Reports and Technical Reports | Faculty and Researchers' Publications

2015-01

Towards MIL-STD-1553B covert channel analysis

Nguyen, Thuy D.

Monterey, California. Naval Postgraduate School

https://hdl.handle.net/10945/44707

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

TOWARDS MIL-STD-1553B COVERT CHANNEL ANALYSIS

by

Thuy D. Nguyen

January 2015

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 15-01-2015	**2. REPORT TYPE** Technical Report	**3. DATES COVERED** *(From-To)*

4. TITLE AND SUBTITLE TOWARDS MIL-STD-1553B COVERT CHANNEL ANALYSIS	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Thuy D. Nguyen	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER** NPS-CAG-15-001
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

The views expressed in this material are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

14. ABSTRACT

Covert channel analysis is a critical, yet challenging, security engineering task. Despite numerous descriptions of covert channel attacks on ground-based systems and networks, such attacks have not been examined in the context of data bus protocols used in commercial space platforms hosting government payloads. Our contribution is to identify relevant concerns that have yet to be addressed in this domain, largely due to the lack of security requirements for hosted payload space applications. In this paper, we describe a policy-driven threat model and then develop hypothetical attack scenarios in the context of the MIL-STD-1553B protocol. Our initial analysis identifies several covert timing and storage channels.

15. SUBJECT TERMS

Covert channel, cross domain, multilevel security, MIL-STD-1553B

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Thuy D. Nguyen
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	35	
Unclassified	Unclassified	Unclassified			**19b. TELEPHONE NUMBER** *(include area code)* (831) 656-3989

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Ronald A. Route   Douglas A. Hensler
President   Provost

The report entitled "*Towards MIL-STD-1553B Covert Channel Analysis*" was prepared
for the Cyber Academic Group at the Naval Postgraduate School.

Further distribution of all or part of this report is authorized.

This report was prepared by:

_____
Thuy D. Nguyen
Faculty Associate – Research
Department of Computer Science

Reviewed by: **Released by:**

_____   _____
Cynthia E. Irvine   Jeffrey D. Paduan
Chair of Cyber Academic Group   Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Covert channel analysis is a critical, yet challenging, security engineering task. Despite numerous descriptions of covert channel attacks on ground-based systems and networks, such attacks have not been examined in the context of data bus protocols used in commercial space platforms hosting government payloads. Our contribution is to identify relevant concerns that have yet to be addressed in this domain, largely due to the lack of security requirements for hosted payload space applications. In this paper, we describe a policy-driven threat model and then develop hypothetical attack scenarios in the context of the MIL-STD-1553B protocol. Our initial analysis identifies several covert timing and storage channels.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I.   INTRODUCTION

With the ever-increasing reliance on space-based communications, satellites have become targets of cyber attacks. The 2011 Report to Congress by the U.S.-China Economic and Security Review Commission warned, "Malicious actors can use cyber activities to compromise, disrupt, deny, degrade, deceive, or destroy space systems. Exploitations or attacks could target ground-based infrastructure, space-based systems, or the communications links between the two." The Report highlighted several suspicious cyber events that interfered with two U.S. Government satellites as evidence of cyber attacks directed against U.S. satellites in 2007 and 2008. The U.S. Geological Survey and National Aeronautics and Space Administration confirmed the attacks on two earth observation satellites Landsat-7 and Terra EOS AM-1, respectively. In both cases, the intruders could have taken over the satellite but did not issue commands to do so [1]. It is unknown whether or what kind of malware was planted on these satellites for future Advanced Persistent Threat activities.

In response to new fiscal realities, the U.S. space community has embraced the innovative re-use of commercial space platforms (SP) to host mission payloads. These new strategies promise to reduce cost while providing shorter mission cycles and faster access to space [2]. The CHIRP program was the first to use a commercial communication satellite to host a government payload [3]. Following the success of CHIRP, the U.S. Air Force issued a multiple-award contract under the Hosted Payload Solutions (HoPS) program to acquire on-orbit and ground services for government-furnished hosted payloads (HPs) on commercial space platforms (SPs) [4]. The HoPS program specifies two reference mission architectures for protected HPs: embedded and dedicated-link. For the embedded HP architecture, the HP transfers its commanding and telemetry streams via the SP's commanding and data handling subsystem. For the dedicated-link architecture, the HP transfers its commands and data through a dedicated transponder channel provided by the SP. In both cases, a government-supplied Hosted Payload Interface Unit (HPIU) provides cryptographically-enforced separation between the protected HP and the SP. The HPIU can support MIL-STD-1553B, SpaceWire and RS-422 buses [5].

The HoPS program plans to use encryption to prevent any information leakage from the HP in violation of system policy. In the case of government hosted payloads requiring stringent confidentiality protection, the system's policy is naturally expressed as a mandatory information flow control policy (i.e., no read-up and no write-down with respect to levels of confidentiality). It is well-known that encryption is not sufficient to control all possible flows in a mandatory access control policy: covert and side channels may still exist in the presence of shared resources, e.g., the data buses between the HPIU and the space platform [6]. A covert channel allows two cooperating entities to communicate secretly by manipulating shared resources, in violation of the security policy [7,8]. In contrast, a side channel leaks information to other parties, and does not require the cooperation of some malicious entity on the high side. For example, two cooperating remote terminal (RT) devices on a MIL-STD-1553B bus may be able to modulate metadata using valid protocol operations to transfer information in unexpected and unintended ways, illegally and undetectably.

In this work, we perform a preliminary study of protocol-based covert channels on the MIL-STD-1553B (1553B herein) data bus. These channels include those exploitable via misuse of protocol options, unused or undefined fields in a protocol data unit, or timing behavior. Our general strategy employs the *flaw hypothesis methodology* [9,10,11] to identify potential storage and timing channels through analysis of the 1553B standard and documentation of various 1553B products.

Our work focuses on covert channel attacks against data bus protocols used in satellites with cross-domain capabilities, i.e., those hosting payloads operating at different sensitivity levels. Both types of channel may admit clandestine exfiltration of critical data in violation of the intended system policy. Our objective is to begin the process of identifying unexpected channels in hosted payload systems, laying the groundwork for mitigation techniques useful in real-world scenarios, i.e., to eliminate or constrain attacks against hosted payloads launched from a Trojan within the payload itself or from a compromised platform hosting the payload.

In this paper, we define covert channels in the context of 1553B protocol, discuss the threat model and hypothesized attack scenarios, and present some initial findings of this analysis.

II.   BACKGROUND AND DEFINITIONS

The 1553B bus architecture [12, 13] is the focus of our study due its maturity and utilization in U.S. space systems. A 1553B system is comprised of a bus controller (BC) and one or more remote terminals (RT), connected by a serial data bus. Bus management is accomplished via a strict master-slave relationship between the BC and RTs. Optionally, there may be one or more bus monitors (BM) that can passively monitor and record traffic on the bus. A mission-critical system typically utilizes several 1553B buses to provide multiple data paths for redundancy [14, 15]. A 1553B subsystem is a functional unit of an RT that sends or receives data from the data bus [16].

The time division multiplexing, half-duplex command/response protocol defined in MIL-STD-1553B is commonly used in spacecraft on-board data handling. All bus transmissions are accessible to all units connected to the bus, but only one unit can "speak" at a time. The BC initiates all bus transfers by sending a command message to individual RTs, and each RT is required to respond with a message acknowledging receipt of the BC's message.

For the purposes of this study, we adopted the definition of a covert channel from *A Guide to Understanding Covert Channel Analysis of Trusted Systems* [17], which states that a covert channel is "a communication channel that allows a process to transfer information in a manner that violates the system's security policy." Other definitions exist. For example, Schaefer et al. stated that a covert communication channel exists if it is based on "transmission by storage into variables that describe resource states" [18]. This definition, however, is specific to the storage of variables and its context is only meaningful for a stateful operating system. Kemmerer defines covert channels as those that "use entities not normally viewed as data objects to transfer information from one subject to another" [19]. While this definition is more generic and can be applied to stateless networks, it does not address the notion that covert channels depend on a system's security policy and how the system implements that policy. In this work, our use of the term 'side channel' is more closely aligned with Kemmerer's (policy-agnostic, unexpected) communication channels, whereas we reserve the term 'covert' to describe channels used by entities to violate an information flow policy.

As applied to the 1553B protocol, the applicable security policy is a traditional mandatory access control policy in which the active entities with the potential to cause information flow, viz. subjects, map to the units connected to the 1553B bus, and "information" maps to *data words* defined in the 1553B protocol. The data transmitted via 1553B data words are specifically distinguishable from other information defined in the 1553B protocol in that the contents of data words are not interpreted by the 1553B protocol in any way, i.e., have no semantic meaning to the protocol.

This may be contrasted with other aspects of the 1553B protocol such as *command words* and *status words* that define the formats and semantically meaningful control information that form the basis of the protocol. In this context, "covert channel" refers to the illegal flow of information effected via 1553B protocol constructs.

We also adopted Kemmerer's definitions of storage channels and timing channels. Specifically, a covert channel is a storage channel if "the sending process alters a particular data item, and the receiving process detects and interprets the value of the altered data to receive information covertly." A covert channel is a timing channel if "the sending process modulates the amount of time required for the receiving process to perform a task or detect a change in an attribute, and the receiving process interprets this delay or lack of delay as information" [19].

III. THREAT MODEL

The 1553B standards specify three types of validation testing that a 1553B unit must pass to ensure conformance to the 1553B specification: electrical, protocol, and noise reduction [14]. Passing the validation tests does not guarantee that the design and implementation of a bus unit is trustworthy or free of unintended leakage channels. Furthermore, malicious software can be inserted during initial development, or intercepted and modified in the supply chain, either creating or exploiting channel vulnerabilities. This is a concern for all cross-domain systems and, in particular, is explicitly required by the *Cross Domain Solution Overlay* in the U.S. [20]. Our analysis is intended to inform relevant concerns that have yet to be expressed in this domain, i.e., due to the lack of an overlay for hosted payload space applications.

For protected hosted payload missions, the critical payload data are encrypted. However, the protocol metadata in a 1553B message are transmitted in the clear on the data bus. Our covert channel analysis focuses on this type of data to find illegal communication channels between 1553B units connected on the same bus (see Figure 1).
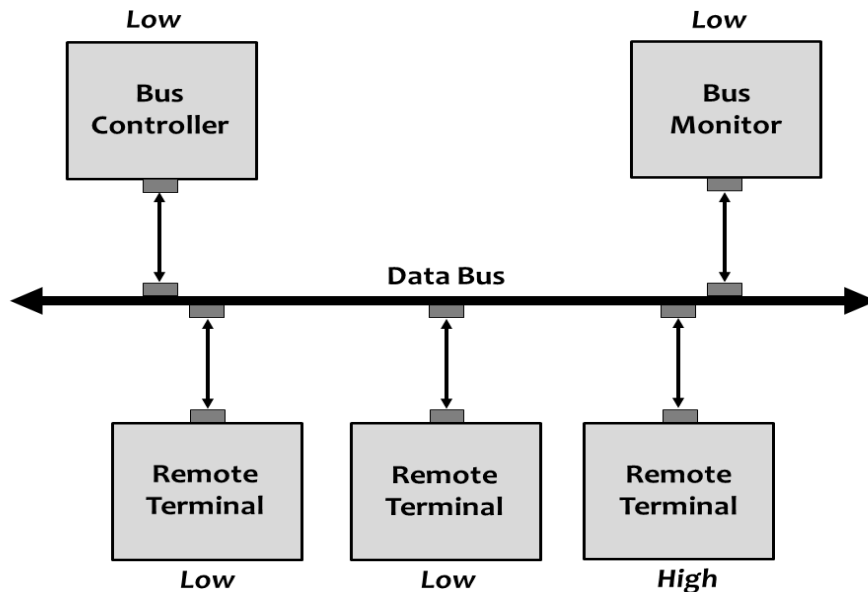

Figure 1. Notional 1553B architecture.

In our analysis, we use the traditional multilevel security (MLS) confidentiality policy as modeled by Bell and LaPadula [21]. This policy disallows the flow of information from a unit operating at a high level of confidentiality and a unit operating at a low level of confidentiality.

We began our analysis drawing from the threat models and hypothesized attack scenarios outlined in Table 1. A participating unit may be the BC, BM, or an RT. For our analysis, channels associated with cooperating units are called 'covert channels' whereas channels associated with active and passive monitoring are called 'side channels.' Side channels can be exploited to leak information without the aid of a malicious entity on the high side. Channels that require persistent physical access to exploit—such as channels exploitable via differential power analysis—are out of scope of our analysis; we believe these to be difficult to exploit via malicious software or firmware and, thus, may be unrealistic attack to consider against remote, space platforms.

Table 1. Threat models

Threat models	*Attack scenarios*		
	Storage channel attacks *Observation of protocol control information using valid protocol operations*	*Storage channel attacks* *Observation of RT-specific protocol control information using RT implementation-specific operations*	*Timing channel attacks* *Observation of RT-specific timing behavior*
Covert channel	Cooperating units use valid protocol operations to transmit information via protocol control fields. See Section IV.C.	Cooperating units use unit-specific protocol behavior to transmit information via protocol control fields. See Section IV.B.	Cooperating units use unit-specific timing behavior to transmit information. See Section IV.A.
Side channel (active monitoring)	Attacking unit (BC or RT) induces target RT into disclosing information via protocol control fields using valid protocol operations.	Attacking unit (BC or RT) utilizes behavior unique to target RT to induce disclosure of information.	Attacking unit (BC or RT) probes target RT by creating specific protocol conditions and observing target RT timing behavior.
Side channel (passive monitoring)	Attacking unit (BC, BM or RT) infers activity of target RT by monitoring protocol control fields.	Attacking unit (BC, BM or RT) infers activity of target RT by monitoring target RT-specific protocol control fields.	Attacking unit (BC, BM or RT) infers activity of target RT by monitoring target RT timing behavior.

The exploitable "protocol control information" refers to any 1553B-defined control and status fields; 1553B-defined data payload fields are specifically excluded. Construction of timing channel attacks does not distinguish the use of valid protocol operations versus invalid and incorrect protocol operations since it is assumed all timing behavior of a specific RT is unique.

Examples of design conditions that could potentially be exploited include: 1) out-of-spec exception handling, such as the incorrect use of the subaddress field for data wraparound; 2) undefined behavior, such as how the BC and RTs handle undefined error conditions, optional parameters and optional commands; and 3) bus control and monitoring—for example, considering acyclic data transfer vs. scheduled data transfer by RTs, or considering recording-only (passive) bus monitors vs. hybrid bus monitors (i.e., able to serve as a back-up bus controller).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDIES

This section describes three examples of the storage and timing covert channels shown in Table 1. The side channel scenarios (shaded in Table 1) are beyond the scope of this paper.

A. TIMING CHANNEL – RT RESPONSE TIME DELAY

This channel allows two cooperating RTs running at different security levels to use RT-specific timing behavior to transmit and observe information.

In a 1553B system, the BC initiates all commands and each RT must respond to a valid command within a time period of 4 to 12 microseconds [12]. Since every connected RT can observe all transmissions on the data bus, one RT can identify all commands sent by the BC to another RT and all responses returned by the target RT. This allows for the existence of a potential timing channel in which a Low RT (receiver) could detect the covertly transmitted information by monitoring the response time delay introduced by a malicious High RT (sender). The signaling mechanism would be the amount of time delayed by the High RT before responding to a command.

Within the allowable response time period (4-12 microseconds), if a High RT is capable of controlling the response time delay to a granularity of one microsecond, it can leak up to three bits of information per message. A number of 1553B products provide board-level APIs that allow applications to set the RT response time to a granularity of nanoseconds [22, 23, 24].

Figure 1 illustrates an example 1-bit timing channel scenario in which the High RT varies the response time to send different bit values. For normal transmissions in this example, the High RT responds to a command in four microseconds. To signal 0 and 1, the High RT increases the response time to eight and twelve microseconds, respectively. The Low RT extracts the leaked information by measuring the time it takes the High RT to respond to a valid command.
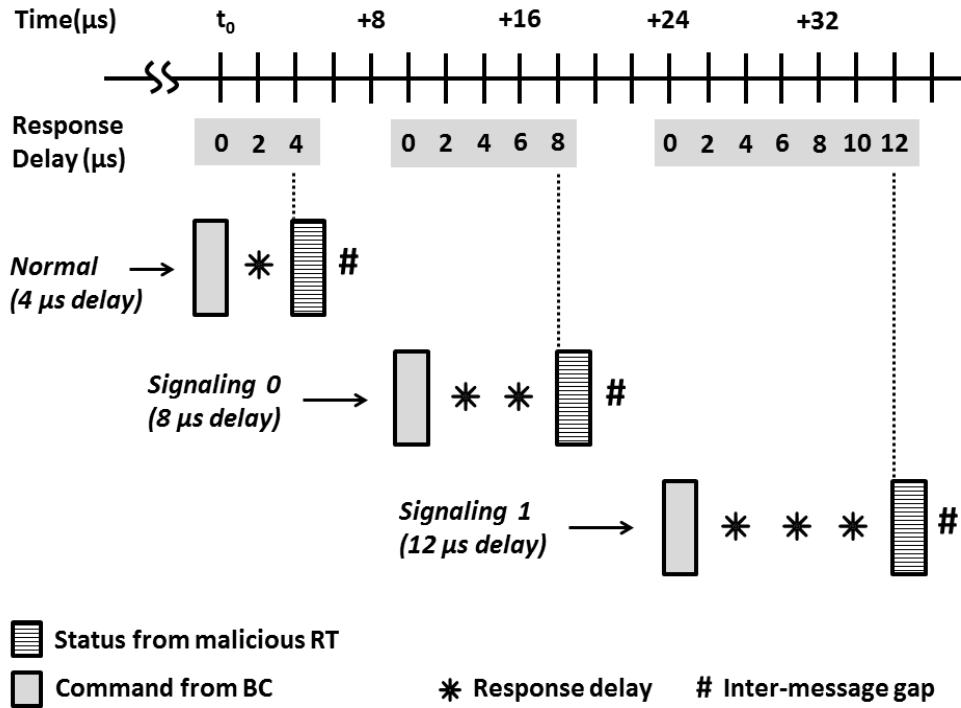
Figure 2. RT response delay timing channel.

To exploit this channel, a malicious High RT must be able to generate delays of arbitrary length before responding and a Low RT must have the ability to measure the response delays. A typical timing channel requires the sender and receiver to have either a common clock or the ability to create a time reference [17]. For this timing channel, the colluding RTs can use the end of a BC command as the common time reference. Synchronization between the two RTs can start after a command word is detected; a command word is always preceded by an inter-message gap of at least 4 microseconds (introduced by the BC), and consists of: a 3-bit sync pattern, sixteen bits of information, and one parity bit.

Another requirement of this channel is that the delay length used as the signaling mechanism needs to be sufficiently large relative to the RT's internal clock period to minimize or eliminate erroneous transmissions.

B.   STORAGE CHANNEL – COMMAND ILLEGALIZATION

This channel allows two cooperating RTs to use RT-specific implementation behavior to leak information via protocol control fields. Command *illegalization* is one such behavior.

An illegal command is a valid command that is not in the set of commands specified for use with the target RT [14]. The set of illegal commands that an RT supports is typically defined by the RT's subsystem via a programming interface provided by the RT core engine, and is kept in an illegalization database in memory [25, 26].

A compliant BC only issues valid commands but, depending on its design, an RT may treat certain commands as illegal and will return a status word with the message error (ME) bit set when such commands are detected. In this case, the RT will discard any information received with the command or disregard the request for information specified in the command [12]. Note that for other error conditions, the RT will set the ME bit in the status word but does not send the status word until the BC explicitly asks for it via a mode command (i.e., Transmit Status or Transmit Last Command).

Although not required by the 1553B standards, a BC can automatically retry the issued command when it receives a status word response for that command with the ME bit set [14]. Different variations of automatic retrying exist. A BC can be programmed by the subsystem to retry a command multiple times on the same data bus or on the alternate bus of a redundant pair of data buses [27]. Another implementation can retry different number of times on the same bus and on the alternate bus, or retry alternately between the two busses for the same number of times [28].

For our analysis, we assume that the BC implements automatic retrying and the High RT supports command illegalization. The BC must retry at least once on the same bus and the High RT must be able to dynamically reject an arbitrary command as illegal.

The High RT and Low RT must previously agree on when the signaling method will be utilized. For example, the agreement can be based on a specific command or commands sent from the BC. Whenever the BC sends a specific command to the High RT, the High RT will signal a bit by selectively rejecting the command or accepting the

command (see Figure 3). The Low RT observes the High RT's action to receive the transmitted bit.
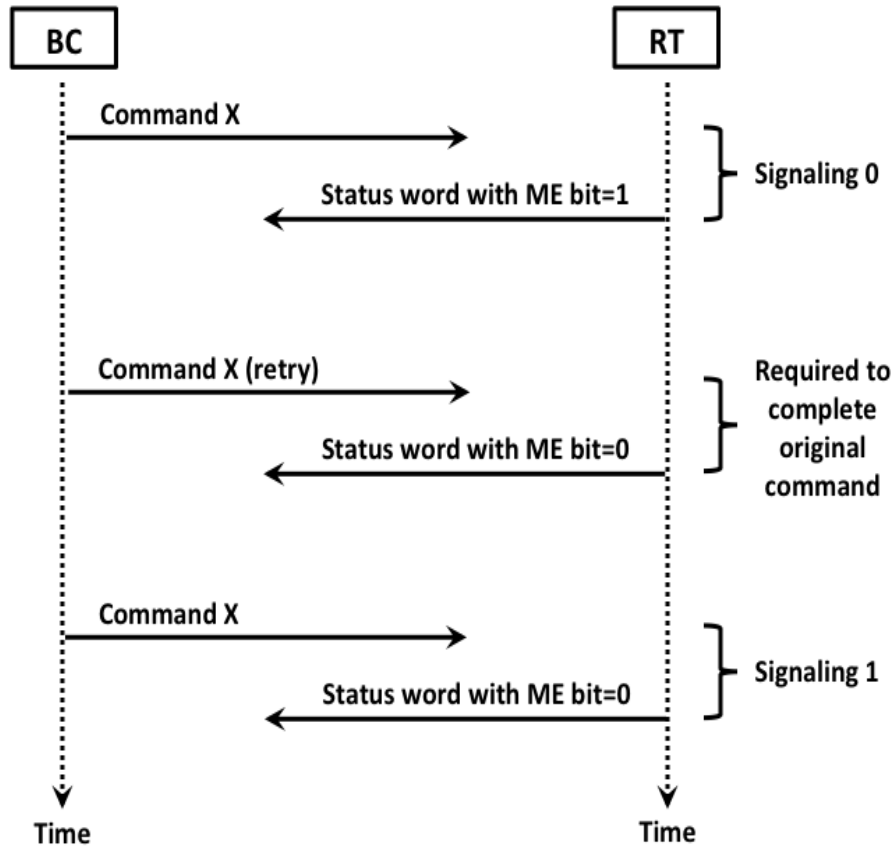

Figure 3. Command illegalization storage channel.

To signal 0, the High RT rejects as illegal a command issued from the BC. When the BC resends the command, the High RT accepts the command and responds normally. The retry from the BC and subsequent normal response from the High RT is necessary to implement the routine operation of the High RT after the High RT falsely rejected the initial BC command as illegal in order to signal a bit value of 0.

To signal 1, the High RT simply responds normally to a command issued from the BC.

This method may be extended to utilize an arbitrary set of commands to signal information. The ability to signal information depends on how often the BC issues the commands that will be used to perform a signaling action. The High and Low RTs can use a defined set of commands to create a larger covert channel alphabet.

12

C.   STORAGE CHANNEL – ACYCLIC TRANSFER

The previous scenario demonstrates an illicit information flow based on an optional but commonly implemented RT feature. Another storage channel can be constructed using the Service Request (SR) bit in the status word. This channel enables two cooperating units to transmit information using valid protocol operations.

In a 1553B system, the BC periodically issues commands to the RTs in a cyclic sequence. The list of commands is predefined and stored in the BC's local memory. To support systems with a need for time-critical asynchronous data transfers, the 1553B standards affords the RT the ability to request the BC to perform operations that are not prescribed in the command list.

When an RT wants to request an acyclic data transfer, it returns a status word with the SR bit set. Depending on the system design, when the BC detects the Service Requested condition, the BC either executes a predefined function or sends a Transmit Vector Word command to obtain additional information from the RT about the requested service. After receiving this command, the RT sends back a vector word specifying the type of service it needs with the SR bit cleared in the associated status word. The RT can request additional services repeatedly by keeping the SR bit set in all subsequent status words until all required services are done [14].

For our analysis, we hypothesize that the BC responds to an asynchronous service request by issuing the Transmit Vector Word mode command, after which the RT responds by transmitting a vector word. The RT may continue to issue asynchronous service requests, and continue to respond to Transmit Vector Word commands from the BC, until the RT sends a vector word that contains all zeroes and discontinues setting the SR bit.

The Low RT receives bits from the High RT by observing the way the High RT issues an asynchronous request. If the High RT follows up the request with transmission of a non-zero vector word, the Low RT knows the High RT is merely performing a legitimate asynchronous request action. If the High RT transmits a single empty vector word, the Low RT interprets the High RT's action as transmission of a bit value of 0. If

the High RT transmits two consecutive empty vector words, the Low RT interprets the High RT's action as transmission of a bit value of 1. Figure 4 illustrates this technique.

To signal 0, the High RT sets the SR bit in the status word returned for an arbitrary BC command. The BC responds by issuing a Transmit Vector Word command. The High RT then immediately transmits an empty (all zeros) vector word with the SR bit cleared. The Low RT observes the High RT's action to receive the bit value of 0.
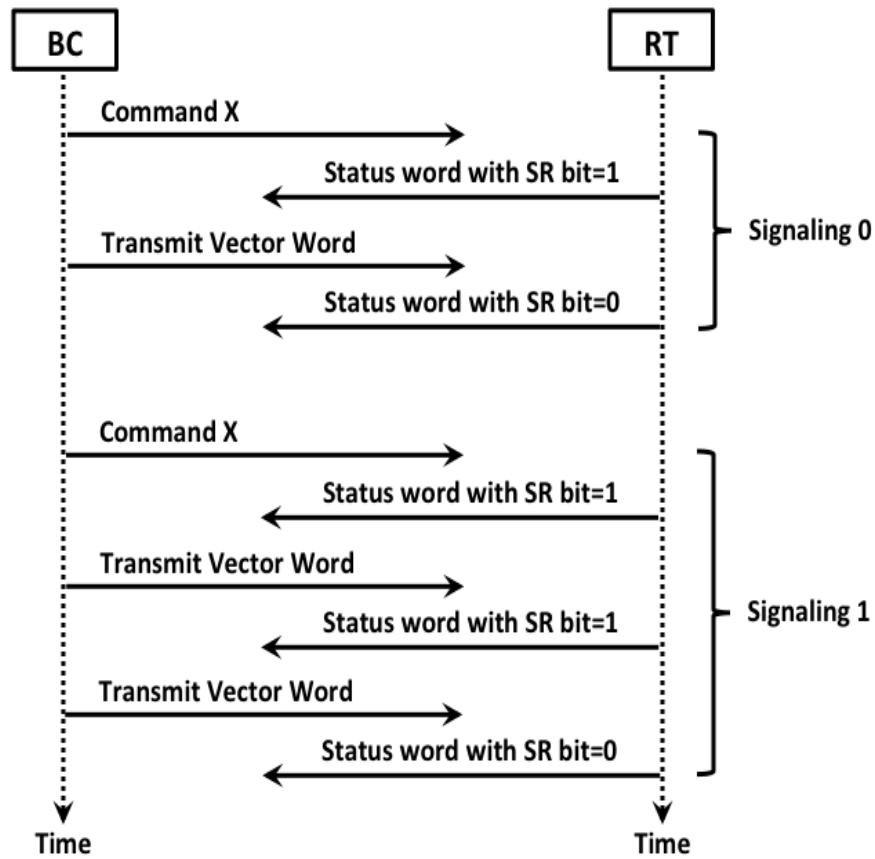

Figure 4. Acyclic transfer storage channel.

In the case that the High RT needs to issue a valid asynchronous service request, the High RT would have transmitted a vector word that contained valid data (non-zero value). The Low RT is able to distinguish the High RT's valid service request action from transmission of the bit value of 0 by observing the contents of the vector word.

To signal 1, the High RT performs a similar action to signaling a 0 bit by setting the SR bit and transmitting an empty vector word. But instead of clearing the SR bit, the High RT sets the SR bit a second time. The BC will discard the vector word because it

14

contains all zeroes, but will issue the High RT a second Transmit Vector Word mode code because the SR bit was set again. The High RT then transmits a second empty vector word and clears the SR bit.

Depending on the behavior of the BC, this method could be extended to transmit multiple bits of information by transmitting additional empty vector words before clearing the SR bit.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

This paper describes the initial findings of our study of covert channels in a 1553B system. We have shown that it is possible to construct timing and storage channels by observing timing behavior, protocol control information, and RT-specific implementation features.

We plan to study the three channels described in Section IV in more depth, and to analyze other potential covert and side channels identified in Table 1, exploring their characteristics through empirical study. This work will include estimation of the rate at which information can be sent over each channel and the feasibility and degree to which each channel can be exploited, calculating the channel capacity, and measuring the signal-to-noise ratio.

We need to further explore methods to close or mitigate these channels. A brute force approach to handle the two identified storage channels is to disallow the use of illegalization and asynchronous service request; they are optional functionality at the protocol level. However, applications may require support for selected optional protocol operations to meet mission-critical needs. Alternatively, a known method of handling covert channels is to implement an audit mechanism that can detect the exploit of a channel. Utilizing a bus monitor to observe and collect traffic on the bus may provide a way to recognize suspicious behavior, after which mitigating action may be taken.

The increasingly popular SpaceWire standard defines a suite of protocols for high-speed networks on spacecraft [29]. A natural progression from the lessons learned in our 1553B study is to investigate potential covert channels in various SpaceWire protocols, e.g., wormhole routing in SpaceWire routers.

We believe this work can help identify security requirements for building secure on-board communications components that can be used in satellite systems with cross domain capabilities such as HoPS. Understanding of the conditions under which different channels may exist, or could be exploited, can help address security risk in the adoption of the hosted payload approach.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] U.S.-China Economic and Security Review Commission, "2011 Report to Congress of the U.S.-China Economic and Security Review Commission," November 2011.

[2] United States Government Accountability Office, "2013 Annual Report: Action Needed to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits," GAO-13-279SP, April 2013.

[3] Andraschko, M.; Antol, J.; Horan, S.; Neil, D., "Commercially hosted government payloads: Lessons from recent programs," 2011 IEEE Aerospace Conference, pp.1-15, 5-12 March 2011.

[4] U.S. Air Force, "Space and Missile Systems Center awards first-of-its-kind hosted payload solutions contract," July 28, 2014. Available at: http://www.af.mil/News/ArticleDisplay/tabid/223/Article/486870/space-and-missile-systems-center-awards-first-of-its-kind-hosted-payload-soluti.aspx

[5] Space and Missile Systems Center, "Hosted Payload Standard Interface Specification (HPSIS)," Hosted Payload Office, United State Air Force, July 31, 2013.

[6] Michael A. Padlipsky, David W. Snow, and Paul A. Karger, "Limitations of End-to-End Encryption in Secure Computer Networks," The MITRE Corporation: Bedford MA, HQ Electronic Systems Division technical report ESD-TR-78-158, August 1978.

[7] B. W. Lampson, "A Note on the Confinement Problem," Communications of the ACM, 16:10, pp. 613-615, October 1973.

[8] Millen, J., "20 years of covert channel modeling and analysis," Proceedings of the 1999 IEEE Symposium on Security and Privacy, pp.113-114, 1999.

[9] Linde, R. R., "Operating System Penetration," in Proceedings of the National Computer Conference, pp. 361-367, 1975.

[10] Weissman, C., "Security Penetration Testing Guideline," Naval Research Laboratory, Unisys Government Systems, 12010 Sunrise Vally Drive, Reston, VA, tm - 8889/000/01, October 1993. Prepared under contract to NRL.

[11] Weissman, C., "Penetration Testing," in Abrams, Jajodia, and Podell, editors. Information Security: An Integrated Collection of Essays, pp. 269-296. IEEE Computer Society Press, Los Alamitos, CA, 1995.

[12] Military Standard MIL–STD–1553B: "Aircraft Internal Time Division Command/Response Multiplex Data Bus," September 21, 1978.

[13] Military Standard MIL–STD–1553B, Notice 1 – 4, February 1980 – January 1996.

[14] Department of Defense Handbook MIL-HDBK-1553A: "Multiplex Applications Handbook," November 1988.

[15] Department of Defense Handbook MIL-HDBK-1553A Notice 1 – 5, January 1993 – May 2013.

[16] Chris deLong , "AS 15531/MIL-STD-1553B Digital Time Division Command/Response Multiplex Data Bus," The Avionics Handbook, Ed. Cary R. Spitzer, Boca Raton, CRC Press LLC, 2001.

[17] V. Gligor, "A Guide to Understanding Covert Channel Analysis of Trusted Systems," NCSC-TG-030, National Computer Security Center, November 1993.

[18] M. Schaefer, B. Gold, R. Linde, and J. Scheid, "Program Confinement in KVM/370," Proceedings of the 1977 Annual ACM Conference, Seattle, Washington, ACM, New York, pp. 404-410, October 1977.

[19] R. A. Kemmerer , "Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels," ACM Transactions on Computer Systems, 1 (3), pp. 256–277, August 1983.

[20] United States Committee on National Security Systems, "CNSSI No. 1253 Security Categorization and Control Selection for National Security Systems, Appendix F Attachment 3, Cross Domain Solution (CDS) Overlay," September 2013.

[21] D. Bell and L. La Padula. "Secure Computer Systems: Unified Exposition and Multics Interpretation," Electronic Systems Division, USAF. ESD-TR-75-306, MTR-2997 Rev.1. Hanscom AFB, MA. 1976.

[22] AIM GmbH, "MIL-STD-1553 Interface Module Programmer's Guide," V22.9x Rev. A, May 2014.

[23] Alta Data Technologies LLC, "AltaAPI Software User's Manual," Rev I2, April 24, 2014.

[24] Excalibur Systems, Inc., "1553Px Family Software Tools Programmer's Reference," Rev C-4, July 2014.

[25] Microsemi Corporation, "Core1553BRM v4.0 Handbook," January 2014.

[26] Alta Data Technologies LLC, "AltaCore-1553 MIL-STD-1553 Protocol Engine Specifications/Users Manual," Rev G3, March 2014.

[27] Aeroflex Microelectronic Solutions, "MIL-STD-1553 UT1553 BCRTMP Data Sheet," August 2003.

[28] Actel Corporation, "Core1553BBC MIL-STD-1553B Bus Controller," December 2005.

[29] ECSS-E-ST-50-12C: "SpaceWire - Links, nodes, routers and networks," European Cooperation for Space Standardization, July 31, 2008.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, CA 93943