CPSC-5620 SPRING 2012

Security Issues of Ad Hoc Networks

Robert Derveloy

4/17/2012

In today's modern world, computers are everywhere. Often, these computers are required to communicate with other devices though purpose built ad hoc networks. With the various routing protocols, resource limitations, and different communications mediums utilized by these networks, security is typically not at the forefront of their design. By examining the potential security issues faced by these networks and reviewing demonstrated attacks, this paper attempts to demonstrate that the use of unprotected ad hoc networks is a haphazard and potentially dangerous practice.

Contents

1. Introduction

In today's modern world, computers are everywhere. They are in automobiles, aircraft, and implantable medical devices to name a few. Often, these computers are required to communicate with other devices though ad hoc networks. As the very nature of such networks is to be developed or customized for a specific purpose, there are a multitude of variants using various routing protocols, resource limitations, and different communications mediums. Consequently, security is typically not at the forefront of these network designs. This paper examines the potential security issues faced by these networks and reviews scenarios in which researchers have effectively attacked systems to either impose control or shut down the network completely.

2. Background

2.1 Nature of Ad Hoc Networks

In order to understand the potential threats to an ad hoc network, it is important to consider the nature of such networks. The term *ad hoc* is Latin and it literally means "for this" as in "for this specific purpose." [1] As the name suggests, ad hoc networks are typically designed for a specific purposes and to work autonomously without having to rely on existing infrastructure. Key characterizations of ad hoc networks are that they can be improvisational, purpose-built, decentralized, and independent. Furthermore, they are typically highly customized for the role for which they are designed to fill. [2] [3]

Unsurprisingly, ad hoc networks do not necessarily adhere to a fixed criterion. However, while individual implementations can vary greatly, they can have common features. Such features may include a lack of central control, limited resources, mobility, dynamic topologies, wireless connectivity, and/or custom routing protocols. These features have distinguishable security implications. For example, if an ad hoc network lacks centralized control it will most likely lack a centralized access control mechanism for the network. Wireless networks can be subject to interference and jamming. Additionally, networks with limited resources may not be able to implement typical routing protocols and, therefore, must run a customized protocol. Custom protocols may or may not have sufficient security measures in place depending on the implementation. [2] [3]

2.2 Governing Bodies

Unlike the public internet, ad hoc networks typically lack governing bodies or organizations to promote security. For example, the Internet Corporation for Assigned Names and Numbers (ICANN) and the World Wide Web Consortium (W3C) are generally tasked with ensuring the smooth running of the internet, at least within their respective spheres of influence. ICANN's security team focuses on the, "security, stability and resiliency" of the internet. [4] The W3C's mission is to, "to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web." [5] It follows that the only tangible influences these organizations would have on ad hoc networks would be if an individual network were to utilize networking protocols that were influenced by either ICANN or the W3C.

2.3 Examples of Ad Hoc Networks

Although the term ad hoc network may imply a connotation of wireless connectivity, an ad hoc network can be wired or wireless, so long as it is designed to fulfill a specific, and most likely limited,

purpose. For example, Nintendo's Game Boy Advance products could connect via a dedicated link cable for multiplayer gameplay. [6] Additional examples include avionics communications networks and some of the automotive bus networks such as the Controller Area Network (CAN) or the Local Interconnect Network (LIN). [7] [8] The CAN bus was developed by Robert Bosh in 1986 to be a robust network in, "electromagnetically noisy environments" and, in addition to automobiles, "CAN buses can also be found in other embedded control applications such as factory automation, building automation, and aerospace systems." [8] The LIN bus system, released in 1999, is a smaller and slower alternative to CAN that is often used to, "integrate intelligent sensors and actuators." [8] Even though wired ad hoc networks are common, wireless ad hoc networks are also becoming more ubiquitous as well. Common examples are Bluetooth networks, peer-to-peer mode WiFi, and the tire pressure monitoring systems (TPMS) that have been installed in modern cars. [9] [10] [11]

3. Threat Models

3.1 Routing Threats

There are a multitude of potential threats facing the routing of ad hoc networks. These include confidentiality, integrity, and availability. When it comes to confidentiality within the realm of routing protocols, the primary threat is towards the, "privacy of the routing data itself." [3] If the routing data were to be compromised, then a secondary threat could occur to other information such as, "the network topology, geographical location, etc." [3] The integrity of an ad hoc network essentially relies on the accuracy of each node's routing information. Potential attacks include those that would either alter existing routing data or introduce new, but incorrect, routing data. Finally, in the context of ad hoc routing, availability fundamentally equates to nodes being able to have on demand access to routing information at all times. Additionally, routing operations should not delay nodes from obtaining up to date information. Consequently, each node within the network should be able to function normally without unnecessary interference from either security or the routing protocol. [3]

Additional threat vectors include authorization, dependability and reliability, and accountability. In its simplest form, authorization refers to whether or not a node is authorized to be on the network. As such, an unauthorized node would be a node that, "is not allowed to have access to routing information, and is not authorized to participate in the ad hoc routing protocol." [3] Given the nature of ad hoc networks, there may or may not be a formal authorization protocol. Nevertheless, it is still a critical security requirement for access control services. [3] Another common use for ad hoc networks, are wireless communications networks that are used during responses to emergencies. [3] [12] Reliable routing with emergency contingency measures should be implemented in order to ensure dependable and reliable operation. "For example, if a routing table becomes full due to memory constraints, a reactive protocol should still be able to find an emergency route to a given destination." [3]

Finally, accountability of network nodes should also be enforced. If an attack cannot be prevented, then it should be detected. By logging actions that may affect the security of the network, appropriate reactionary measures can be taken. [3] "Event logging will also help provide non-repudiation, preventing a node from repudiating involvement in a security violation." [3]

3.2 External Threats

With ad hoc networks, external threats are distinguished from internal threats by classifying external threats as potential attacks performed by unauthorized network nodes or other outside entities. In contrast, internal threats refer to potential attacks originating from internal authorized nodes. In terms of detection difficulty, external threats are typically easier to detect than internal threats. In ad hoc networks with an authentication protocol to block unauthorized nodes from joining the network, external threats typically focus on attacking the data link and physical layers of the network. Also, external attacks can be further classified into two broad categories, passive eavesdropping and active interference. [3]

Passive eavesdropping generally refers to attacks that attempt to simply listen to the transmitted signals and network traffic without disrupting the network. The most basic of which simply involves the discovery of a wireless ad hoc networks by detecting the existence of the appropriate signals. By extension, passive eavesdropping can pose a threat to location privacy. More sophisticated attacks will attempt to capture messages, including routing updates. Routing updates can be used to infer the topology of the network and the identities of the more active, and possibly more critical, network nodes. [3] As demonstrated by devices like those in [13], it is possible to implement passive eavesdropping on wired networks. However, such attacks are typically easier when targeted towards short-range wireless networks that are within close proximity. [3] [11] [14]

In contrast to passive eavesdropping, active interference typically involves launching attacks with the aim of service denial. Normally, the denial of service attacks focus on disrupting or distorting communications. Consequently, their effectiveness is governed by the duration of the attack and the routing protocol used by the network. For example, reactive routing protocols may identify denial of service attacks as line breaks, and trigger an attempt to find an alternative route. On the other hand, proactive routing protocols do not immediately react the non-delivery of packets and instead wait for a connection to time out. Consequently, a denial of service attack may be more effective against networks that employ proactive routing protocols. [3]

The most serious type of external denial of service attacks towards ad hoc networks is referred as the, “sleep deprivation torture attack.” [3] These attacks focus on wasting node energy so that it is deliberately wasted. Networks with limited power and resources are typically the most vulnerable. Fortunately, techniques such as spread spectrum technology have been developed to mitigate these types of threats. However, such protections are not effective at the physical layer. Even though limited power is a physical layer constraint, power levels ultimately affect all operations on an ad hoc network. As a consequence, this makes these types of attacks extremely difficult to guard against. However, in addition to power level attacks, there are also threats that target the networks integrity by attempting to change the order of messages or simply replaying old messages across the network in order to expose the network to out of date information. As a consequence, these attacks can effectively delete currently valid routes or trick nodes into using old routes that are no longer valid; effectively disrupting the network. [3]

3.3 Internal Threats

As mentioned previously, internal threats refer to potential attacks originating from authorized nodes on the network. These types of attacks are potentially very serious since, “internal nodes will have the necessary information to participate in distributed operations.” [3] Typically, the adverse behavior of internal nodes can be classified into four general categories: failed nodes, badly failed nodes, selfish nodes, and malicious nodes. The failed nodes category simply refers to nodes that cannot perform an operation. The badly failed nodes category refers to nodes that behave like failed nodes, but also send out

incorrect routing information. The selfish node category refers to nodes that attempt to exploit the routing protocol to their own advantage by not cooperating when a personal cost is involved. Finally, the malicious node category refers to nodes that deliberately attempt to disrupt the network. Furthermore, a node may demonstrate behaviors from multiple categories and multiple nodes within the same category may have differing degrees of incorrect behavior. [3]

The potential consequences of adverse node behavior vary from category to category. A failed node that cannot send or forward data packets can affect the security of the network if those packets contain authentication or routing data. Dropped error messages may result in network bottlenecks since the originating node may not be aware that a route is broken and may continue to attempt to use it. The consequence of this behavior can have a more serious impact if the failed node or nodes belong to a secure or emergency route. In comparison to failed nodes, badly failed nodes pose an additional threat to the integrity of the network. By sending out incorrect routing information, badly failed nodes can unnecessarily increase network bandwidth consumption, cause working links to be marked as broken, and cause neighbor sensing protocols to detect nonexistent neighbors. Furthermore, selfish nodes can also act like failed nodes depending on the operations that they refuse to perform. The main problem associated with selfish nodes is packet dropping. Since many routing protocols are unable to detect when packets are not forwarded, dropped and partially dropped packets can be difficult to detect. [3]

As mentioned previously, malicious nodes are nodes that intentionally attempt to disrupt the network. Moreover, the effectiveness of a malicious node is amplified if it is in the position to control the flow of information between other groups of nodes. Malicious nodes can also display any of the other categories of abnormal behavior and, as a result, there are many different potential attacks they can perform. The most common of these attacks is the denial of service attack. The most common technique for denial of service attacks is the sleep deprivation torture attack in which malicious nodes force other nodes to consume their resources by performing unnecessary work. Additionally, denial of service attacks also pose a threat to the integrity of the network by deliberately introducing incorrect routing information. Furthermore, as the density of the node population increases, so does the number of nodes affected. [3]

Malicious nodes also pose a threat to networks that utilize neighbor sensing protocols. In this scenario, malicious nodes can force nodes to add nonexistent neighbors or cause other nodes to ignore their neighbors in order to effect a denial of service attack. In addition, malicious nodes can pose as other nodes on the network by using false addresses and disrupt the network's integrity by having other nodes redirect traffic to the malicious node. This technique can be used to perform a black hole attack to capture data or to perform a targeted sleep deprivation attack. In addition to misdirecting traffic, malicious nodes can exploit the route maintenance of the network by propagating false route error messages to mark working links as broken. This can be used to cut a node off from the network or used to force the network to use resources attempting to find alternate routes. Finally, malicious nodes may attempt to use defenses against the network or attack protocol specific optimizations. [3]

4. Successful Test Attacks

In order to demonstrate the serious nature of threats to ad hoc networks, we will examine potential attacks against three different applications that are common to modern life: automobiles, implantable medical devices, and emergency responder communication networks. In each of these cases, the attempted attacks were effectively performed either by malicious nodes on the network or external threats outside of the network. [3] [11] [12] [15] [16] [17]

4.1 Implantable Medical Devices

In [15], the authors worked to examine the security implications of pacemakers and implantable cardioverter defibrillators (ICDs). In their tests, the team was able to reverse engineer the communications protocol used by ICDs and perform passive and active attacks on a test device. To simulate the device being implanted in a human, they placed it in a bag filled with ground beef and bacon. [15]

Implantable medical devices (IMDs) are typically designed with a focus on the medical issue or issues that they are intended to treat. Modern ICDs, "are designed to last several years, use non-rechargeable internal batteries, and have no physical connections outside the body." [15] The ICD that the researchers used to test was equipped with a magnetic switch, which closes in the presence of a magnetic field, that triggers the ICD to wirelessly transmit telemetry data. Furthermore, the ICD model they tested uses a 175 kHz band for communications. Newer devices use the 175 kHz band in addition to a new 402-405 MHz band reserved for medical implants called the Medical Implant Communications (MICS) band. [15]

For their passive attacks, the researchers preprogrammed an ICD with artificial patient data and developed a, "commodity software radio," using the Universal Software Radio Peripheral (USRP) with GNU Radio software libraries. [15] Using their radio, the researchers found clear text representations of patient data within their captured transmissions and were able to conclude that the device did not protect its transmissions with encryption. As a result, they were able to capture, " the patient's name, date of birth, medical ID number, and patient history, […] the name and phone number of the treating physician, the dates of ICD and lead implantation […], the model, and serial number of the ICD and leads." [15] Furthermore, the researchers pointed out that they were able to find other personably identifiable data as well. In addition to personal information, the researchers also found that, once a magnetic field of sufficient strength was introduced to close the ICDs magnetic switch, the telemetry data, which contained electrocardiogram readings, was also transmitted in plaintext. [15]

In addition to the passive attacks, Daniel Halperin et al used their USRP, a BasicTX daughterboard, and a basic amplifier to launch active attacks on the ICD. Using this setup they also found that the magnetic switch could be closed with a RF command, negating the need of a magnet. As a result of their active attacks, they were able to successfully trigger ICD identification, disclose patient data, disclose cardiac data, change the patient's name, set the ICD's internal clock, change or disable therapies (ICD responses to cardiac events), induce fibrillation, and found the potential for a power denial of service attack. This last attack, the power denial of service attack, would invoke a sleep deprivation torture attack that would force the ICD to continuously engage in wireless communication and drain the batteries. [3] [15]

4.2 Automobiles

Another area in which ad hoc networks have become ubiquitous is within modern automobiles. [8] [11] [16] Researchers from the University of Washington and the University of California San Diego have conducted security analysis of networks contained within modern automobiles and have found several different vulnerability classes. These include direct physical vulnerabilities, indirect physical vulnerabilities, short-range wireless vulnerabilities, and long-range wireless vulnerabilities. [11] In [16], the researchers attempted to launch malicious attacks in the test vehicle's Controller Area Network (CAN) bus by connecting to the vehicles on-board diagnostics (ODB-II) port. Using a tool called CarShark to sniff packets on the CAN bus, the researchers were able to figure out how to control many of the systems on the car. They were successful in selectively locking and unlocking brakes, increase the idle RPMs of the engine,

lock and unlock doors, toggle internal and external lights off and on, falsify the speedometer reading, increase radio volume, change the radio display, kill the engine, and more. Furthermore, all but two of their attacks, honking the car alarm and remotely starting the car, were able to be performed at speed and most of the attacks that were tested did not have a manual override. [16]

In [11], the researchers expanded upon their original findings by finding additional entry points into the car network. In addition to attacking through the OBD-II port, which they classified as a direct physical attack, they also conducted indirect physical attacks via the car's CD player and pass through devices. For the CD player attacks, the researchers found they could trigger a firmware update using an ISO 9660 formatted CD with a particularly named file. They also found that they could play a WMA file, which would sound completely normal to someone in the car, but it would secretly send CAN packets of the attacker's choosing. In addition to exploiting the CD player, the researchers found that attacks could be launched via pass-through devices connected to the ODB-II port of the car. Specifically, these devices are designed to support the SAE J2534 PassThru standard. An attacker simply connects a device to the ODB-II port and then use the J2534 API to communicate on the vehicle's internal networks. [11]

In terms of wireless attacks, the researchers tested both short-range wireless attacks through via Bluetooth long-range wireless attacks through cellular networks. When attacking the Bluetooth connection, the researchers attempted both direct and indirect attacks. For the indirect attack, Stephen Checkoway et al a paired an Android smartphone and used a purpose built Trojan Horse application that continuously checks for Bluetooth connections and, when one is connected, sends its attack payload. For the direct attack, the researchers obtain the car's Bluetooth MAC address by sniffing Bluetooth traffic, brute forced the PIN code, and used a buffer overflow attack to inject malicious code. [11]

As in the short range Bluetooth attacks, the researchers also had two approaches for their long range cellular attacks:

> "We demonstrate and evaluate our attack in two concrete forms. First, we implemented an end-to-end attack in which a laptop running our custom aqLink-compatible software modem calls our car repeatedly until it authenticates, changes the timeout from 12 seconds to 60 seconds, and then re-calls our car and exploits the buffer overflow vulnerability we uncovered. The exploit then forces the telematics unit to download and execute additional payload code from the Internet using the IP-addressable 3G data capability. We also found that the entire attack can be implemented in a completely blind fashion - without any capacity to listen to the car's responses. Demonstrating this, we encoded an audio file with the modulated post-authentication exploit payload and loaded that file
> onto an iPod. By manually dialing our car on an office phone and then playing this "song" into the phone's microphone, we are able to achieve the same results and compromise the car." [11]

Furthermore, the researchers were also able to inject CAN packets over the TPMS system, the FM radio receiver via an RDS channel exploit, and were able to expand upon the cellular attack to download an IRC client that will connect to a server and listen for commands sent by an IRC command and control botnet channel. With this last technique, they effectively demonstrated that they could selectively control

cars that were over 1000 miles apart. Ultimately, for each of the vulnerabilities demonstrated, the researchers were, “able to obtain complete control over the vehicle’s systems.” [11]

4.3 Emergency Responder Communications

Project 25, or P25, two-way radio systems are widely used by police, firefighters, and other first responders. [17] Project 25 itself refers to, “a suit of digital protocols and standards designed for use in narrowband short-range (VHF and UHF) land-mobile wireless two-way communications systems.” [12] The standards aim to provide interoperability in order to allow communication, “across departmental and jurisdictional lines using equipment from various manufacturers.” [17] One of the ways P25 radios maintain compatibility with other radio equipment is that they, use a modulation scheme designed to fit into channels compatible with current spectrum management practices for two-way land mobile radio.” [12] As a result of this design constraint, P25 radios are unable to leverage digital spread spectrum techniques to resist jamming. Even worse, the result is that the P25 radios are even more vulnerable to jamming than the legacy equipment they are designed to replace. [12] To test the system’s vulnerability to jamming, the researchers developed a jammer using Texas Instruments CC1110 chips found in a Girl Tech IM-Me, “a toy for preteen text messaging that retails for about $30.” [17] With each IM-Me device, the researchers were able to make two jammers. In addition, they found that they could use standard off the shelf external RF amplifiers to extend the range of the device. “‘We expect that an attacker would face few technical difficulties scaling a jammer within the signal range of a typical metropolitan area.’” [17]

5. Potential Vulnerabilities

Ad hoc networks are becoming more and more common. Although it is impossible to predict how vulnerable future systems will be, we can take a look at an example of new implementations that are just now beginning entering mainstream use. One such example are the internal networks inside of commercial aircraft. Today, airlines such as Virgin America, are offering integrated in-flight entertainment systems. [18] In addition, commercial jetliner manufactures such as Boeing are advertising these systems to potential buyers as ways to create passenger loyalty and, by extension, increase revenue. [19] However, in 2008, the Federal Aviation Administration released a report expressing concerns that Boeing’s 787 passenger jet had potential security and safety issues and claimed that the onboard computer networks could allow passengers to access to the aircraft safety and control systems. [7] In response, Boeing implemented fixes to resolve the potential security threats and promised to thoroughly test the aircraft before delivery to customers. [7] [20] While there has not been a great deal of research into the potential security threats of on-board aviation data networks, it is clear that they are in need of scrutiny as passenger accessible computer networks become more conventional.

6. Conclusion

The nature of ad hoc networks is a double-edged sword from a network security standpoint. Their isolated nature increases the difficulty of remote attacks and limits the potential for multiple network attacks. However, each ad hoc network is potentially vulnerable since it is up to each manufacturer to employ security measures. As the ubiquity of ad hoc networks increases, the need to keep potentially vulnerable networks isolated from emergency or critical systems becomes apparent. Furthermore, stringent security measures with robust reactive routing protocols should be a requirement for any ad hoc network that needs to be employed as a component of systems that are responsible for human life, safety, or wellbeing.

7. Works Cited

[1] D. Harper, "ad hoc," Online Etymology Dictionary, 2012. [Online]. Available: http://www.etymonline.com/index.php?term=ad+hoc&allowed_in_frame=0. [Accessed 15 April 2012].

[2] Merriam-Webster, "ad hoc," Merriam-Webster, 2012. [Online]. Available: http://www.merriam-webster.com/dictionary/ad%20hoc. [Accessed 15 April 2012].

[3] P.-W. Yau and C. J. Mitchell, "Security Vulnerabilities in Ad Hoc Networks," 2003. [Online]. [Accessed 15 April 2012].

[4] Internet Corporation for Assigned Names and Numbers, "Security Team," 2012. [Online]. Available: https://www.icann.org/en/about/staff/security. [Accessed 15 April 2012].

[5] World Wide Web Consortium, "W3C Mission," 2009. [Online]. Available: http://www.w3.org/Consortium/mission. [Accessed 15 April 2012].

[6] Nintendo, "Game Boy Player - Playing Multiplayer Games," 2012. [Online]. Available: http://www.nintendo.com/consumer/systems/nintendogamecube/gameboyplayer_multi.jsp. [Accessed 15 April 2012].

[7] United States Department of Transportation Federal Avaition Administration, "Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security--Isolation or Protection From Unauthorized PassengerDomain Systems Access," 2 January 2008. [Online]. Available: http://cryptome.info/faa010208.htm. [Accessed 15 April 2012].

[8] Clemson University Vehicular Electronics Laboratory, "Automotive Buses," [Online]. Available: http://www.cvel.clemson.edu/auto/auto_buses01.html. [Accessed 15 April 2012].

[9] K. Dunne, E. Roche, D. O'Loghlin and L. Rhatigan, "Bluetooth for Ad-Hoc Networking," [Online]. Available: http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group3/index.html. [Accessed 15 April 2012].

[10] B. Mitchell, "What is Ad-Hoc Mode in Wireless Networking?," About.com, 2012. [Online]. Available: http://compnetworking.about.com/cs/wirelessfaqs/f/adhocwireless.htm. [Accessed 15 April 2012].

[11] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, a. S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," March 2011. [Online]. Available: http://www.autosec.org/pubs/cars-usenixsec2011.pdf. [Accessed 15 April 2012].

[12] S. Clark, P. Metzger, Z. Wasserman, K. Xu and M. A. Blaze, "Security Weaknesses in the APCO Project 25 Two-Way Radio System," 18 November 2010. [Online]. Available: http://repository.upenn.edu/cgi/viewcontent.cgi?article=1990&context=cis_reports. [Accessed 15 April 2012].

[13 Hakshop, "Throwing Star LAN Tap," 2012. [Online]. Available:

] http://hakshop.myshopify.com/products/throwing-star-lan-tap. [Accessed 15 April 2012].

[14 I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe and] I. Seskar, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," 2010. [Online]. Available: http://www.winlab.rutgers.edu/~gruteser/papers/xu_tpms10.pdf. [Accessed 15 April 2012].

[15 D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan,] K. Fu, T. Kohno and W. H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," 2008. [Online]. Available: http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1067&context=cs_faculty_pubs. [Accessed 15 April 2012].

[16 K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy,] B. Kantor, D. Anderson, H. Shacham and S. Savage, "Experimental Security Analysis of a Modern Automobile," May 2010. [Online]. Available: http://www.autosec.org/pubs/cars-oakland2010.pdf. [Accessed 15 April 2012].

[17 W. Jackson, "P25 radios vulnerable to eavesdropping, can be jammed by child's] toy," 1105 Media, 11 August 2011. [Online]. Available: http://gcn.com/Articles/2011/08/11/P25-radios-eavesdropping-jamming.aspx. [Accessed 15 April 2012].

[18 Virgin America, "VIRGIN AMERICA AND LUFTHANSA SYSTEMS TAKE IN-] FLIGHT ENTERTAINMENT TO NEW HEIGHTS: AIRLINE TO LAUNCH NEXT GENERATION RED IN-FLIGHT ENTERTAINMENT PLATFORM IN 2012," 13 September 2011. [Online]. Available: http://www.virginamerica.com/press-release/2011/virgin-america-and-lufthansa-systems-take-in-flight-entertainment-to-new-heights.html. [Accessed 15 April 2012].

[19 Boeing, "Boeing: Commercial Airplanes - Commercial Aviation Services - Fleet] Enhancements - In-Flight Entertainment Systems Integration," 2012. [Online]. Available: http://www.boeing.com/commercial/modifications/inflight_entertainment.html. [Accessed 15 April 2012].

[20 K. Zetter, "FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack," Wired, 4] January 2008. [Online]. Available: http://www.wired.com/politics/security/news/2008/01/dreamliner_security. [Accessed 15 April 2012].

[21 P. Assady, "A New Multiplication Algorithm Using High-Speed Counters," *European] Journal of Scientific Research,* vol. 26, no. 3, pp. 362-368, 2009.

[22 J. D. D. II, "The Datapath," in *Computer Architecture, Fundamentals and Principles] of Computer Design*, Boca Raton, FL, CRC Press, 2006, pp. 111-139.

[23 National Instruments, "SPICE Simulation Fundamentals," 11 April 2012. [Online].] Available: http://zone.ni.com/devzone/cda/tut/p/id/5413. [Accessed 18 April 2012].

[24 N. Hendrich, "Adders and Arithmetic," 2006. [Online]. Available: http://tams-] www.informatik.uni-hamburg.de/applets/hades/webdemos/20-arithmetic/10-

adders/chapter.html. [Accessed 18 April 2012].