value that is pre-defined for Tag ID and Savi reserved space
15-17	13	File Type	$E0 $01 $02	Official JDTAV 2.0 data format identifier
18	1	Reserved		
19-34	16	Tag Name	16 ASCII char	Tag name character limit is 16, with NULL terminator added to names < 16 and NULL single for undefined names
35-39	3	Date Tag was Last Written	2-digit hexadecimal value for timestamp	*Year* (00-99). i.e. 98h is 1998 *Month* (01-12). i.e. 07h is July *Day* (01-31). i.e. 20h is the 20th day *Hour* (00-23). i.e. 13h is 13, from 13:30 *Minute* (00-59). i.e. 30h is 30, from 13:30
40-42	3	Pointer to Extended Memory	End of File Pointer	

Figure 2. Example of RF-Tag Standard Memory Allocation (AIT, 2005)

The standard memory contains memory addresses pertaining to common tag-related data, including the tag's file type, tag name and timestamp. The file type contains hexadecimal value $E0 $01 $02 signifying that the tag is of JDTAV RF-Tag Database format. The tag name identifies the tag, with a maximum name size of 16 characters, a NULL terminator added for names less than 16 characters and a single NULL is used when the name is not defined. The date field contains a military timestamp value in Binary Coded Decimal (BCD) format.

ADDRESS	SECTION
0000	*Reserved*
0001 0254	**License Plate Data**
0255	*Reserved*
0256 0467	Database Table Pre-Header

ADDRESS	SECTION
0468 0511	*Reserved*
0512 0527	Database Table Header
0528 120127	**Commodity Item records & Single Data Item Records**
120128	*Unused*

ADDRESS	SECTION
120129 124730	4602 Reserved Bytes for Database Query Results
124731 131050	**TCMD Records**
131051 131071	*Unused*

Figure 3. RF-Tag Extended Memory Layout, (AIT, 2005)

Beyond the obvious Y2K issue of only storing a two digit year value, the other questionable practice is the storage of integers in a hexadecimal format. As may be seen in figure 2, while the hexadecimal value of 98 is actually 62 the format ignores the rules of mathematics and simply stores this as 98h. Thus there is actually no reason to use hexadecimal values and their inclusion in such a manner will likely result in implementation issues.

The SealTag & 410R tags have an extended memory of 128k battery backed RAM containing the data file consisting of license plate data, database structure information, Transportation Control Management Document (TCMD) data, commodity item database and single data item records. The overall layout of the extended memory is detailed in figure 3.

The license plate data consists of 254 bytes, containing easily accessible tag summary information. Each piece of information in this area is no more than 20 characters in length, to facilitate displaying the data on a Hand Held Interrogator (HHI). This area must be in the sustainment, unit movement or free text license plate format.

License Plate - Sustainment Data Format

The sustainment license plate data is derived from the information in the Transport Control and Movement Documentation (TCMD) area. An overview of this format is detailed in figure four below with fixed information shown in bold.

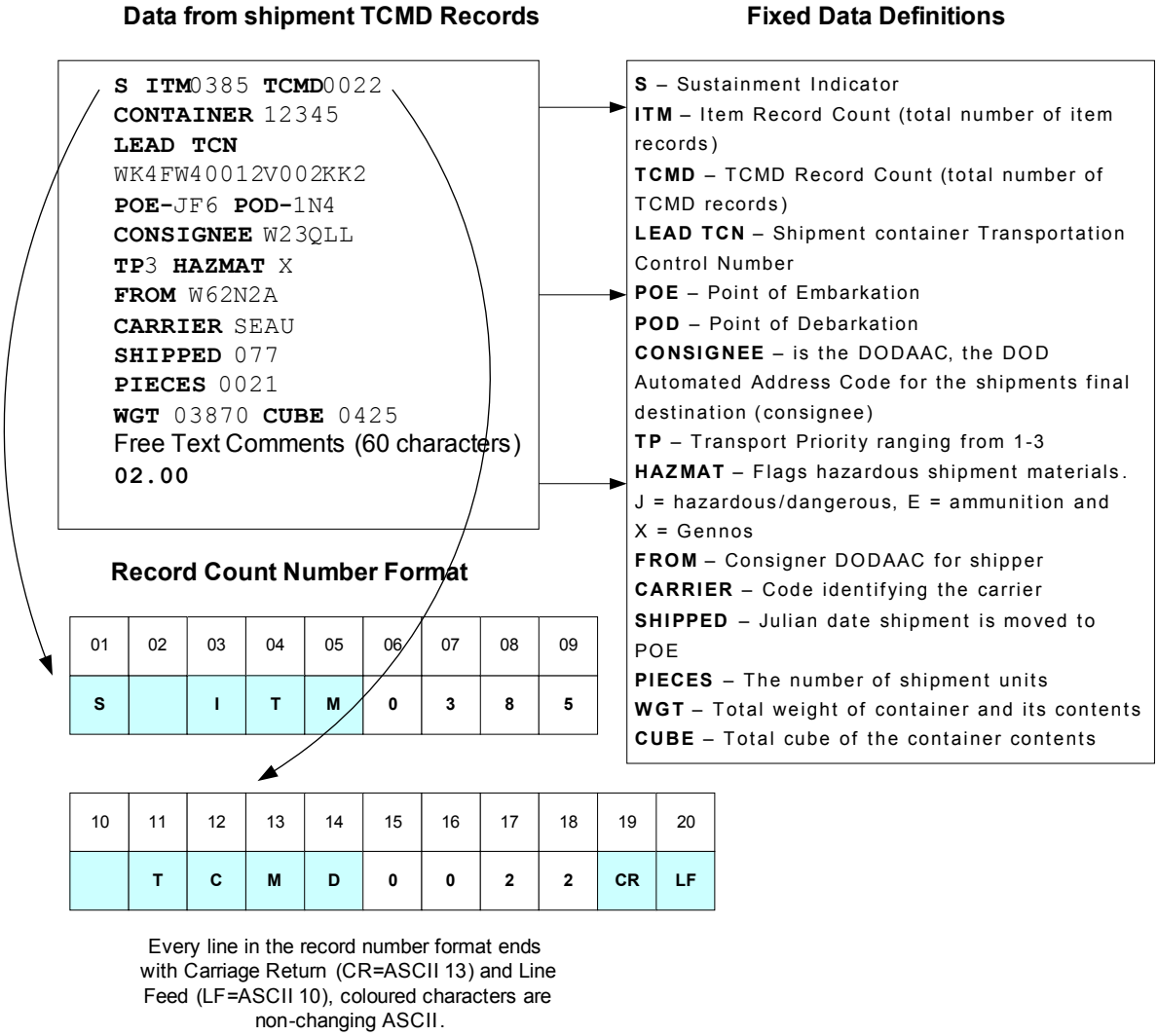

Figure 4. Example of Sustainment License Plate Data Format (AIT, 2005)

License Plate - Unit Movement Data Format

The unit movement data contains information regarding unit movement including further shipment details; the format is similar to sustainment data in that it uses a numbered format to allocate memory addresses and uses CR and LF to indicate the end of lines. The difference between the unit movement format and sustainment data format is that the unit movement data format uses a line feed value of (ASCII 10) [6] and allocates memory in a repeating number range from 0-9 as opposed to 01-254 used in sustainment data. An overview of this format is detailed in figure five below with fixed information shown in bold.

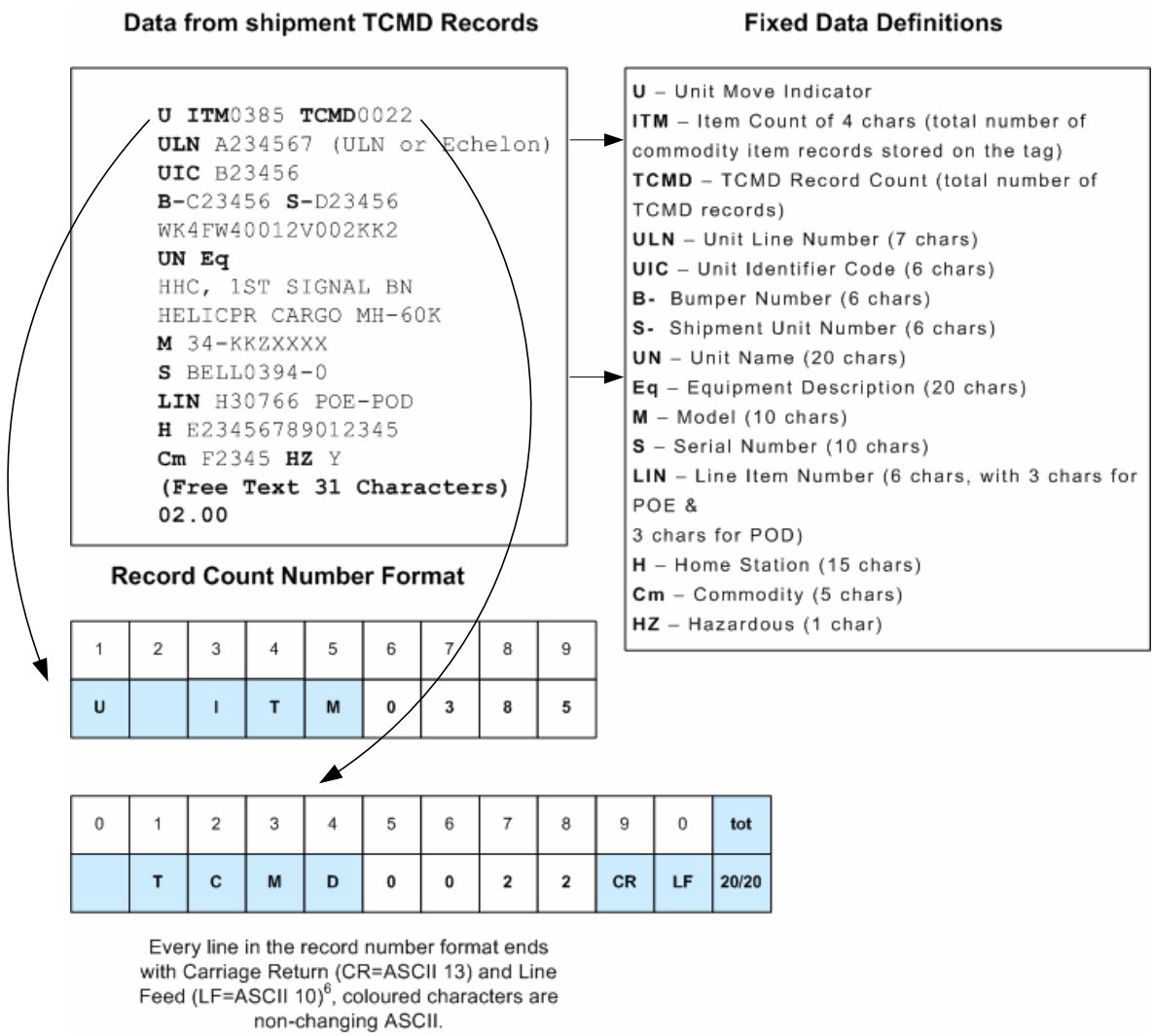

Figure 5. Example of Unit Movement Data Format, (AIT, 2005)

License Plate - Free Text Data Format

The free text data format is used as a last resort when shipment information is incomplete or incompatible with the previously mentioned formats. The information stored includes type identifier; Item and TCMD record count, 229 free characters for ASCII and the format version number. This format adopts the same carriage return, line feed values and the two-digit format for allocating memory as the sustainment format. An overview of this format is detailed in figure six.

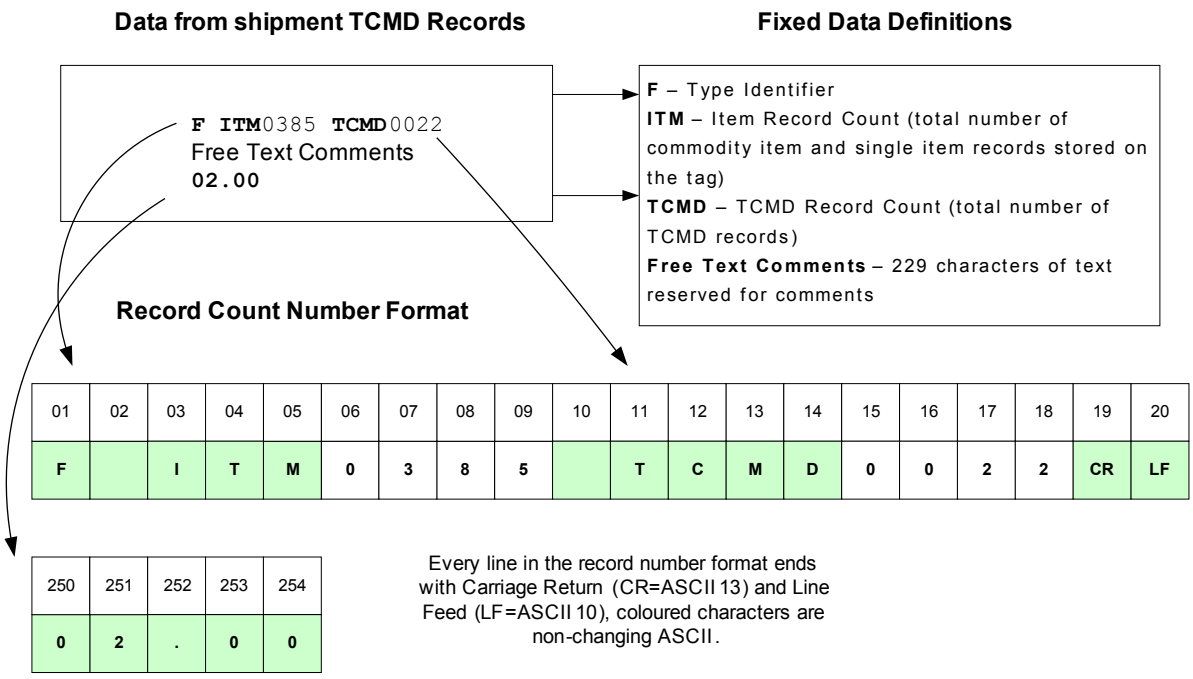

Figure 6. Example of Free Text Data Format, (AIT, 2005)

Database Structure Information

Database structure information consists of 272 bytes, starting at extended memory address 256. The information is divided into a database table pre-header and a database table header. The pre-header holds field names and types used by a Hand Held Interrogator (HHI) and other applications for displaying the field name; it is located from memory address 256 to 388. It is mandatory for it to be written and be unchanged on all tags, with modification only occurring upon formatting of the tag, following the standard set in figure seven.

ADDRESS												
256	12	12	T	A	V						00	00
268	A	00	N	O	M	E	N	C	L	A	T	R
280	A	00	D	O	C	U	M	E	N	T		
292	A	00	L	I	N							
304	A	00	N	S	N							
316	A	00	R	I	C							
328	A	00	U	N	I	T	_	I	S	S	U	E
340	A	00	Q	U	A	N	T	I	T	Y		
352	A	00	C	O	N	D	_	C	O	D	E	
364	A	00	I	N	T	_	T	C	N			
376	A	00	M	I	S	C	1					
388	A	00	M	I	S	C	2					

[White is ASCII text, Blue is binary value]

Figure 7. Exact Values for Database Pre-Header, (AIT, 2005).

The database table header contains specific field data that is used in searches by the tag database engine; it is located from memory space 512 to 527. This data includes the total number of records made up of commodity item and single item counts and locations of fields and record offsets, seen below in figure 8.

ADDRESS	LENGTH	DECIMAL VALUE	DESCRIPTION
512	**2**	Sum of commodity item count & Single data item count	The total number of records in the database as the sum of commodity and single item counts
514	**1**	**11**	Number of fields in each record
515	**1**	**16**	Offset from 512 to the beginning of the database
516	**1**	**00**	Record offset to 1st field
517	**1**	**10**	Record offset to 2nd field
518	**1**	**25**	Record offset to 3rd field
519	**1**	**31**	Record offset to 4th field
520	**1**	**46**	Record offset to 5th field
521	**1**	**49**	Record offset to 6th field
522	**1**	**51**	Record offset to 7th field
523	**1**	**56**	Record offset to 8th field
524	**1**	**57**	Record offset to 9th field
525	**1**	**74**	Record offset to 10th field
526	**1**	**88**	Record offset to 11th field
527	**1**	**104**	Record Size

Figure 8. Database Table Header Format, (AIT, 2005).

TCMD Data

The Transportation Control Management Document (TCMD) data utilizes the 80-character MILSTRIP record format, with a limit of 79 TCMD records in total, starting at extended memory address 124731. Unlike the license plate data, the TCMD records do not require the carriage return and line feed combination.

Database Data Types and Record Format

The commodity item and single item database consist of an 1150 record maximum, with each record consisting of 104 characters, starting at extended memory address 528. These records may be one of two types, namely, commodity item records or single data item records. The commodity item records are the preferred format and are detailed in figure 9.

Commodity Item Database Record Format Values

Record Offset	Field Length	Database Table Name	Field Name	Example
00	10	NOMENCLATR	Nomenclature	Rockets
10	15	DOCUMENT	Document Number	WK4F4250120003
25	6	LIN	Line Item Number	000123
31	15	NSN	National Stock Number	
46	3	ICP RIC	Routing Identification Number	
49	2	UNIT_ISSUE	Unit of Issue	
51	5	QUANTITY	Quantity Shipped	
56	1	COND	Condition Code	
57	17	INT_TCN	Intermediate TCN	
74	14	MISC1	User Defined Data	
88	16	MISC2	User Defined Data	

Example of Commodity Item Database Record

00	01	02	03	04	05	06	07	08	09
R	O	C	K	E	T				

10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
W	K	4	F	4	2	5	0	1	2	0	0	0	3	

25	26	27	28	29	30
0	0	0	1	2	3

Figure 9. Example of the Commodity Item Database Record Format, (AIT, 2005)

The single item database records are used for items not found in the commodity item database. While the 104 character record may be freely defined, typically such entries utilise the 14-character MISC1 field and 16-character MISC2 field, demonstrated in figure 10.

MISC 1	MISC 2
SERVICE	ARMY
CONTAINER NUM	51547
OPERATION	DESERT STORM
HAZMAT CODE	E

Figure 10. Example of Single Data Item Entries in Database, (AIT, 2005).

412 TAGS

Unlike the aforementioned tags the 412 tag has no support for extended memory, instead consisting of 4096 bytes of serial Electrically Erasable Programmable Read Only Memory (EEPROM) for standard memory, with space for 17 single or commodity item records and 19 TCMD records (Bista, 2006). The EEPROM is further divided into simulated standard memory of 109 bytes and simulated extended memory of 3987 bytes, providing for compatibility with the 410 tags. As an additional benefit the firmware used by the 412 tags adds an additional layer of security that restricts access to certain areas of memory. The emulation of a 410 tag is illustrated in figure 11.

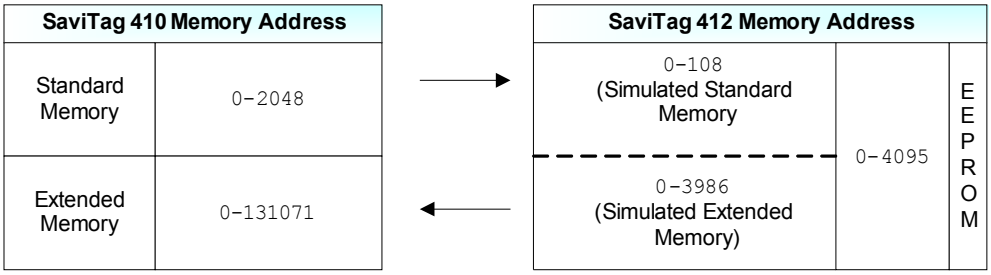

Figure 11. Emulation of a 410 tag, (AIT, 2005)

SECURITY ISSUES

While the clear text nature of this format allows for easy usage with HIH units in the field, this in no way makes up for the lack of security features. The level of unrestricted information available in the license plate data format in combination with TCMD records poses a real threat to operational security. For example, the sustainment data format holds critical shipment information including the Point of Embarkation (POE) and Point of Debarkation (POD), carrier and consigner codes, transport priority and a vast array of shipment details. Such information may be used to ascertain likely troop numbers and movements.

The format also leaves the systems highly vulnerable to man in the middle threats, counterfeiting and theft. If an unauthorised party was to scan a unit movement tag they would immediately garner highly specific logistical information including equipment descriptions, model and serial numbers. Such data would aid in the identification of critical equipment for sabotage or theft. Counterfeiting in America according to DNA Technologies is responsible for the loss of 750000 jobs and over $200 billion of lost revenue per year (Pearson, 2006). Whilst US $20-60 billion is lost annually due to cargo theft, highlighting the level of security concerns related to such items (Tata Consultancy Service Limited, 2006).

The DoD supply chain operates by placing an active RF-tag on a desired container, which the sends item information to a national Independent Television (ITV) server for tracking purposes. The tracking locations are updated when a ground-based or handheld reader collects the tag information, consequently sending tag information to be updated at the ITV server. A number of threats are posed in this supply chain including false tracking, and confusion resulting from falsely labelling containers. False tracking can be achieved by removing the RF-tag from the container to a new location or by changing tag information such as the Tag ID. This Results in false information being sent to the ITV server, which affects the integrity and reliability of item tracking. Such

tracking may be achieved through currently available software such as RF-DUMP which allows the attacker to write their own globally unique tracking ID to unlocked memory on a tag.

Furthermore if tag information is modified or erased, a container full of ammunition could have all item related information erased. This threat is reminiscent of the situation in the Gulf War when thousands of containers with unknown contents stayed in Saudi Arabia, meaning every container had to be physically searched, this resulted in a bottleneck in supply distribution, and had impacts on operational decisions (Davis, 2005).

CONCLUSION

The current global situation requires the US military to perform ongoing supply operations to multiple active theatres of war. Overriding any concerns of cost, the efficient management and transfer of necessary equipment and supplies may be the difference between life and death. The aim of these standards is to aid the United States Department of Defence by increasing the efficiency between logisticians and suppliers and thus hopefully resulting in a faster, more efficient supply chain (Davis, 2004).

Unfortunately, the level of security specified in the RF-Tag Data Format 2.0 is almost non-existent. Information including shipment details, arrival/departure information, potential ammunition and unit movement data are all stored in clear text and thus vulnerable. Further, the standards fail to provide methods to prevent unauthorised users from modifying tag data, perhaps leading to serious logistical problems in hostile environments. While it is likely that later iterations of the standards will address these issues the current usage is of definite concern.

The implementation of the JDTAV format 2.0 into mainstream American working class will involve careful planning on all levels of security, even though the RFID industry only earned $300 million in 2004, revenues have been forecast in excess of $28 billion by 2009 (Smith, 2004). The cost of implementation is a big issue and the end product must justify the purpose, with tag prices varying from USD 20-50 cents, readers costing USD $1000-$3000 and RFID related antennas costing USD $250+ (Perset, 2005). Due to such equipment costs, a standard format with inherently sound security options is required, or money spent on implementation will be lost to security threats.

REFERENCES

AIT. (2005). *RF-Tag Data Format Specification - Version 2.0*. Fort Belvoir: Department of Defense Logistics Automatic Identification Technology Office.

Bolan, C. (2005). Radio Frequency Identification - A Review of Low Cost Tag Security Proposals. *Proceedings of the 3rd Australian Computer, Network & Information Forensics Conference*. Perth, Western Australia: School of Computer and Information Science, Edith Cowan University.

Bista, B. (2006). *Compact Flash Memory and Data Recovery*. Retrieved October 2006, from

http://www.articles-hub.com/Article/Print/79214.html.

Davis, H. (2004). *RFID technology: is the capability a boon or burden for DoD?*. Retrieved October 2006, from http://www.findarticles.com/p/articles/mi_m0IBO/is_4_28/ai_n13797629/pg_1.

EETimes. (2004). DoD spending bill includes nanotechnology funds. Retrieved 25/04/2005, from http://www.eetimes.com/news/latest/showArticle.jhtml;jsessionid=ENI1XXCLQQGI4QSNDBCSKHSCJUMEKJVN?articleID=25600219&_requestid=673339

Juels, A. (2006). *RFID Security and Privacy: A Research Survey*. Retrieved October 2006, from http://ieeexplore.ieee.org/iel5/49/33490/01589116.pdf.

Pearson. (2006). Increasing Security in the Supply Chain with Electronic Security Markers. Retrieved October 2006, from http://www.rfidjournal.com/whitepapers/1.

Perset, K. (2005). *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations*. Retrieved October 2006, from http://www.oecd.org/dataoecd/57/43/36323191.pdf.

Peris-Lopez et al. (2006). *RFID Systems: A Survey on Security Threats and Proposed Solutions*. Retrieved October 2006, from http://lasecwww.epfl.ch/~gavoine/download/papers/PerisHER-2006-pwc.pdf.

Smith, R. (2004). RFID: A Brief Technology Analysis. Retrieved October 2006, from http://www.rfidconsultation.eu/docs/ficheiros/RFID_analysis.pdf.

Tata Consultancy Services Limited. (2006). Stop Getting Strangled by your Supply Chain.

Wynne, M. W. (2003). Update for Policy for Unique Identification (UID) of Tangible Items. Retrieved 25/04/2005, from http://www.acq.osd.mil/dpap/Docs/uid/Signed%20memo%20and%20attachments.pdf

COPYRIGHT

Uros Urosevic & Christopher Bolan ©2006. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors