SANDIA REPORT

SAND2003-3623
Unlimited Release
Printed October 2003

Views of Wireless Network Systems

David P. Duggan and William F. Young

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2003-3623
Unlimited Release
Printed October 2003

Views of Wireless Network Systems

David P. Duggan and William F. Young
Networked Systems Survivability
And
Assurance Department
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-0785
{dduggan@sandia.gov, wfyoung@sandia.gov}

Abstract

Wireless networking is becoming a common element of industrial, corporate, and home networks. Commercial wireless network systems have become reliable, while the cost of these solutions has become more affordable than equivalent wired network solutions. The security risks of wireless systems are higher than wired and have not been studied in depth. This report starts to bring together information on wireless architectures and their connection to wired networks. We detail information contained on the many different views of a wireless network system. The method of using multiple views of a system to assist in the determination of vulnerabilities comes from the Information Design Assurance Red Team (IDART™) Methodology of system analysis developed at Sandia National Laboratories.

This page intentionally left blank.

Table of Contents

Section 1) Introduction 7
Section 2) IDART$_{TM}$ Methodology 8
Section 3) Example Network Description 9
3.1 Key Features 9
Section 4) Views of the System 11
4.1 Physical View 11
4.2 Data Path/Flow View 11
4.3 Network View 14
4.4 Logical View 15
4.5 Temporal View 16
4.6 Spatial View 17
Section 5) Operations of Interest 19
Section 6) Path Vulnerabilities 20
Section 7) Benefits to Mitigation Design Approach 23
Section 8) Conclusions 24
References 25

List of Tables

Table 1: Features of the Example Wireless Network 11
Table 2: Data Path/Flow View 12
Table 3: Operations of Interest to an Adversary 20
Table 4: Path Vulnerability Table 21

List of Figures

Figure 1. Physical View 10
Figure 2. Network View 15
Figure 3. Logical View 16
Figure 4. Temporal View 17
Figure 5. Spatial View #1 18
Figure 6. Spatial View #2 19

This page intentionally left blank.

Views of Wireless Network Systems

Section 1) Introduction

Wireless networking is becoming a common element of industrial, corporate, and home networks. Commercial wireless network systems have become reliable while the cost of these solutions has become more affordable than equivalent wired network solutions. Unfortunately, the security risks of wireless systems are higher than wired and have not been studied in depth. This report is a start in bringing together information on wireless architectures and their connection to wired networks. We detail information contained on the many different views of a wireless network system. The method of using multiple views of a system to assist in the determination of vulnerabilities comes from the Information Design Assurance Red Team (IDART$_{TM}$) Methodology of system analysis. The goal of the methodology is to identify architectural vulnerabilities of a system to some specific level of adversary. Effective and sustainable security requires a complete system approach rather than the application of individual security patches. The views are used to help determine vulnerabilities that might exist within various architectural pieces of the system.

The main goal of this report is to provide guidance in performing system level security vulnerability analysis in hybrid wired/wireless systems, i.e., communication systems that contain hard wired and wireless communication links, protocols, and/or nodes. We draw a strong distinction between system level vulnerabilities and point level vulnerabilities, such as the ineffectiveness of the Wireless Equivalent Protocol (WEP). Our analysis approach will help identify where security mechanisms such as firewalls, intrusion detection devices, IPSec, IEEE 802.1x, should be integrated into the system in order to mitigate vulnerabilities. Vulnerability analysis of any information systems that utilizes a combination of wireless and wired communication technologies, such as Supervisory Control and Data Acquisition (SCADA) systems, corporate networks, emergency response command centers, can benefit from the approach presented in this document. In addition, the uniqueness and complexities of modern hybrid information systems requires system level analysis to establish a meaningful understanding of the security posture of the system.

The approach presented in this report differs from typical wireless security vulnerability analysis is several important ways. First, most security analyses focus on a single component, protocol, or sub-process, and give limited consideration to the interaction with other components, protocols, or sub-processes. Examples include *Security in Wireless Residential Networks*[1] and *Intercepting Mobile Communications: The Insecurity of 802.11*[2]. Our approach utilizes a system perspective by developing several views of the system (described below). Second, efforts such as *Draft: Wireless Network Security, 802.11, Bluetooth^{TM} and Handheld Devices*[3], *Secure and Mobile Networking*[4] and *Defending Wireless Infrastructure Against the Challenge of DDoS Attacks*[5] provide more of a system perspective, but as in most other cases, the emphasis is on potential solutions, rather than describing the vulnerabilities with context of a system. Third, texts *Wireless Security Models, Threats, and Solutions*[6]and *Wireless Security End to End*[7], provide reasonable levels of detail on wireless specific issues such as unique wireless threats and security solutions for particular threats, but neither outlines how to analyze a hybrid system. While solutions to security vulnerabilities are obviously the ultimate goal, without a thorough system analysis, confidence in the true

effectiveness of a proposed solution is limited. Interaction between components, protocols and sub-systems must be considered to both discover system level vulnerabilities, and to evaluate proposed system level mitigation strategies.

Our presentation utilizes an example hybrid system in order to illustrate as many common wireless components as possible, within the limitations of the technologies. We will concentrate our analysis on the wireless-to-wired network areas. With the methodology used, not every component is shown in every view; only the components that might be active or visible for that view will appear. This report assumes the reader has some basic knowledge about wireless networking and terminologies. The views presented here may contain assumptions about other infrastructure components that may or may not actually be implemented within any given real wireless-to-wired architecture. Those assumptions are identified, as they become relevant for a particular view. The views presented here are those of the physical network, the logical network, one of network functionality, a spatial representation, and a temporal view. There may be many different names for each view, but each view is unique with respect to certain analysis points. The name given to each view is not important and is only meant for reference purposes. There may be more than one visual for each view category, when necessary to show additional detail.

The remainder of the report proceeds as follows. Section 2) provides a brief overview of the IDART$_{TM}$ methodology developed at Sandia National Laboratories. Section 3) describes the example network utilized for the view development and corresponding vulnerability analysis. Section 4) includes several views with explanations of the example system described in section 3. Section 5) discusses some operations of interest derived from the established views. Section 6) identifies some generic security vulnerabilities based on sections 3, 4, and 5. Section 7) outlines how to develop mitigation strategies based on the preceding results. And finally, section 8) draws some conclusions on the overall approach.

Section 2) IDART$_{TM}$ Methodology

The Sandia National Laboratories IDART$_{TM}$ methodology includes several elements and activities supporting a structured process of analysis. This brief discussion covers those aspects of the process pertinent to this analysis. The discussion is not intended to serve as description of the complete IDART$_{TM}$ methodology (there is a multi-day class for this purpose), but as introductory material to assist the reader in understanding the upcoming analysis. As applied in this analysis, the IDART$_{TM}$ methodology exhibits three principal characteristics, listed below.

1. It is a systematic approach, which supports:
    a. consistency of analysis; and
    b. repeatability of results.
2. The distillation of design information related to the system under analysis provides:
    a. the creation of multiple views, which enhances the overall system understanding; and
    b. multiple views that direct analysis along different levels[1] and perspectives; and
    c. supplemental security design material often lacking in original system and design documentation.

[1] Levels, in this context might refer to different layers of the protocol stack.

3. The process utilizes a variety of experts, while:
    a. enabling experts from related fields to provide useful analysis;
    b. integrating the analysis of multiple personnel.

Achieving a complete understanding of highly complex systems is impractical, if not impossible. However, through meaningful assumptions and simplifying representations, the IDART$_{TM}$ methodology captures the principle features of the system. This integrated, system level perspective allows subsystem experts to identify and postulate the effect of subsystem vulnerabilities on the overall system. In addition, the methodology allows for continuing the process through to creation of actual exploits for the identified vulnerabilities. (This particular analysis does not include the creation of actual exploits.) Combining the insight gained from creating various views, the indicated Operations of Interest, and the knowledge of subsystem vulnerabilities enables the identification of system vulnerabilities.

The IDART$_{TM}$ methodology helps create an integrated understanding of the system to support effective vulnerability analysis. This method utilizes multiple views of the system to assist in understanding process, and in the identification of critical interfaces and components. The views presented are based on an example system, described in section 3. Not all views will provide useful insight to some possible vulnerability, but multiple views are included to demonstrate the view creation aspect of the IDART$_{TM}$ methodology. The next several sections provide explanations for the included views.

Note: a view within the context of the IDART$_{TM}$ methodology represents aspects of the system. The views can take the form of illustrations, network diagrams, tables, flowcharts, etc. The goal is to choose a view or series of views that help provide insight to the overall system.

Section 3) Example Network Description

The example network, shown in Figure 1, contains many different wireless and wired network features. Most current networks will not include all the features and devices depicted or implied in Figure 1, but the eclectic illustration assists the completeness of the analysis. Below is a listing of key wireless features found in this network.

3.1 Key Features

The wireless features discussed here are those most representative of features that are currently in use or might well be used in the future. Some features may have variations that are not depicted in this view, or any of the views that are presented in this report. The features are listed within Table 1 below, in no special order, but are numbered only for easier reference. Multiple features might exist on a single device, but shown as separate devices depending on the view.

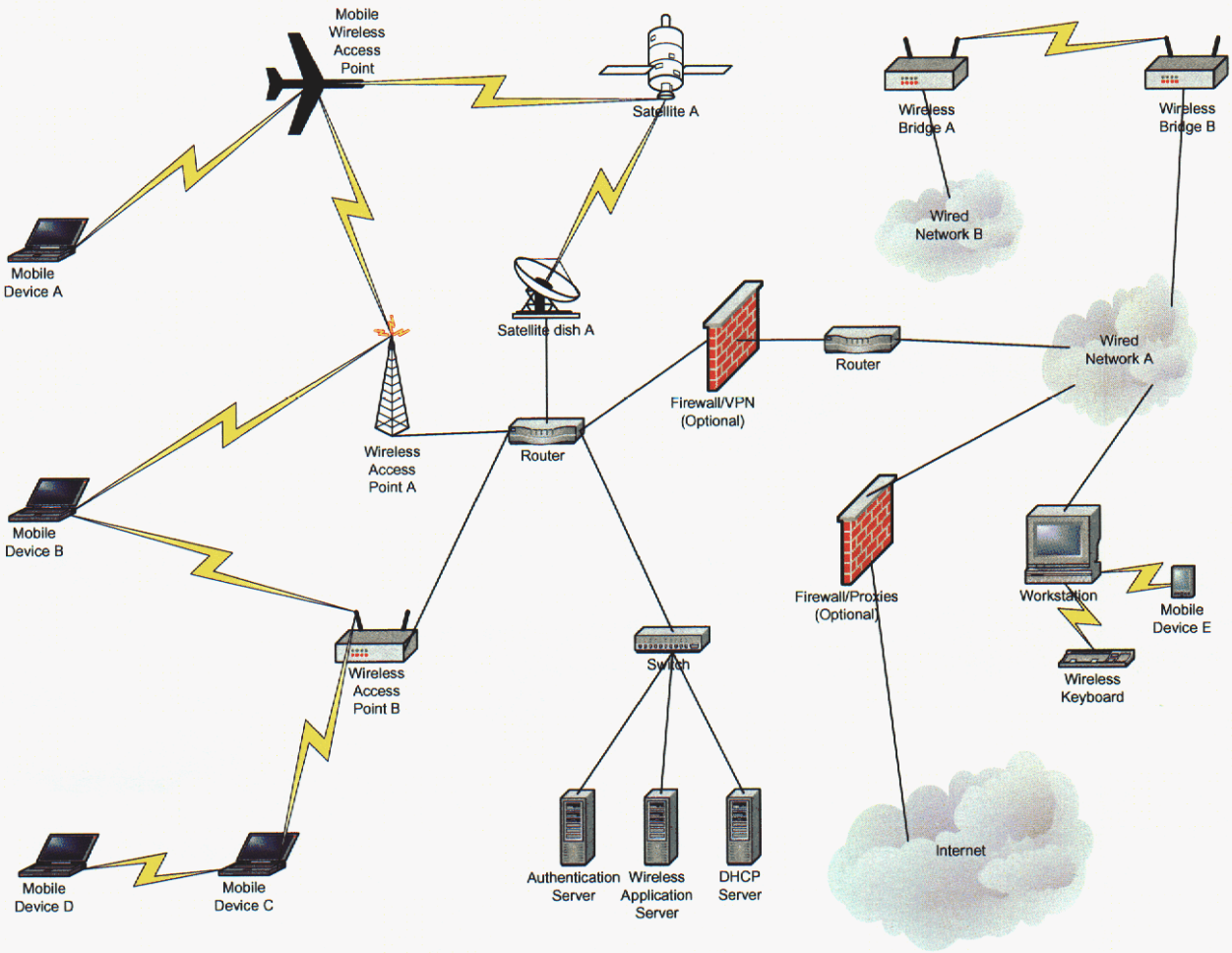

Figure 1. Physical View

Table 1: Features of the Example Wireless Network

Features
1. Multiple wireless access points (WAPs)
2. Wireless clients that may access multiple WAPs
3. Wireless clients that may access other wireless clients directly
4. Wireless application server
5. Authentication server for Extended Authentication Protocol (EAP)
6. DHCP server for issuing IP addresses
7. Connection to wired network through optional firewall and/or VPN device
8. Wired network connected to the Internet
9. Optional firewall and/or proxies between wired network and the Internet
10. Wireless (either through a satellite or point-to-point) link between portions of the wired network
11. Wireless keyboard inside the wired network
12. Mobile WAP

Section 4) Views of the System

4.1 Physical View

The physical view depicts all the physical components of the system, and the connectivity between those components. A link is identified between components as long as there is a physical layer connection (i.e. wired or wireless), regardless of any logical controls placed upon that link. A firewall or other device that contains access-control lists (or some other method of limiting dataflow) to limit or deny access between network segments is still connected to both segments and is capable of allowing data to flow between the segments. Other views, such as the Logical or Functional, are used to capture the operation of that component based upon its functionality and not its physical connectivity.

This view contains many features that may be used in wireless networks along with a description of important data paths and the functions performed on those data paths. Not all features will be used in the average implementation. However, many features are used in combination. Most, if not all, of the components that make up the wireless system will be shown in this view, even if they might be passive in nature. Figure 1 is the graphic of this view.

4.2 Data Path/Flow View

The data paths or flows represent a key view in determining vulnerabilities. An attempt was made to identify all the paths that were available, according to the Physical View shown in Figure 1, that utilize some sort of wireless component and fixed infrastructure. Some paths are only of interest during setup of a network connection while others are most important after the connection is established and application data is flowing over the link. Many of the paths listed utilize the same transmission medium, but interact with different layers of the networking protocols and therefore are listed independently. Although we cannot illustrate

every conceivable path, we provide a substantial number of paths here to help the reader apply this analysis approach to their unique system.

The paths of interest in this paper are listed in Table 2 below, where the paths are separated into categories. Within each category, the possible physical paths are listed, with all intermediate points. Not all paths listed will expose a system vulnerability. However, the identification of all paths is critical to ensuring completeness of the analysis.

Table 2: Data Path/Flow View

#	Category	Data Path
1	Wireless client to/from wireless client	1. Mobile Device D – Mobile Device C
2	Wireless client to/from WAP	1. Mobile Device D – Mobile Device C – WAP B
		2. Mobile Device C – WAP B
		3. Mobile Device B – WAP B
		4. Mobile Device B – WAP A
		5. Mobile Device A – Mobile WAP
3	Wireless client to/from wireless application server (WAS)	1. Mobile Device D – Mobile Device C – WAP B – network device(s) – WAS
		2. Mobile Device C – WAP B – network device(s) – WAS
		3. Mobile Device B – WAP B – network device(s) – WAS
		4. Mobile Device B – WAP A – network device(s) – WAS
		5. Mobile Device A – Mobile WAP – WAP A – network device(s) – WAS
		6. Mobile Device A – Mobile WAP – Satellite A – Satellite dish A – network device(s) – WAS
4	Wireless client to/from DHCP server	1. Mobile Device D – Mobile Device C – WAP B – network device(s) – DHCP
		2. Mobile Device C – WAP B – network device(s) – DHCP
		3. Mobile Device B – WAP B – network device(s) – DHCP
		4. Mobile Device B – WAP A – network device(s) – DHCP
		5. Mobile Device A – Mobile WAP – WAP A – network device(s) – DHCP
		6. Mobile Device A – Mobile WAP – Satellite A – Satellite dish A – network device(s) – DHCP
5	Wireless client to/from extended authentication server (EAP)	1. Mobile Device D – Mobile Device C – WAP B – network device(s) – EAP
		2. Mobile Device C – WAP B – network device(s) – EAP
		3. Mobile Device B – WAP B – network device(s) – EAP
		4. Mobile Device B – WAP A – network device(s) – EAP
		5. Mobile Device A – Mobile WAP – WAP A – network device(s) – EAP
		6. Mobile Device A – Mobile WAP – Satellite A – Satellite dish A – network device(s) – EAP

#	Category	Data Path
6	Wireless client to/from wireless gateway firewall	1. Mobile Device D – Mobile Device C – WAP B – network device(s) – firewall
		2. Mobile Device C – WAP B – network device(s) – firewall
		3. Mobile Device B – WAP B – network device(s) – firewall
		4. Mobile Device B – WAP A – network device(s) – firewall
		5. Mobile Device A – Mobile WAP – WAP A – network device(s) – firewall
		6. Mobile Device A – Mobile WAP – Satellite A – Satellite dish A – network device(s) – firewall
7	Wireless client to/from VPN server	1. Mobile Device D – Mobile Device C – WAP B – network device(s) – VPN server
		2. Mobile Device C – WAP B – network device(s) – VPN server
		3. Mobile Device B – WAP B – network device(s) – VPN server
		4. Mobile Device B – WAP A – network device(s) – VPN server
		5. Mobile Device A – Mobile WAP – WAP A – network device(s) – VPN server
		6. Mobile Device A – Mobile WAP – Satellite A – Satellite dish A – network device(s) – VPN server
8	Wireless client to/from wired network hosts/servers	1. Mobile Device D – Mobile Device C – WAP B – network device(s) – firewall/VPN – wired systems
		2. Mobile Device C – WAP B – network device(s) – firewall/VPN – wired systems
		3. Mobile Device B – WAP B – network device(s) – firewall/VPN – wired systems
		4. Mobile Device B – WAP A – network device(s) – firewall/VPN – wired systems
		5. Mobile Device A – Mobile WAP – WAP A – network device(s) – firewall/VPN – wired systems
		6. Mobile Device A – Mobile WAP – Satellite A – Satellite dish A – network device(s) – firewall/VPN – wired systems
		7. Mobile Device E – Wired Workstation
9	Wireless client to/from Internet, through firewall/proxies	1. Mobile Device D – Mobile Device C – WAP B – network device(s) – firewall/VPN – wired network – firewall/proxies – Internet
		2. Mobile Device C – WAP B – network device(s) – firewall/VPN – wired network – firewall/proxies– Internet
		3. Mobile Device B – WAP B – network device(s) – firewall/VPN – wired network – firewall/proxies– Internet
		4. Mobile Device B – WAP A – network device(s) – firewall/VPN – wired network – firewall/proxies– Internet
		5. Mobile Device A – Mobile WAP – WAP A – network device(s) – firewall/VPN – wired network – firewall/proxies– Internet
		6. Mobile Device A – Mobile WAP – Satellite A – Satellite dish A – network device(s) – firewall/VPN – wired network – firewall/proxies– Internet
10	Wireless client to/from	1. Mobile Device D – Mobile Device C – WAP B – network device(s)

#	Category	Data Path
	wireless concentrating network devices (i.e. WAPs)	2. Mobile Device C – WAP B – network device(s)
		3. Mobile Device B – WAP B – network device(s)
		4. Mobile Device B – WAP A – network device(s)
		5. Mobile Device A – Mobile WAP – WAP A – network device(s)
		6. Mobile Device A – Mobile WAP – Satellite A – Satellite dish A – network device(s)
11	Wireless keyboard client to/from wired workstation	1. Wireless Keyboard – Workstation
12	Wired hosts/servers through wireless bridges	1. Wired workstation – Wireless Bridge A – Wireless Bridge B – Wired workstation
13	Wireless client to/from mobile WAP	1. Mobile Device A – Mobile WAP
14	Mobile WAP to/from stationary WAP	1. Mobile WAP – WAP A
15	Mobile WAP to/from satellite	1. Mobile WAP – Satellite A – Satellite dish A

4.3 Network View

The network view, shown in Figure 2, focuses on network operations, and represents a cross between the logical and physical views. Components are shown with regards to the networking function they provide. For example, the WAPs become hubs in this view since they concentrate data, but the data they concentrate can be accessible to all others near that same location.[2] The wireless links have been replaced with implied wires since the device is communicating with the WAP. The wireless components shown in Figure 1 to connect the wired networks together (Wireless Bridges A & B) disappear in this view and are replaced by a "hub", just as the other WAPs. This hub implies that the data travels "outside" when moving between Wired Network A and Wired Network B.

[2] A hub uses a shared backplane that allows all physically connected devices to see all data that flows through the hub. For wireless networks, all devices that use the same physical layer methods are essentially using a shared backplane.

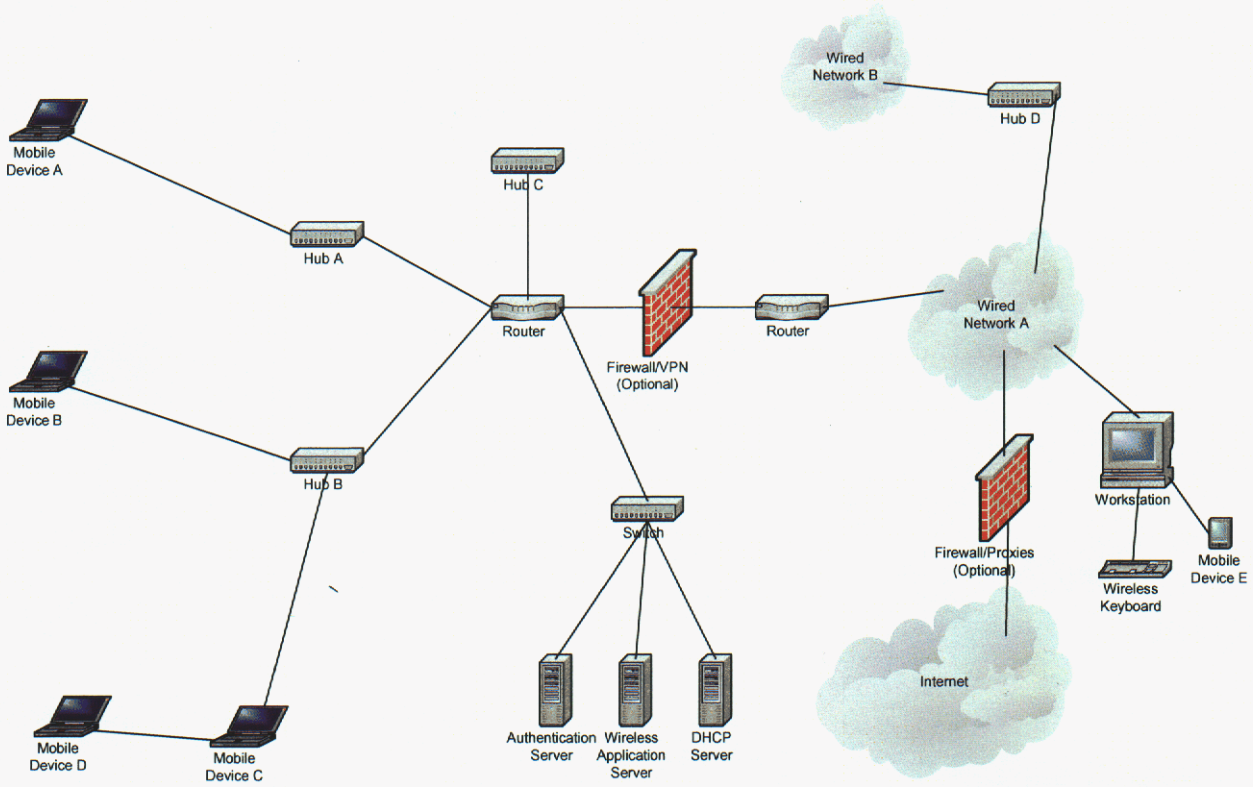

Figure 2. Network View

4.4 Logical View

This view shows the logical network connections as seen by the user, and is sometimes referred to as the application-level view. Implied wires replace the wireless devices and networking equipment. Connections to the application servers are the only interesting features in this view, following data from the client device to the various servers. The wireless components shown in Figure 1 that connect parts of the wired network together (Wireless Bridges A & B) disappear altogether from this view, as does the separation of the two wired networks. See Figure 3 for this view.

The Logical view incorporates the functional features of the devices in the system and arrives at a logical depiction of possible connections. Functions that require coordination between multiple devices are also included. For example, to authenticate a mobile device to a WAP, the intermediate network devices must allow connection to an authentication server. Communication must be supported and allowed between the mobile device and the WAP, as well as between the WAP and the authentication server.

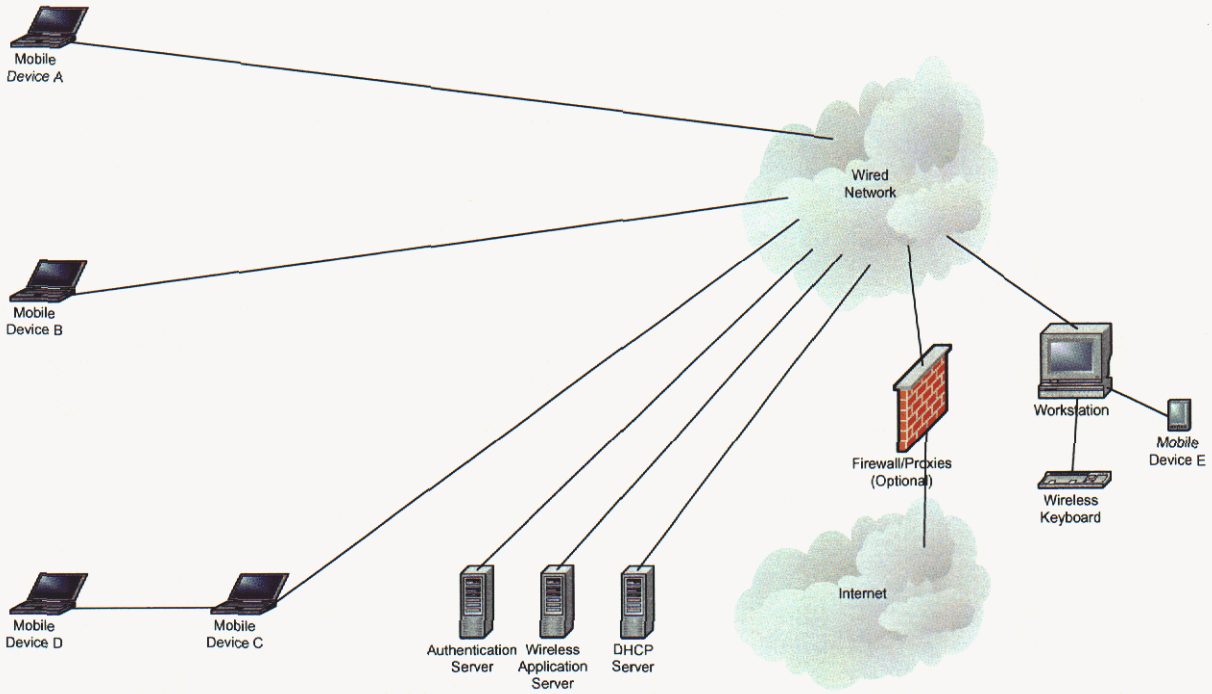

Figure 3. Logical View

4.5 Temporal View

The temporal view captures the aspect of change in the system over time. Many aspects of an information system may change over time, including communication connectivity, traffic volume, types of applications supported, etc. The selection of a time scale determines which temporal aspects are important in the analysis. For example, when a mobile wireless device connects to a wired infrastructure, the wireless link connectivity may change in a matter of seconds, as compared to the wired connectivity that is available from days to months. Thus, if a timescale of minutes is important to the functionality of the system, wireless connectivity is an important element of the system to analyze.

There are multiple time periods shown on the temporal view. The black lines indicate both physical wires and wireless links that are intended to be constant. The dashed black lines are wireless links that are intended to be intermittent in nature such that if they aren't available, no problem is to be indicated. The solid green lines are to show links that are in place at some arbitrary time "X". The solid red lines are the links that are in place at some later time, "X" + "Y". This is to show that a wireless device can move from one "hub" to another at any point in time. This is not usually a feature of most wired networks. Figure 4 shows this view.

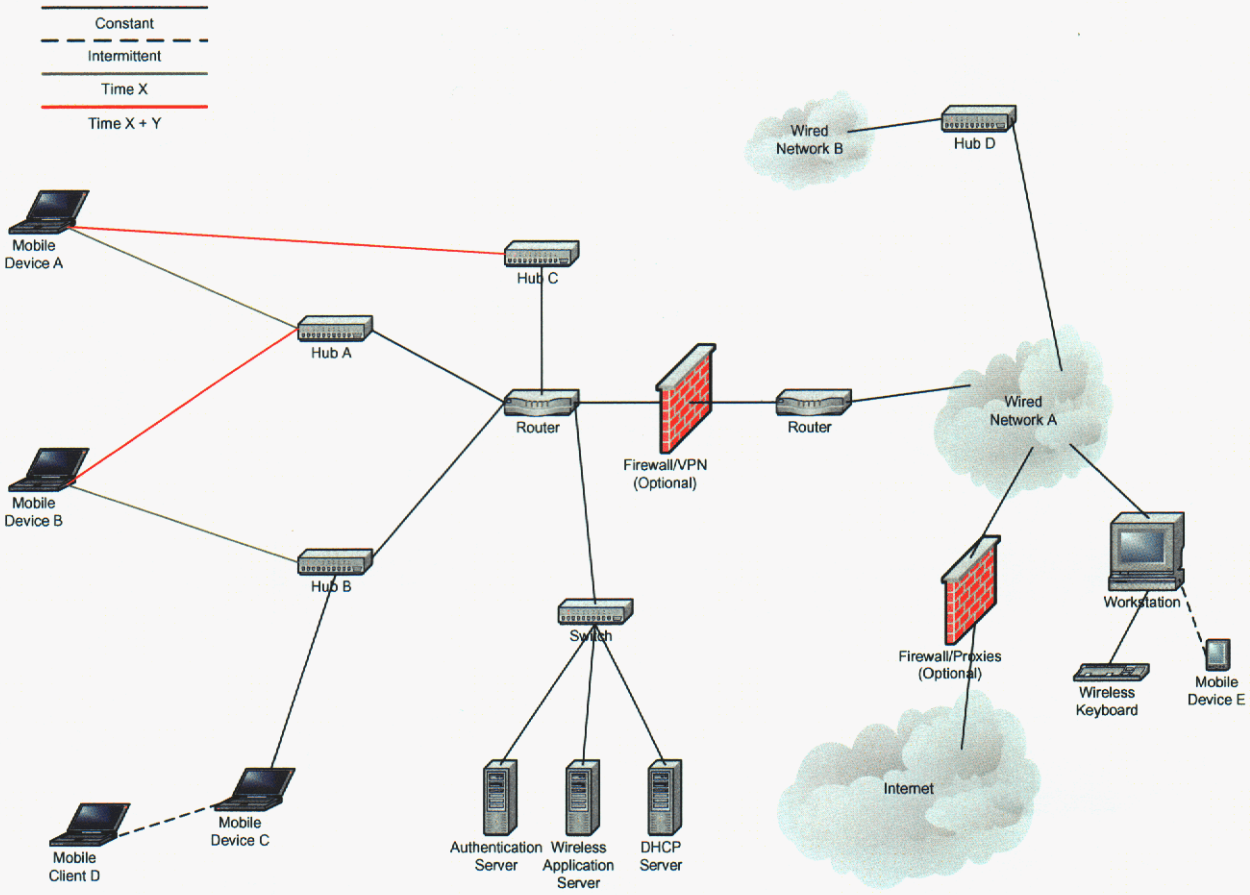

Figure 4. Temporal View

4.6 Spatial View

The spatial view depicts the relative physical location of components of the system. In addition, referencing the spatial view with a fixed infrastructure or location enables establishment of physical boundaries. This view is particularly important to wireless information systems because it illustrates the coverage area for wireless communication systems, where the coverage area is specified by normal or intended operations. Introducing different communication components, such as directional antennas, higher-gain transmitters/receivers, can modify this coverage area.

Multiple spatial views are included below, where each view represents a specific aspect of the overall system, but are shown separately to allow the depiction of additional details that can affect the performance of the wireless link.

The first view, the one with two stationary WAPs, shows three mobile clients at different locations and is shown by Figure 5. Two clients do not have access to both WAPs at the same time, while one is within range of both. However, the proximity of the mobile clients would put mobile client B in a position to "see" communications to and from the other two mobile clients and their respective WAPs.

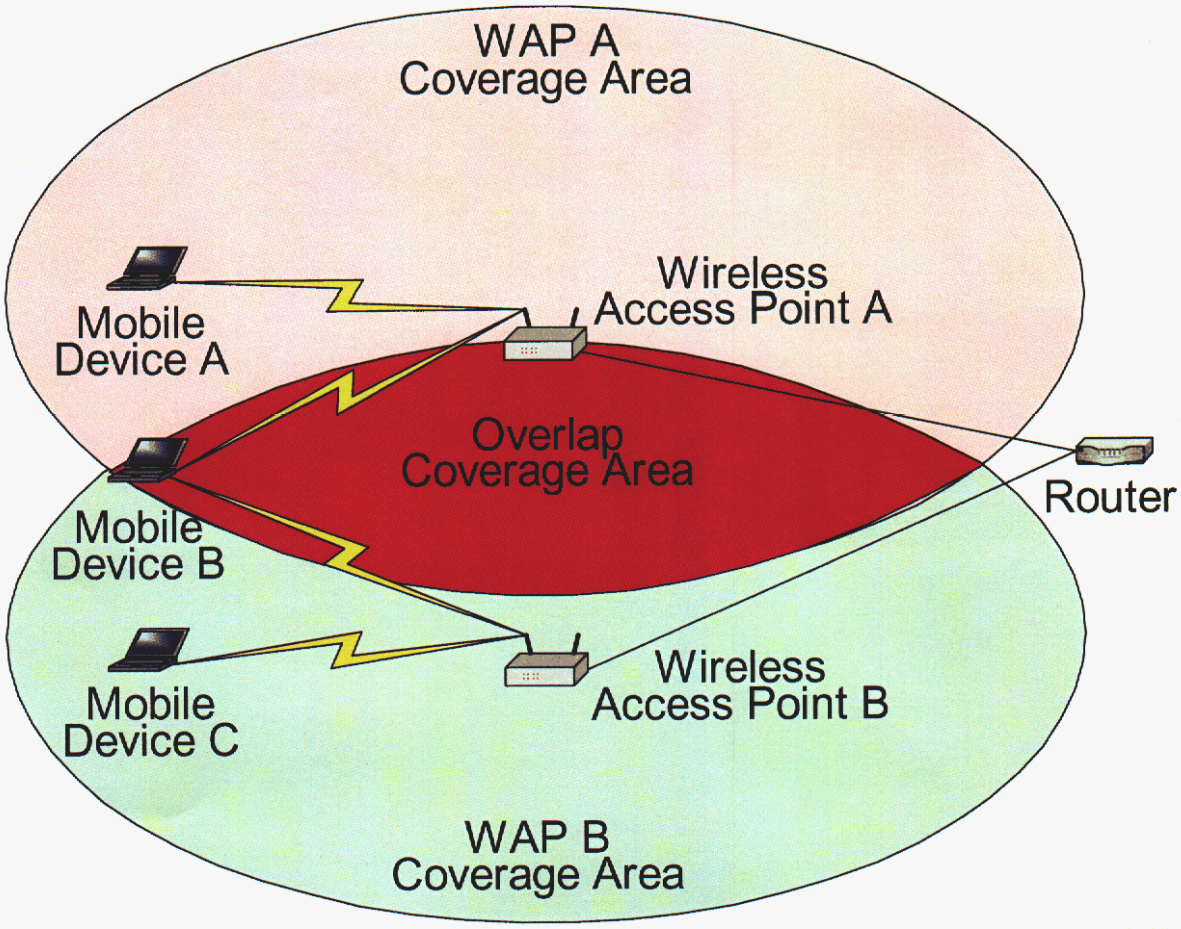

Figure 5. Spatial View #1

The second view, Figure 6 is the one with the mobile WAP and shows it communicating with a stationary WAP while at Location X. The second location, Y, is only in range of another mobile WAP that has multiple wireless hops to get back to the wired network.

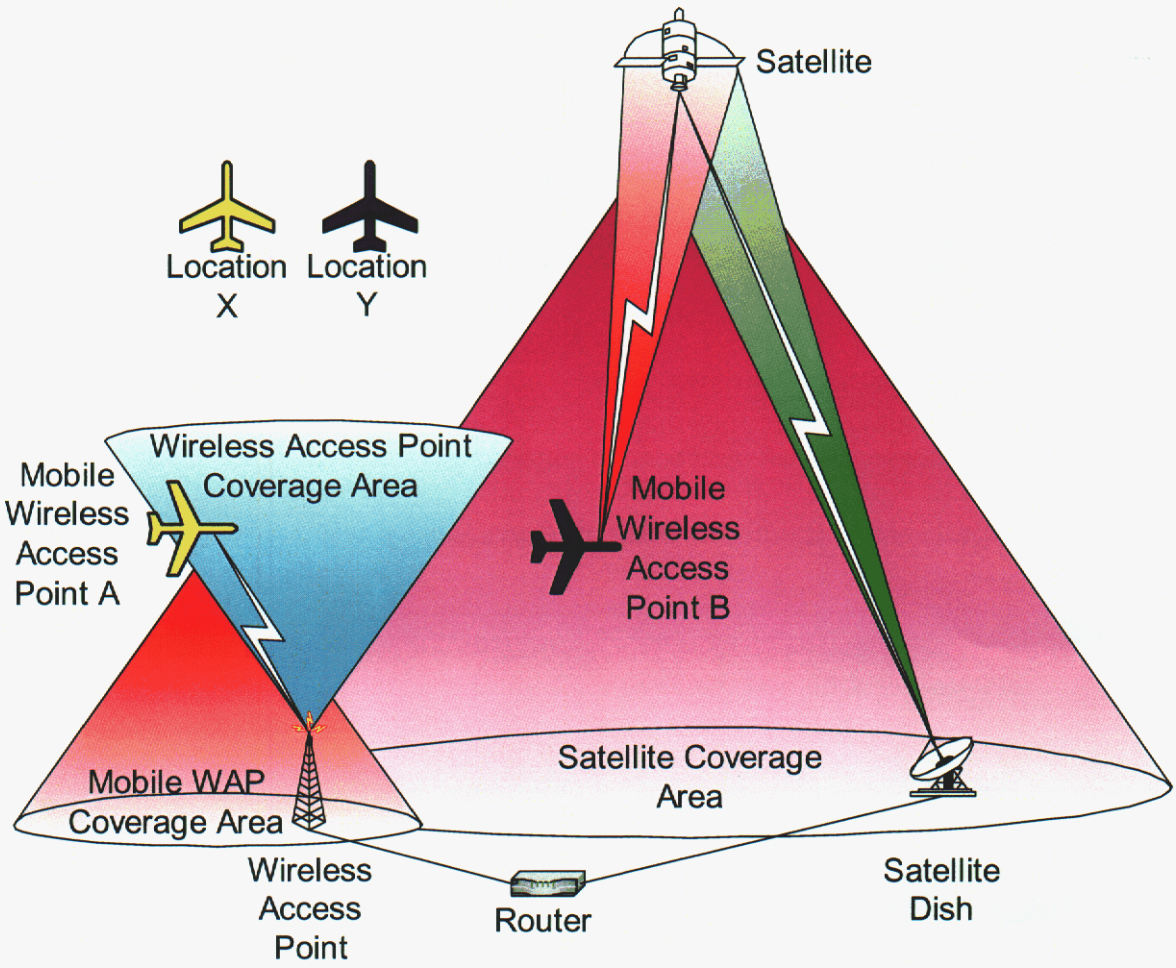

Figure 6. Spatial View #2

There was no spatial view created for the wireless keyboard. That device is a short-range device that must be within some small number of feet from the workstation, depending upon the actual protocol being used between the devices. There was also no spatial view created for the Mobile Device E (PDA-type device) either.

Section 5) Operations of Interest

The views described above help establish a baseline understanding of the system. The analysis now focuses on actions or operations that occur in the system. While there many different types of actions performed over the above paths, there are particular operations that typically interest an adversary. Paths of interest to an adversary normally include paths that provide control functions or some authentication function that might be subverted. Some of the more interesting operations are listed in Table 3 below.

Table 3: Operations of Interest to an Adversary

Operations
1. Initiate/terminate connection to stationary WAP
2. Initiate/terminate connection to mobile WAP
3. Physical movement causing handoff from one WAP to another WAP
4. Connection to workstation from wireless keyboard
5. Authentication to stationary WAP
6. Authentication to mobile WAP
7. Authentication to wireless application server
8. Utilize wireless application servers
9. Utilize wired application servers

Section 6) Path Vulnerabilities

This section will focus on identification of vulnerabilities for the various data paths. We make use of the various views and operations of interest documented in the previous sections to determine these paths and the corresponding vulnerabilities. Data paths identified previously (see Table 2) may be sub-paths of longer paths. Thus, if a path is contained within a longer path, the longer path will also contain the vulnerability identified for the shorter path. The vulnerabilities in this report are defined as affecting the confidentiality, integrity, or availability of a system. If a method for exploiting the vulnerability is known, it will be cited at the point the vulnerability is identified.

All wireless client paths have, to some extent, the following generic vulnerabilities:

- Confidentiality – Data capture when 1) transmission not encrypted, 2) Weak encryption or algorithm is used, e.g. Wired Equivalency Protocol (WEP).
- Integrity – 1) Man-in-the-middle (MITM), attacker not necessarily closer to target, 2) spoofing, attacker not necessarily closer to target, 3) attacker can become a false WAP.
- Availability – Denial-of-Service (DOS) by 1) frequency jamming, 2) flooding WAP with "valid" traffic.
- Physical – Mobile devices are generally less protected and more accessible for physical-type access attacks.

Specific instances of vulnerabilities are listed here.

- Mobile-to-Mobile attacks. These include any attacks that could be perpetrated from machine to machine in a wired network. In the wireless world, these would be difficult to trace since there is not actual wiring to follow back to the attacker.
- Keystroke capture for wireless keyboard is a very stealthy method to use at a distance with a directional antenna. Additionally, sending keystrokes may be accomplished for systems using wireless keyboards, when they are left unattended.
- Man-in-the-Middle attacks can be accomplished with a pair of directional antennas and don't require the attacker to be physically between the client and the WAP.
- Access to the plain-text and the cipher-text for the same packet is available for some paths. This makes breaking the key possible for stream ciphers.

The following table, Table 4, contains a high-level identification of vulnerability categories that are identified with each path. It contains the same paths identified in Table 2, in the left column. The right column contains the vulnerabilities associated with breaching Confidentiality (C), Integrity (I), and Availability (A) on that path. These are vulnerability categories and not specific attacks that have been seen on the Internet. The listed vulnerabilities for a path must be examined with respect to the application that is to use that path to determine whether they are applicable or not.

Table 4: Path Vulnerability Table

#	Path Category	Path Vulnerability
1	Wireless client to/from wireless client	**C**: Leakage of authentication information between these wireless systems. **I**: Adversary could become relay between the systems, modifying any information that it passes. **A**: Depending upon the application being run by the remote system, denial to the services could be critical. The node could become isolated or the network partitioned.
2	Wireless client to/from WAP	**C**: Leakage of authentication or addressing information. **I**: Adversary could place a WAP between the client and authorized WAP to collect or change information between the systems. They could also change important data as it passes. **A**: Without access to the WAP, most wireless clients will not be able to access services they need on the network.
3	Wireless client to/from wireless application server (WAS)	**C**: Information leakage, which is possibly sensitive if it contains usernames and passwords or other information, such as personnel information or design specifications. **I**: The level of this vulnerability depends upon the importance of the information that can be modified. Modification of data that is destined as input to any program is always a bad thing. **A**: The importance of immediate access to the WAS is dependent on the importance of the service being provided.
4	Wireless client to/from DHCP server	**C**: Target identification is enhanced by the leakage of DHCP information. **I**: Modification of DHCP traffic allows adversary to place a rogue DHCP server in place and control all the parameters such as Domain Name Servers and Default Gateway. This is used for Man-In-The-Middle setups. **A**: Without access to the DHCP server, a user workstation might not be able to connect to the network properly and therefore receives no service from the system.
5	Wireless client to/from extended authentication server (EAP)	**C**: Leakage of authentication credentials, passwords, password hashes, or certificates allow impersonation by an adversary. **I**: Modification of authentication stream can allow adversary to blacklist user, modify login parameters, or steal a users identity. **A**: Denying access to the authentication server will keep authorized users from accessing any facilities or services of the system.

#	Path Category	Path Vulnerability
6	Wireless client to/from wireless gateway firewall	**C**: Leakage of sensitive information, such as usernames, passwords, keys, certificates, and other sensitive application information allowing impersonation or data theft. **I**: Modification of application data, passwords, and other information can occur with varying degrees of importance. **A**: Without access to the gateway, the client system will not be able to acquire services from the networked systems.
7	Wireless client to/from VPN server	**C**: Leakage of application data, which could include usernames, passwords, keys, sensitive information, etc. The main function of a VPN is to disallow this. **I**: Modification of possibly sensitive information. **A**: Without network access to the VPN server, processing of sensitive information is forced to be in the clear.
8	Wireless client to/from wired network hosts/servers	**C**: Leakage of information that normally wouldn't be available. The wired servers or hosts might normally be accessed by internally wired systems and the applications aren't protecting the information from disclosure during transmission. **I**: Modification of information during transmission is allowed due to the use of a wireless component. Wired hosts and servers could have the implied assumption that all users are connecting via a wired connection. **A**: Denying this access will keep information from being sent or received with a remote site. If decisions are being based on this information, timely decisions will be affected.
9	Wireless client to/from Internet, through firewall/proxies	**C**: Leakage of encrypted traffic could occur since adversary could have access to the plaintext and encrypted text for the same message. **I**: With broken encryption keys from the above attack, new messages could be created as modifications or real traffic. **A**: See #8 above.
10	Wireless client to/from wireless concentrating network devices	See #6 above.
11	Wireless keyboard client to/from wired workstation	**C**: Leakage of sensitive information, such as usernames and passwords as well as other information that is typed into applications. **I**: Modification of input to applications. Input to the workstation from a distance without knowledge of the user. The running of programs without knowledge of the user. **A**: Without keyboard access to most workstations, it is difficult to perform any real tasks. Console access is generally better connected, with more privileges, than remote access.

#	Path Category	Path Vulnerability
12	Wired hosts/servers to/from satellite	**C**: Leakage of sensitive information, including usernames, passwords, keys, other credentials, and sensitive application data. This information might normally be protected from disclosure by being sent through a protected wire and is now sent wireless. **I**: There is some chance that modification of information as it passes by can be accomplished. It would need to be extremely targeted. Injection of data packets would be possible. A: Denying access to the satellite will keep information from being sent or received with a remote site. If decisions are being based on this information, timely decisions will be affected.
13	Wireless client to/from mobile WAP	See #2 above.
14	Mobile WAP to/from stationary WAP	**C**: Leakage of information, such as address information or authentication information as it is passed between WAPs. **I**: Modification of address or authentication information to allow adversary system to supplant identity of an already authenticated system. A: Denial of this transfer will cause a re-authentication of the original system to occur.
15	Mobile WAP to/from satellite	See #14 above.

An important item to note is that some applications could make implicit assumptions that traffic between the client and server take place on a wire, not a wireless link. This type of assumption might come into play with applications that were written before wireless networking was readily available. Remember too, that modification of any data destined to a program is probably a bad thing.

Section 7) Benefits to Mitigation Design Approach

This section discusses advantages that might be gained by mitigation design with regards to vulnerabilities identified. As in any good design project, the actual design would be created for a specific system, according to the needs of its functional and security requirements. However, there are other factors that will influence the security design of any mitigation for a system.

To develop strategies for mitigation of vulnerabilities, one must first have determined the vulnerabilities. Examination of Table 3 allows the determination of which operations an adversary might examine to identify their opportunities. Even though this list is small in size, it is rich with specific areas to be explored. Table 4 also needs to be examined when determining which vulnerabilities need to be mitigated. Utilizing these lists, a set of priorities is developed with which to guide the design of mitigations.

Advantages of this strategy include:

- An overall understanding of how and where data flows (both control and application)
- Better understanding of communications needs

- Removal of "low-hanging fruit" from adversary reach
- More robust system

For insight into how this type of analysis relates to designing a secure system, the reader is encouraged to look at *Communication Vulnerabilities and Mitigations in Wind Power SCADA Systems* [8]. That document outlines an approach for designing securing wind power SCADA systems. An import task included in the approach is the identification of potential system level communication vulnerabilities, which follow directly from the process discussed in this document.

Section 8) Conclusions

In this paper, we have identified many of the wireless networking structures that are likely to be found in deployed communication networks and information systems. Using the IDART™ assessment technique for assessing systems, which is described within the paper, we then identified vulnerabilities that can exist within these systems. From this analysis, it is clear that there are multiple points where security must be integrated into the wireless system, based upon the functional and security requirements of the system. Specific mitigations for vulnerabilities have not been identified since they will realistically depend upon the level of security needed for a particular application within a system.

Wireless components can be securely integrated into information systems, but do require the integrator to design specific mitigations using a systems perspective. If wireless networking is being added to existing systems, a security assessment must be performed on the system to determine the necessary mitigations and their placement. These mitigations must be designed from the systems perspective and serve a specific purpose within the Confidentiality, Integrity, and Availability goals for that system.

Finally, this report covers one of the two main results from the LDRD effort entitled, "Surety Enhancement for Wireless Automated Control Networks." The other principal result is discussed in the paper, *Communication Vulnerabilities and Mitigations in Wind Power SCADA Systems*, which was presented at WindPower 2003, May 18-21, 2003 in Austin, TX. In that paper, we describe key aspects of how to approach securing a wind power SCADA system. Although we specifically focused on wind power issues, the approach applies to most other SCADA systems. The connection between the two documents is that the analysis of the wireless vulnerabilities of a system should be performed in conjunction with the overall secure system design. For instances, in the *Communication Vulnerabilities and Mitigations in Wind Power SCADA Systems* document, several wireless vulnerabilities which arise from weaknesses in current technology combined with common SCADA communication architectures are listed. While this document focuses on general wireless vulnerability analysis, the *Communication Vulnerabilities and Mitigations in Wind Power SCADA Systems* document provides an example of how to proceed with designing of a secure SCADA system. We encourage the use of both documents in the process of developing a secure system.

References

[1] Krishnamurthy, P., Kabara, J., Anusas-amornkul, T., *Security in Wireless Residential Networks*; IEEE Transactions on Consumer Electronics, Vol. 48, No.1, pp. 157-166, February 2002.

[2] Borisov, N., Goldberg, I., Wagner, D., *Intercepting Mobile Communications: The Insecurity of 802.11*, Seventh Annual International Conference on Mobile Computing And Networking, July 16–21, 2001.

[3] Karygiannis, T., Owens, L., *Draft: Wireless Network Security, 802.11, Bluetooth™ and Handheld Devices*, National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, Gaithersburg, MD, U.S. Department of Commerce; Special Publication 800-48.

[4] Gupta, V., and Montenegro, G., *Secure and Mobile Networking*; Mobile Networks and Applications, Special Issue: *Mobile Networking in the Internet*; Volume 3, Issue 4, 1999, ACM Press, New York, USA.

[5] Geng, X., Huang, Y., and Whinston, A.B.; *Defending Wireless Infrastructure Against the Challenge of DDoS Attacks*, Mobile Networks and Applications, Volume 7, Issue 3, June 2002, ACM Press, New York, USA.

[6] Nichols, R.K. and Lekkas, P.C., *Wireless Security Models, Threats, and Solutions*, McGraw-Hill, © 2002.

[7] Carter, B., and Shumway, R., *Wireless Security End to End*, Wiley Publishing Inc., Indianapolis, Indiana, © 2002.

[8] Young, W., Rumsey, M., Dillinger, J., and Stamp, J., *Communication Vulnerabilities and Mitigations in Wind Power SCADA Systems*, WindPower 2003, May 18-21, 2003.

DISTRIBUTION:

1 MS 0785
R. E. Trellue, 5501

1 MS 0784
M. J. Skroch, 5512

1 MS 0784
R. A. Duggan, 5512

1 MS 0785
R. L. Hutchinson, 5516

10 MS0785
D. P. Duggan, 5516

1 MS 0785
D. Kilman, 5516

1 MS 0785
W. F. Young, 5516

1 MS 0785
B. P. Van Leeuwen, 5516

2 MS 0899
Technical Library, 9616

1 MS 9018
Central Technical Files, 8945-1