Next Generation Aircraft Architecture and Digital Forensic

Dustin Michael Mink
University of South Alabama
dmm1521@jagmail.southalabama.edu

Alec Yasinsac
University of South Alabama
yasinsac@southalabama.edu

Kim-Kwang Raymond Choo
University of South Australia
raymond.choo@fulbrightmail.org

William Bradley Glisson
University of South Alabama
bglisson@southalabama.edu

Abstract

The focus of this research is to establish a baseline understanding of the supervisory control and data acquisition (SCADA) systems that enable air travel. This includes the digital forensics needed to identify vulnerabilities, mitigate those vulnerabilities, and develop processes to mitigate the introduction of vulnerabilities into those systems. The pre-NextGen notional aircraft architecture uses air gap interconnection, non-IP-based communications, and non-integrated modular avionics. The degree of digital forensics accessibility is determined by the comparison of pre-NextGen Notional Aircraft Architecture and NextGen Notional Aircraft Architecture. Digital forensics accessibility is defined by addressing Eden's five challenges facing SCADA forensic investigators. The propositional and predicate logic analysis indicates that the NextGen Notional Aircraft Architecture is not digital forensic accessible.

Keywords (Required)

Digital Forensics, Security Strategies, Next Generation Air Transportations System, SCADA Forensics

Introduction

In today's digital and highly connected society, it is distressing that aircraft go missing or to fail for undetermined reasons. Recent compromised cybersecurity events have the public concerned about the security of the digital safety systems (Administration 2014; Committee 2015). The Federal Aviation Administration (FAA) is seeking to address the public safety concerns which include concerns falling within the context of cybersecurity within the Next Generation Air Transportations System.

In less than a two-year time span, there have been several high profile incidents that have raised concerns and, perhaps, speculation about aircraft cybersecurity. On Monday, March 24, 2014 Malaysian Prime Minister Mohamed Najib bin Abdul Najib Razak stated, it had to be assumed that flight ML370 had crashed into the sea with the loss of all on board (Administration 2014). 16 days prior, on Saturday, March 8, 2014, Malaysian flight ML370's Co-pilot, Fariq Abdul Hamid, announced a change of control from Subang Traffic Control Center (ACC) to HO Chi Minh ACC (MH370 2015). Flight ML370 was never heard from again 40 minutes after takeoff. Malaysia had the help of the world community in the form of a Joint Investigation Team (JIT), consisting of United States, Malaysia, Australia, China, United Kingdom, and France, yet found nothing more than a right wing flaperon of the Boeing 777 off the west coast of Australia. Some may question what digital system aboard was compromised that would allow such a large airliner to completely drop off the grid.

More recently, on February 9, 2015, Dyre malware was detected on the FAA infrastructure (Committee 2015). Approximately 4500 FAA machines were infected with the Dyre malware. It took 36 hours to contain the Dyre malware. Dyre is categorized as a downloader (Symantec 2015). A downloader is a type of malware; a malicious computer program that transfers malicious computer programs to the computer. Dyre is primarily used for financial gain by cybercriminals, but in the case of February 9, the FAA infrastructure was compromised. A plausible scenario could consist of the following activities: 1) the cyber-criminal sends spam emails, 2) victims open malicious link or attachment in phishing emails, 3) delivers main payload, 4) hijacks browser and sends banking credentials to attacker server, 5) may download additional spam modules from command and control server, 6) infected machines send phishing emails to other targets. The Dyre malware exploits the Microsoft Windows Kernel 'Win32k.sys' Local Privilege Escalation Vulnerability ((CVE) 2014); first seen in October 2014 ((CVE) 2014). While the malware does not appear to have impacted air traffic control systems, it did highlight a potentially exploitable threat. The identification of this threat appears to have contributed to prompting action.

As a result, the United States Government Accountability Office (GAO) was asked by Congress to review FAA's cybersecurity efforts (United States Government Accountability Office 2015). The GAO report entitled "FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transition to NextGen" was published in April 2015. Within the Next Generation Air Transportation System (NextGen) report, three cybersecurity challenges faced by the FAA were identified. The first challenge is to protect Air-Traffic Control (ATC) information systems. The second challenge is to protect aircraft avionics used to operate and guide aircraft. The final challenge is to clarify cybersecurity roles and responsibilities among multiple FAA offices. This paper addresses one of the three challenges facing the FAA in cybersecurity, namely: protecting aircraft avionics used to operate and guide aircraft.

The remainder of this paper is organized as follows. Section 2 summarizes relevant works within computer forensics, network forensics, and FAA's approach to NextGen. Section 3 reviews the methodologies by using Eden's five challenges facing SCADA forensic investigators. Section 4 discusses the results, which are a side-by-side comparison of the three pre-NextGen and NextGen notional aircraft architecture principles using Eden's five challenges. Section 5 gives a conclusive summary of the three hypotheses validity, and discusses further research on the digital forensics of NextGen Architecture.

Relevant Work

The three elements relevant to establishing a baseline understanding of SCADA systems used in air travel are computer forensics, network forensics, and airborne network design considerations. Computer based forensics concentrates on the host computing system to include the processor, busses, and memories. Network forensics concentrates on the protocols used to transmit data from one system (e.g. computer and other computing device) to another and the method used to store and process such data. Finally, the airborne network considerations include highly interconnected and ethernet networks in addition to the integrated avionics which include inter-process communication (IPC), if not fully virtualized network switches.

Computer Forensics

Computer forensics or computer forensic science is a subset of digital forensics, which is confined to the computer and typically focuses on digital storage (Noblett et al. 2000). Computer forensics allows evidence to be preserved from a computer which can be used in many situations, especially in court cases. Physical computer evidence includes chips, central processing units, storage media, monitors, and printers. Natural evidence includes logging, description, storage, and disposition. Physical computer evidence is not unique since forensics naturally handles physical evidence. On the other hand, data contained on the physical evidence is in a metaphysical electronic form and poses challenges to be addressed (Noblett et al. 2000). Computer forensics was used by the Federal Bureau of Investigation (FBI) in 1984. Two examples of early computer forensics used in evidence in criminal law are: 1) investigators were led to Sharon Lopaka's killer, Robert Glass by emails on Sharon Lopaka's computer and 2) a spreadsheet used to plan crimes recovered from Joseph E. Duncan III's computer showed premeditation and justified the death penalty (Casey 2009; Casey 2011).

In 1995, a United States Secret Service's survey determined 48 percent of agencies forensic laboratories and 68 percent were seizing computer evidence to be sent to external computer forensic laboratories. In addition to computer forensics being used in support of other civil or criminal proceedings, host-based forensics used in computer-based crime jumped 67 percent from 2002 to 2003 alone (Leigland and Krings 2004). The 2002 published book, "Computer Forensics", authored by Kruse and Heiser, defined a forensics methodology including the preservation, identification, extraction, documentation and interpretation of computer data (Kruse 2002). Law enforcement organizations are training officers and administrators for computer forensics. The industries are not doing the same with their professionals. There is a gap between law enforcement's rigid and lacking flexibility to meet jurisdiction obligations where industry is more flexible (Reith et al. 2002; Yasinsac et al. 2003). The jurisdictional system requires computer forensic evidence to be authentic, reliably obtained, and admissible (Adams 2012). Practices differ between countries, but most computer forensics are in compliance with Association of Chief Police Officers guidelines to help ensure the authenticity and integrity of evidence. Investigations are generally performed on static data rather than live computer systems (Casey 2011). However, early computer forensics were performed on live computer systems because of the lack of specialized tools. Analysis tools typically include manual review of media, windows' registry, cracking passwords, keyword searches, and extraction of e-mail and pictures. The standard digital forensic process is broken into four phases: acquisition, examination, analysis, and reporting (Kent et al. 2006). A number of techniques are used in computer forensics investigations such as cross-drive analysis where information found on multiple hard drives are correlated and can be used to map social networks (Otherwise known as link angles) (Casey 2009; Dunbar 2002; Garfinkel 2006; Geiger 2005; Halderman et al. 2009; Philipp et al. 2009). Another technique is recovery of deleted files and the possibility of a reconstruction of a hard drive. Criminals have used steganography to hide data within digital images. Steganalysis is used to glean information about steganographic through, in some cases, comparing hashes of the original and possibly changed images. Information stored within random access memory (RAM) must be recovered before power is lost because RAM memories are volatile. In some cases, the file system on the non-volatile secondary storage such as New Technology File System (NTFS) will persist part of RAM within a page file, which can be used to recreate RAM at the time of power lost The volatile natural of RAM can be slowed by cooling the RAM below -60 degrees Celsius. Regardless of the device being investigated recent research heightens interest in digital forensics by indicating that residual data is continuing to have an escalating impact in legal environments (Berman et al. 2015; McMillan et al. 2013).

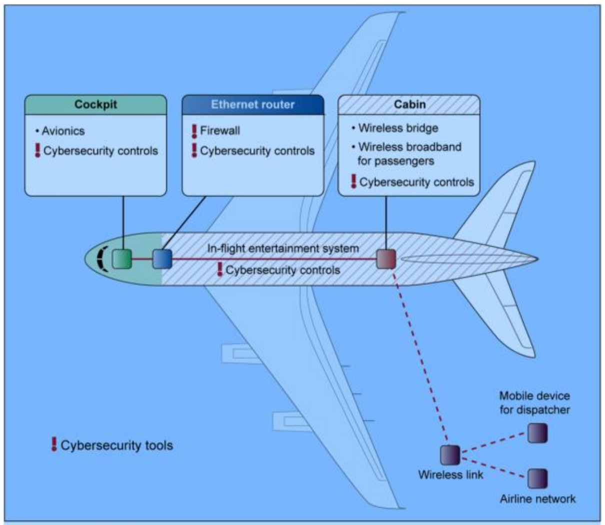
Network Forensics

Network forensics is also a subset of digital forensics (Casey 2011; Hjelmvik 2008; Palmer 2001; Ranum 2008). Network forensics analyzes the volatile and dynamic nature of computer network traffic. Captured network traffic can be used to analyze transferred file, email, and chat sessions. Captured network traffic is not dependent on computer forensics being available (Casey 2011; Hjelmvik 2008; Palmer 2001; Ranum 2008). Marcus Ranum defined network forensics as, "the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents" (Garfinkel 2002). Two methods of network collection for forensics use are: "catch-it-as-you-can" and "stop, look, and listen" (Garfinkel 2002). "Catch-it-as-you-can" captures all packets requiring vast amounts of data storage capacity. While "Stop, look, and listen" may not require vast amounts of data storage capacity, it does require more processing power in order to determine what packets to save.

Federal Aviation Agency Approach to NextGen

In October 2008, the Boeing Company conducted a study of the potential safety impacts introduced by networking local area network (LANs) onboard aircraft (Fleischman 2008). The study entitled, "The FAA Handbook for Networked Local Area Networks in Aircraft," proposed three airborne network design considerations: to move from a non-IP-based to IP-based communications, air gap to no air gap interconnection, and non-integrated to integrated modular avionics (Fleischman 2008). The FAA sponsored study encouraged aircraft manufacturers to increase networking onboard aircraft. On November 18, 2013, aircraft manufacturers applied for special conditions approval for their aircraft design to incorporate increasing networking onboard. A special condition is issued when an aircraft manufacturer employs new technologies, such as Internet Protocol (IP).

The FAA issued special conditions for the Boeing 777, 787, and Airbus A350 to address the increased interconnection among aircraft cockpit and cabin systems, and the inherent cybersecurity considerations (Administration 2007; U.S. Department of Transportation 2013a; U.S. Department of Transportation 2013b). The FAA aircraft-airworthiness certification does not address cybersecurity assurance (U.S. Department of Transportation 2015). The basic eligibility requirements for FAA aircraft-airworthiness certification are: 1) The aircraft must be airworthy, and 2) Any major alterations were accomplished in accordance with an approved Supplemental Type Certificate (STC), Type Certificate (TC), or other FAA-approved data. If altered while in another category, the aircraft continues to meet, or has been returned to, its approved type design configuration, 3) The aircraft complies with all applicable Airworthiness Directive (ADs), and any major repairs must conform to FAA-approved data or performed in accordance with bilateral agreement procedures. However, the FAA aircraft-airworthiness certification does have a special conditions part used for cybersecurity assurance and other topics. After many special conditions, on February 4, 2015, the GAO report entitled "FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transition to NextGen" was published (Office 2015). The report included an alternative notional aircraft architecture to address cybersecurity considerations. The alternative notional aircraft consists of three groupings, namely: the cockpit, ethernet router, and cabin (see Figure 1).



Source: GAO. | GAO-15-370

Figure 1. GAO's Notional Aircraft Architecture

The GAO report defines the cockpit to include flight guidance and control functionality through the use of avionics systems. The Ethernet router acts as a firewall to protect avionics systems located within the cockpit from attackers within the cabin. The cabin is the location where passengers use in-flight entertainment systems.

Forensics Methodology

Traditional forensics uses both computer and network forensics may apply to NextGen, but because of the nature of the NextGen-governed systems, many more challenges are introduced. Eden's five challenges facing SCADA forensic investigators are live forensics, rapid response, integrity and validity, incident relevant logs, and lack of SCADA forensic tools (Eden et al. 2015). Live forensics (LF) is accessing physical memories without the aid of the Application Programming Interface (API) while the system is still operating (Fabro and Cornelius 2008). Many SCADA systems cannot be turned off in order to perform digital forensics. A rapid response (RR) will minimize the time between when the incident occurred and the forensics response in order to mitigate the probability of data being overwritten (Taveras 2013). Digital evidence's Integrity and Validity (I&V) is verified by a digital fingerprint called a hash (Taveras 2013). The stored hash is taken at the forefront of the forensics process to be compared with the evidence in order to prove there was no evidence tampering. Incident relevant logs (IRL) help forensics investigators piece together the puzzle of the timeline of events by writing events to a file (Fabro and Cornelius 2008). Many systems have their logging disabled or logs are replaced before the logs can be used because of the lack of succedent data storage capacity. The lack of SCADA forensic tools (FT) has led to many SCADA system developers to incorporate proprietary communication protocols and log formats (Ahmed et al. 2012). The lack of transparency of SCADA systems due to their proprietary nature may have prevented the production of SCADA forensic tools.

The pre-NextGen notional aircraft architecture used air gap interconnection, non-IP-based communications, and non-integrated modular avionics. The degree of digital forensics accessibility is determined by the comparison of pre-NextGen Notional Aircraft Architecture and NextGen Notional Aircraft Architecture. Digital forensics accessibility is defined by addressing Eden's five challenges facing SCADA forensic investigators. Considering Eden's five challenges in conjunction with the architectures prompted the following hypothesis:

1. Hypothesis one (p1), the use of non-air gap interconnects is digital forensic accessible.
2. Hypothesis two (p2), the use of IP-based communications is digital forensic accessible.
3. Hypothesis three (p3), the use of integrated modular avionics is digital forensic accessible.

In order to conclude (q1), the NextGen Notional Aircraft Architecture is digital forensic accessible, all three premises have to be true. To validate each hypothesis, both propositional and predicate logic are applied to the environment (Cormen 2009; Epp 2010; Rosen and Krithivasan 1999). There are three conditional statements to shown to be valid or invalid through careful and exhaustive research and analysis. Conditional statement one, (p1) implies (q1) if the use of non-air gap interconnects is digital forensic accessible, then the NextGen Notional Aircraft Architecture is digital forensic accessible. Conditional statement two, (p2) implies (q1) if the use of IP-based communication is digital forensic accessible, then the NextGen Notional Aircraft Architecture is digital forensic accessible. Conditional statement three, (p3) implies (q1) if the use of integrated modular avionics is digital forensic accessible, then the NextGen Notional Aircraft Architecture is digital forensic accessible.

Results

The results of this analysis are consolidated within a visual representation in Table 1. The columns of Table 1 are pre-NextGen and NextGen notional aircraft architecture principle by their section number. The rows of the table are Eden's five challenges facing SCADA forensic investigators by their section number. The last row is the summation of the Eden's five challenges facing SCADA forensic investigators. Each challenge receives a score of one or zero for a maximum of 5 for the summation. One is equivalent to true; the challenge is addressed by the method implored for the principle. Zero is equivalent to false; the challenge is not addressed by the method implored for the principle.

	Air-gap	**Non-air-gap**
LF	0	1
RR	0	1
I&V	1	0
IRL	0	1
FT	0	1
Summation	**1**	**4**

Table 1. Air-gap versus non-air-gap interconnection

Air-gap versus non-air-gap interconnection

Both air-gap and non-air-gap target approaches are subject to internet-based threats (Fleischman 2008). The air-gap offers stronger security properties than the non-air-gap interconnection but requires greater size, weight, and power. The risk mitigation controls are very similar in the two approaches, as both use the same proposed target network architecture design. Historically, air-gap aircraft isolated their flight guidance and control functionality. Therefore, their avionics systems were protected from remote attacks (United States Government Accountability Office 2015).

Based on Eden's five challenges facing SCADA forensic investigators, live forensics is found to be true. The use of non-air gap interconnection is digital forensic accessible because live forensics is enabled by the interconnection between the aircraft and ATC's systems (Cassidy et al. 2007). Rapid response is found to be true. The use of non-air gap interconnection is digital forensic accessible because rapid response can be achieved while the aircraft is still in flight by the interconnection between the aircraft and ATC's systems (Cassidy et al. 2007). Integrity and validity is found to be false. The use of non-air gap interconnection is not digital forensic accessible because historically, air-gap aircraft isolated their flight guidance and control functionality (United States Government Accountability Office 2015). The contradiction of a non-air gap interconnection not being digital forensic accessible implies the use of an air gap interconnection being digital forensic accessible because aircraft manufacturers isolated their flight guidance and control functionality. Therefore, their avionics systems are protected from remote attacks. The incident relevant logs are found to be true. The use of a non-air gap interconnection is digital forensic accessible because of the lack of data storage. One of the major considerations of incident relevant logs can be addressed through a consolidated Storage Area Network (SAN) (Afzaal et al. 2012). The lack of SCADA forensics tools is found to be true. The use of a non-air gap interconnection is digital forensic accessible because SCADA forensics tools are more likely to be developed. SCADA forensics tools are more likely to be developed because of the common interconnection required by multiple systems communicating on the same interconnection (Wu et al. 2013). The five challenges addressed above, as they apply to air-gap versus non-air-gap interconnections, are visual depicted in Table 1. The hypothesis one (p1), the use of non-air gap interconnection is digital forensic accessible is found to be true by 4 out of 5 challenges.

Non-IP-based versus IP-based communication

IP-based communication shares a common IP-based network system (Fleischman 2008). The passenger services, aircraft control, and airline information services share a common network system. Specific aircraft control and airline information services processes distributed network relationships with National Airspace System (NAS) found computers and, potentially, other aircraft. IP-based communication are increasingly used in aircraft system; therefore, it creates the possibility of unauthorized individuals accessing or compromising aircraft avionics systems (United States Government Accountability Office 2015).

Based on Eden's five challenges facing SCADA forensic investigators, live forensics is found to be true. The use of IP-based communications is digital forensic accessible because live forensic is enabled by the distributed network relationships within the distributed network (Cassidy et al. 2007). Rapid response is found to be true. The use of IP-based communications is digital forensic accessible because rapid response is enabled by the distributed network relationships within the distributed network (Cassidy et al. 2007). Integrity and validity are found to be false.

	Non-IP-based	IP-based
LF	0	1
RR	0	1
I&V	1	0
IRL	0	1
FT	0	1
Summation	**1**	**4**

Table 2. Non-IP-based versus IP-based Communications

The use of IP-based communications is not digital forensic accessible because integrity and validity can be compromised without the aid of encryption. The contradiction of IP-based communications not being digital forensics accessible implies the use of non-IP-based communication being digital forensic accessible because integrity and validity were isolated to their proprietary protocols. Incident relevant logs are found to be true. The use of IP-based communications is digital forensic accessible because incident relevant logs contain many of the same attributes of non-SCADA IP-based communications (Afzaal et al. 2012). The lack of SCADA forensic tools are found to be true. The use of IP-based communications are digital forensic accessible because communication off the shelf (COTS) forensic tools feature IP-based network forensics (Wu et al. 2013). The five challenges addressed above as they apply to non-IP-based versus IP-based communications are visual depicted in Table 2. Premise P two (p2), the use of IP-based communications is digital forensic accessible, is found to be true by a 4 out of 5 challenges.

Non-integrated modular avionics versus integrated modular avionics

Integrated modular avionics describes a distributed real-time computer network aboard an aircraft (Fleischman 2008). The network consists of a number of computing modules capable of supporting numerous applications operating at differing safety criticality levels. An example of integrated modular avionics is the real time operating system VxWorks used within the Boeing 787 and many other aircraft. Yannick Formaggio, an IT security researcher, worked as a consultant for Airbus and Thales and holds a master of science in Cryptography (Database 2015; Formaggio 2015a; Formaggio 2015b; River 2015), presented "Attacking VxWorks: from Stone Age to Interstellar" at the 44con conference (Formaggio 2015a). VxWorks is a real time operating system (RTOS) used within the Boeing 787 and many other embedded systems. Yannick did a quick, non-exhaustive internet scan showed at least 100,000 devices running VxWorks building the bases of the Internet-of-Things. The vulnerability for CVE-2015-3963 was demonstrated and thus allowed remote code execution.

	Non-integrated	Integrated
LF	0	1
RR	0	1
I&V	1	0
IRL	1	0
FT	1	0
Summation	**3**	**2**

Table 3. Non-integrated versus Integrated Modular Avionics.

Based on Eden's five challenges facing SCADA forensic investigators, live forensics are found to be true. The use of integrated modular avionics is digital forensic accessible because, by executing a watch dog application with minimal performance impact, live forensics can be performed at all times. Think of it as the new digital black box. Rapid response is found to be true. The use of integrated modular avionics is digital forensic accessible because, by executing a watch dog application with minimal performance impact, live forensics can be performed at all times. The black box with real time data can be retrieved anytime in, simply, the time it takes to be downloaded. Integrity and validity are found to be false. The use of integrated modular avionics is not digital forensic accessible because, without process signing, integrity cannot be ensured. The contradiction of integrated modular avionics not being digital forensic accessible implies the use of non-integrated modular avionics being digital forensic accessible, because there is only one application executing.

Thus, within normal operations, integrity can be ensured through a mathematical proof by contradiction. If no other application is executing, then it must be the only application executing. Incident relevant logs are found to be false. The use of integrated modular avionics is not digital forensic accessible because, by adding more applications per embedded systems, more application incident relevant logs will be created. More application incident relevant logs will require more data storage capacity. The contradiction of integrated modular avionics not being digital forensic accessible implies the use of non-integrated modular avionics being digital forensic accessible because one application per embedded system will create less application incident relevant logs. The generation of smaller amounts of log data will require less data storage capacity. The lack of SCADA forensic tools is found to be false. The use of integrated modular avionics is not digital forensic accessible even with the success of network-based forensics using forensic tools such as EnCase (Wu et al. 2013). There is no evidence that integrated modular avionics will aid in the process of computer-based forensics of SCADA. Quite the opposite, by adding more applications, the isolation of processes will become more convoluted. The contradiction of integrated modular avionics is not digital forensic accessible implies the use of non-integrated modular avionics is digital forensic accessible. The complexity on one operating system (OS) such as VxWorks with one application is a simpler problem set to solve in the short term before added multiple applications create cross contamination. The five challenges addressed above as they apply to non-integrated versus integrated modular avionics are visual depicted in Table 3. The premise p3: The use of integrated modular avionics was digital forensic accessible is found to be false by 3 out of 5 challenges. The negation of hypothesis three (not p3), the use of integrated modular avionics is not digital forensic accessible implies a fourth hypothesis (p4), the use of non-integrated modular avionics is digital forensic accessible.

Conclusions and Future Work

The NextGen Notional Aircraft Architecture is determined not to be digital forensic accessible. Only two of the three hypotheses are found to be valid arguments through the use of both propositional and predicate logic. The third argument is found to be invalid, but there are alternate possibilities for the invalid conclusion.

Argument one (A1) is valid by means of the rule of inference, Modus Ponens. Conditional statement one (p1) implies (q1), if the use of non-air gap interconnection is digital forensic accessible, then the NextGen Notional Aircraft Architecture is digital forensic accessible. Combine conditional statement one, (p1) implies (q1) with the logic connective "and" with hypothesis one (p1), the use of non-air gap interconnection is digital forensic accessible. Concluding (c1), therefore, the NextGen Notional Aircraft Architecture is digital forensic accessible.

Argument two (A2) is valid by means of the rule of inference, Modus Ponens. Conditional statement one (p2) implies (q1), if the use of IP-based communications is digital forensic accessible, then the NextGen Notional Aircraft Architecture is digital forensic accessible. Combine conditional statement two, (p2) implies (q1) with the logic connective "and" with the hypothesis two (p2), the use of IP-based communications are digital forensic accessible. Concluding (c2), therefore, the NextGen Notional Aircraft Architecture is digital forensic accessible.

Argument three (A3) is invalid. Conditional statement one (p3) implies (q1), if the use of integrated modular avionics is digital forensic accessible, then the NextGen Notional Aircraft Architecture is digital forensic accessible. Combine conditional statement three, (p3) implies (q1) with the logic connective "and" with the negation of hypothesis three (not p3), the use of integrated modular avionics is not digital forensic accessible implies a fourth hypothesis (p4), the use of non-integrated modular avionics is not digital forensic accessible. Concluding (c3), therefore, the NextGen Notional Aircraft Architecture is not digital forensic accessible. The three arguments use an "and" connective to show their relationship with each other, A1 and A2 and not A3. Note argument three is negated disproving the hypothesis of the NextGen Notional Aircraft Architecture is digital forensic accessible.

Future research includes developing a process to performing digital forensics on NextGen aircraft architectures. Future research would include developing techniques to perform digital forensics on NextGen aircraft architectures. Future work should refocus studies on the rest of the NextGen system by conducting forensic accessible study on the ATC, and designing integrating forensic-by-design principles (Rahman et al. 2016 (In press) ; Rahman et al. 2016) in future NextGen aircraft architectures.

References

(CVE), C. V. a. E. 2014. "CVE - CVE-2014-4113,").

Adams, R. 2012. "The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice." Murdoch University.

Administration, F. A. 2007. "14 CFR Part 25, Special Conditions: Boeing model 787-8 airplane; systems and data networks security protection of airplane systems and data networks from unauthorized external access,").

Administration, F. A. 2014. "WAAS (WAAS-SUB) Batch Brief", A.B. Smith, C.D. Jones, and E.F. Roberts,").

Afzaal, M., Sarno, C. D., Coppolino, L., D'Antonio, S., and Romano, L. 2012. "A resilient architecture for forensic storage of events in critical infrastructures," *High-Assurance Systems Engineering (HASE), 2012 IEEE 14th International Symposium on*: IEEE, pp. 48-55.

Ahmed, I., Obermeier, S., Naedele, M., and Richard III, G. G. 2012. "SCADA systems: Challenges for forensic investigators," *Computer*:12), pp. 44-51.

Berman, K., Glisson, W. B., and Glisson, L. M. 2015. "Investigating the Impact of Global Positioning System (GPS) Evidence in Court Cases," in: *Hawaii International Conference on System Sciences (HICSS-48)*. Kauai, Hawaii IEEE

Casey, E. 2009. *Handbook of digital forensics and investigation*. Academic Press.

Casey, E. 2011. *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Cassidy, R. F., Chavez, A., Trent, J., and Urrea, J. 2007. "Remote forensic analysis of process control systems," in *Critical infrastructure protection*. Springer, pp. 223-235.

Committee, F. C. S. 2015. "15S.24 IT Risk Management and Information Systems Security,").

Cormen, T. H. 2009. *Introduction to algorithms*. MIT press.

Database, N. V. 2015. "Vulnerability Summary for CVE-2015-3963,").

Dunbar, B. 2002. "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment," *Sans Institute* (2002), pp. 1-9.

Eden, P., Blyth, A., Burnap, P., Jones, K., and Stoddart, K. 2015. "A Forensic Taxonomy of SCADA Systems and Approach to Incident Response," *3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015)*).

Epp, S. 2010. *Discrete mathematics with applications*. Cengage Learning.

Fabro, M., and Cornelius, E. 2008. "Recommended practice: Creating cyber forensics plans for control systems," *Department of Homeland Security*).

Fleischman, E. 2008. "Handbook for Networked Local Area Networks in Aircraft,").

Formaggio, Y. 2015a. "Attacking vxWorks: from Stone Age to Interstellar,").

Formaggio, Y. 2015b. "Speaker Profile,").

Garfinkel, S. 2002. "Network forensics: Tapping the internet," *O'Reilly Network. Retrieved on January* (25), p. 2014.

Garfinkel, S. L. 2006. "Forensic feature extraction and cross-drive analysis," *digital investigation* (3), pp. 71-81.

Geiger, M. 2005. "Evaluating Commercial Counter-Forensic Tools," *DFRWS*.

Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A., Feldman, A. J., Appelbaum, J., and Felten, E. W. 2009. "Lest we remember: cold-boot attacks on encryption keys," *Communications of the ACM* (52:5), pp. 91-98.

Hjelmvik, E. 2008. "Passive network security analysis with NetworkMiner," *IN) SECURE*:18), pp. 1-100.

Kent, K., Chevalier, S., Grance, T., and Dang, H. 2006. "Guide to integrating forensic techniques into incident response," *NIST Special Publication*), pp. 800-886.

Kruse, W. 2002. "II, and Heiser, JG," *Computer Forensics–Incident Response Essentials, Addison-Wesley*).

Leigland, R., and Krings, A. W. 2004. "A formalization of digital forensics," *International Journal of Digital Evidence* (3:2), pp. 1-32.

McMillan, J., Glisson, W. B., and Bromby, M. 2013. "Investigating the Increase in Mobile Phone Evidence in Criminal Activities," in: *Hawaii International Conference on System Sciences (HICSS-46)*. Wailea, Hawaii: IEEE.

MH370, T. M. I. A. S. I. T. f. 2015. "Malaysia Airlines MH370 Boeing B777-200ER (9M-MRO) 08 March 2014,").

Noblett, M. G., Pollitt, M. M., and Presley, L. A. 2000. "Recovering and examining computer forensic evidence," *Forensic Science Communications* (2:4), pp. 1-13.

Palmer, G. 2001. "A road map for digital forensics research-report from the first Digital Forensics Research Workshop (DFRWS)," *Utica, New York*).

Philipp, A., Cowen, D., and Davis, C. 2009. *Hacking exposed computer forensics*. McGraw-Hill, Inc.

Rahman, N. H. A., Cahyani, N. D. W., and Choo, K.-K. R. 2016 (In press) "Cloud incident handling and forensic-by-design: Cloud storage as a case study," *Concurrency and Computation: Practice and Experience*).

Rahman, N. H. A., Glisson, W. B., Yang, Y., and Choo, K.-K. R. 2016. "Forensic-by-Design Framework for Cyber-Physical Cloud Systems," *IEEE Cloud Computing* (3:1).

Ranum, M. 2008. "Network flight recorder," *Inc. Intrusion Detection: Challenges and Myths*).

Reith, M., Carr, C., and Gunsch, G. 2002. "An examination of digital forensic models," *International Journal of Digital Evidence* (1:3), pp. 1-12.

River, W. 2015. "VxWorks,").

Rosen, K. H., and Krithivasan, K. 1999. *Discrete mathematics and its applications*. McGraw-Hill New York.

Symantec. 2015. "Dyre: Emerging threat on financial fraud landscape,").

Taveras, P. 2013. "SCADA live forensics: real time data acquisition process to detect, prevent or evaluate critical situations," *European Scientific Journal*).

U.S. Department of Transportation. 2013a. "Special Conditions: Boeing Model 777– 200, –300, and –300ER Series Airplanes; Aircraft Electronic System Security Protection From Unauthorized External Access,").

U.S. Department of Transportation. 2013b. "Special Conditions: Boeing Model 777– 200, –300, and –300ER Series Airplanes; Aircraft Electronic System Security Protection From Unauthorized Internal Access,").

U.S. Department of Transportation. 2015. "Airworthiness Certification of Products and Articles,").

United States Government Accountability Office. 2015. "FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen,").

Wu, T., Disso, J. F. P., Jones, K., and Campos, A. 2013. "Towards a SCADA forensics architecture," *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013*: BCS, pp. 12-21.

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., and Sommer, P. M. 2003. "Computer forensics education," *IEEE Security & Privacy*:4), pp. 15-23.