



NCS TIB 05-4

NATIONAL COMMUNICATIONS SYSTEM

TECHNICAL INFORMATION BULLETIN 05-4

**Cyber Vulnerabilities within the National
Infrastructure's Supervisory Control and Data
Acquisition Systems:**

**Cyber Vulnerabilities within
Telecommunication Supervisory Control and
Data Acquisition Systems**

May 2005

**OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM
701 SOUTH COURT HOUSE ROAD
ARLINGTON, VA 22204-2198**

This document was prepared under contract to the

Office of the Manager
National Communications System



Contract No. V674P-3498
Delivery Order No. 674-S40011

Prepared by:

Evan T. Grim and Michael W. Raschke
Southwest Research Institute®
P.O. Drawer 28510
San Antonio, TX 78228
Grim: 210-522-2850 (Voice)
Raschke: 210-522-6603 (Voice)
210-522-5499 (Fax)



SwRI Project No. 10.10403

NCS TECHNICAL INFORMATION BULLETIN 05-4

CYBER VULNERABILITIES WITHIN THE NATIONAL INFRASTRUCTURE'S
SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEMS: CYBER
VULNERABILITIES WITHIN TELECOMMUNICATION SUPERVISORY CONTROL AND
DATA ACQUISITION SYSTEMS

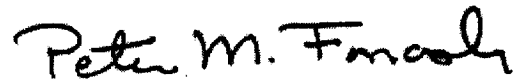
May 2005

PROJECT OFFICER



DALE BARR, JR.
Chief, Advanced Technology
Technology & Programs Division

APPROVED FOR PUBLICATION:



PETER M. FONASH, Ph. D.
Deputy Manager,
National Communications
System

FOREWORD

Among the responsibilities assigned to the National Communications System, is the management of the Federal Telecommunications Standards Program. Under this program, the NCS, with the assistance of the Federal Telecommunications Standards Committee identifies, develops, and coordinates proposed Federal Standards which either contribute to the interoperability of functionally similar Federal telecommunications systems or to the achievement of a compatible and efficient interface between computer and telecommunications systems. In developing and coordinating these standards, a considerable amount of effort is expended in initiating and pursuing joint standards development efforts with appropriate technical committees of the International Organization for Standardization, the International Telecommunication Union-Telecommunications Standardization Sector, and the American National Standards Institute. This Technical Information Bulletin presents an overview of an effort which is contributing to the development of compatible Federal and national standards in the area of national security and emergency preparedness (NS/EP). It has been prepared to inform interested Federal and industry activities. Any comments, inputs or statements of requirements which could assist in the advancement of this work are welcome and should be addressed to:

National Communications System
PO Box 4502
Arlington, VA 22204-4502

EXECUTIVE SUMMARY

In 1876, Alexander Graham Bell invented an amazing device that astonished people far and wide. Since then, countless numbers of people have worked countless numbers of hours to evolve that invention into one of the most influential and efficient communications systems in the world. It has become one of our country's most critical infrastructures. Today modern civilization depends on the reliable operation of this system for many services like nothing else. Now, as time quickly marches through the first decade of the new millennium, terrorists and adversaries have likely spied that system as a prime target to hit and to hit hard. The successful crippling of the telecommunications system could wreck havoc upon the wellbeing, stability, security, and economy of the United States and the western developed countries.

Through the years, the telecommunications system has grown to include a supervisory control and data acquisition capability, which is commonly referred to as the Telecommunications Management Network (TMN) in the telecommunications industry. The TMN is the tool that is used to monitor and supervise all aspects of the underlying telecommunications system. As such, the TMN has become very important to the correct operation of the telecommunications network (TN), and therefore, its correct operation is imperative to the national security of the United States. To control the TMN is to control the complete operation of the United States' communications infrastructure. All systems face threats, but critical systems face constant threats.

Overall, the level of security protecting the national telecommunication infrastructure is leaps and bounds ahead of the security of other critical infrastructure providers, such as natural gas, water, and electricity. However, current security measures always leave room for improvement and must continuously be reviewed and modified. The TN, in particular, has several unique vulnerabilities that warrant special attention. This report explores this network, its vulnerabilities, and its threats. It describes the various security tools, services, practices, and research that are recommended for all telecommunications companies to consider. The prime focus is on security as it relates to potential cyber attacks against our nation's ability to communicate in times of need. The analysis includes:

- The evolution and architecture of the TMN,
- The common and critical cyber threats to the TMN,
- Descriptions of the voice and data portions of the underlying telecommunications network including control systems and assessments of vulnerability,
- Explanations of how the voice and data networks are traversing down a convergent path, exploring the emerging difficulties and security considerations such convergence will bring, and
- Recommendations on how to best move forward to secure this critical infrastructure control system.

Securing the nation's telecommunications control infrastructure is hardly as simple as flipping a switch. It is a complex balancing act involving a host of parameters. Those charged with securing this system have a never-ending task of evaluating cost against risk, threat against vulnerability, and functionality against protection. Such decisions require a wealth of information, and it is the purpose of this report to provide the necessary insight and knowledge for these decisions to be made wisely.

TABLE OF CONTENTS

Executive Summary	i
Table of Contents	ii
List of Figures	iv
List of Tables	v
List of Acronyms	vi
1.0 Introduction	1
2.0 Evolution of the Telecommunications Managed Network	3
2.1 History of the Telecommunications Management Network.....	3
2.2 Overview of the Telecommunications Network.....	4
2.2.1 Circuit-Switched vs. Packet-Switched Networks	5
2.2.2 Transport Plane vs. Control Plane	6
2.3 Telecommunications Management Network Architecture.....	6
2.3.1 TMN Functional Architecture.....	7
2.3.2 TMN Information Architecture.....	8
2.3.3 TMN Physical Architecture	9
3.0 The Phantom Menace	11
3.1 Threats Explored.....	11
3.1.1 Attacker Groups	12
3.1.2 Attacker Type.....	12
3.1.3 Attack Type.....	13
3.1.4 Attack Activities	13
3.1.5 Attack Classification.....	14
3.2 Two Households.....	14
3.2.1 Telephony Networks.....	15
3.2.1.1 Control and Data Acquisition Systems	15
3.2.1.1.1 Signaling System No. 7	15
3.2.1.1.2 Telecommunications Management Network.....	16
3.2.1.2 Vulnerability Assessment.....	16
3.2.1.2.1 Imperfect Past.....	17
3.2.1.2.2 Toll Fraud	18
3.2.1.2.3 Signaling System No. 7	18
3.2.1.2.4 Bugs.....	19
3.2.1.2.5 Threats	20
3.2.2 Data Networks	21
3.2.2.1 Control and Data Acquisition Systems	21
3.2.2.1.1 Routing	22
3.2.2.1.2 Domain Name System.....	22

3.2.2.1.3	Simple Network Management Protocol	23
3.2.2.2	Vulnerability Assessment.....	24
3.2.2.2.1	Architectural Concerns.....	25
3.2.2.2.2	Software.....	26
3.2.2.2.3	In-band Management.....	27
3.2.2.2.4	Human Factor	28
3.3	Network Convergence.....	30
3.3.1	Difficulties	30
3.3.2	Security Considerations	31
4.0	Recommendations.....	33
4.1	Security Tools.....	33
4.1.1	Hashing	33
4.1.2	Encryption.....	34
4.1.3	Digital Signatures.....	35
4.1.4	Certificates	35
4.2	Security Services	36
4.2.1	Connection Access Control.....	36
4.2.2	Peer Entity Authentication.....	36
4.2.3	Data Origin Authentication.....	37
4.2.4	Integrity.....	37
4.2.5	Confidentiality	37
4.2.6	Non-repudiation	37
4.2.7	Security Alarm	37
4.2.8	Security Audit Trail	38
4.3	Utility Security Recommendations.....	38
4.4	Research Areas	38
5.0	Conclusion	41
6.0	List of References.....	42

LIST OF FIGURES

Figure 1: Circuit-Switched Network vs. Packet-Switched Network	6
--	---

LIST OF TABLES

Table 1. TMN Subject Areas 7

LIST OF ACRONYMS

AD	Adaptation Transformation Device
ANSI	American National Standards Institute
CA	Certificate Authority
CLEC	Competitive Local Exchange Carrier
CUG	Closed User Groups
DCN	Data Communication Network
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DNS	Domain Name System
DoS	Denial of Service
ETSI	European Telecommunications Standards Institute
GLBA	Gramm-Leach-Bliley Act
HIPPA	Health Insurance Portability and Accountability Act
ICEC	Inter-Carrier Electronic Commerce
IETF	Internet Engineering Task Force
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
IRS	Internal Revenue Service
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU-T	International Telecommunications Union
LEC	Local Exchange Carrier
LNP	Local Number Portability
MD	Mediation Transformation Device
MD5	Message Digest Algorithm 5
MF	Multiple Frequency
MFA	Management Functional Areas
MIB	Management Information Base
NE	Network Element
NMA	Network Monitoring and Analysis
NMF	Network Management Forum

NOC	Network Operations Center
NS/EP	National Security/Emergency Preparedness
OS	Operating System
PKI	Public Key Infrastructure
PSTN	Public Switched Telephone Network
RBOC	Regional Bell Operating Company
ReMOB	Remote Observation
RSA	Rivest-Shamir-Adelman
SA	Subject Areas
SCADA	Supervisory Control and Data Acquisitions
SCP	Service Control Point
SHA	Secure Hashing Algorithm
SMS	Service Management System
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SS7	Signaling System No. 7
SSP	Service Switching Point
STP	Signal Transfer Point
TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top Level Domain
TMF	TeleManagement Forum
TMN	Telecommunications Management Network
TN	Telecommunications Network
TTL	Time To Live
US	Unites States
VOIP	Voice Over Internet Protocol
WS	Workstation

1.0 INTRODUCTION

“My God, it talks!”

Brazilian Emperor Dom Pedro uttered these words of amazement after first witnessing a telephone in operation at the Centennial Exhibition of Philadelphia in 1876[1]. His exclamation mirrored the wonder he shared with all whom first experienced the eerie spectacle of a disembodied voice with no visible owner nearby. In this instance, the owner was none other than Alexander Graham Bell reading Hamlet’s famous soliloquy. Bell could only dream of what his invention would come to be. The ubiquitous telecommunications system that grew from his work has become a massively complex, reliable, impressive, and global service that reaches into the daily lives of people. It affects us in ways we rarely stop to contemplate, except in the rare case when service is interrupted.

Today, society depends on the reliability of the telecommunications network like no other system. We expect it to always work under the most extreme and demanding conditions. This requirement is constantly levied on those individuals involved in the day-to-day operations and maintenance of this system. Anything that presents even a miniscule possibility of affecting the reliability of the system is scrutinized to the utmost extent.

As the avenues of communications spread throughout the lives of people, the expectation arises that the system will always be available. In times of dire need, such as during national security/emergency preparedness (NS/EP) situations, reliable communications networks are a must. First response disaster relief typically focuses on treating the injured, assessing the situation, coordinating assistance, and restoring communications to the affected areas. The communications system must be capable of tolerating difficult conditions and being restored easily if damaged.

The complex operations and stringent reliability requirements of the telecommunications system have spawned the development of the Telecommunications Management Network (TMN). While terminology such as Supervisory Control and Data Acquisition (SCADA) is not commonly used in the telecommunication paradigm, it is the TMN which performs SCADA’s identical functions. The TMN has the directive of facilitating the maintenance and operations of the massive underlying telecommunications system. As such, it is imperative that the TMN be capable of quickly identifying, isolating, and reporting the presence of anomalies and faults in the system. We have become so dependent upon the TMN’s capabilities that its correct operation is imperative to the national security of the United States (US).

To control the TMN is to control the complete operation of our nation’s communications infrastructure. Computers may be hacked, networks may be compromised, and devices may be subverted for the purpose of disabling communications system components or misdirecting resources. For example, consider the potential impact upon the security of our nation if a terrorist commandeered the TMN. The terrorist could command the underlying telecommunications system to grind to a halt, thus crippling our ability to communicate or to defend ourselves during NS/EP situations. Therefore, guarding the operations of the TMN is akin to guarding our nation.

This study will bring into perspective the relationship between the TMN and the telecommunications system it controls. The focus will be on security as it relates to potential cyber attacks against our nation's ability to communicate in times of need. The analysis will:

- describe the evolution and architecture of the TMN;
- explore common and critical cyber threats to the TMN including identifying the potential attackers, possible attack types and methods, and subsequent consequences of an attack;
- explain both sides (voice and data) of the underlying telecommunications network including control systems and assessments of vulnerability;
- show how the voice and data networks are traversing down a path towards true convergence and explore the emerging difficulties and security considerations such convergence brings; and
- provide recommendations on how to best move forward on securing this critical infrastructure control system.

2.0 EVOLUTION OF THE TELECOMMUNICATIONS MANAGED NETWORK

The telecommunications network (TN) is a huge, multi-carrier circuit-switched network that spans the globe for the purpose of delivering extremely reliable, toll quality voice communications at an affordable price. The TN is the standard before which all other voice services must withstand scrutiny. As such, the TN has evolved to include an overall TMN that provides for the intricate, reliable, and effective management of its resources.

2.1 History of the Telecommunications Management Network

In the late 1960s, the basic computer element was introduced into the telecommunications network to facilitate command and control operations. However, it was limited in reach as an operator was required to type commands directly at the switch terminal to implement changes. It was a rather decentralized and labor intensive approach to telecommunications network management.

Then, in the 1970s, the proliferation of telephone exchanges warranted the development of a more centralized capability for operations and maintenance. Vendors of Network Elements (NEs) began to develop their own proprietary Operations Systems (OSs) to provide this capability to operate and maintain the TN.

In 1984, when the Bell System was broken up, the Local Exchange Carriers (LECs) quickly realized that the myriad of vendor-supplied OSs were incompatible with other vendors' OSs. Multiple vendors meant that multiple OSs had to be used for all aspects of the operation, maintenance, and administration of the divested telecommunications network. This multitude of tools meant that the LECs had to tolerate higher costs for training, maintenance, and use of the tools. The original tools were confusing and did not include standardized features. Obviously, a common telecommunications network management tool was desperately needed. According to Rosenblit [2] several important criteria for a new TMN would be required for it to be successful, namely:

- Interoperability,
- Full network management functionality,
- Complete freedom of local implementation, and
- Broad industry acceptance.

Today, security of the TMN is commonly understood to be one of the most important operational criteria.

In 1985, the initial definition of the TMN resulted in International Telecommunications Union (ITU-T) Recommendation M.3000. Soon thereafter, a series of recommendations were developed to help define the TMN. Additional standards organizations began to assist and supplement the ITU-T. They included the American National Standards Institute (ANSI), the European Telecommunications Standards Institute (ETSI), and the

TeleManagement Forum (TMF), which was formerly the Network Management Forum (NMF). These organizations created a massive collection of documents that would be used in developing the TMN to enable the exchange of information between connected telecommunication networks so that end-to-end services could be managed and controlled effectively.

2.2 Overview of the Telecommunications Network

The TN evolved over the years as a result of two major driving forces in the telecommunications industry. One driving factor is providing the customer reliable communications with ever-increasing capabilities. The other driving factor is to provide these services at an ever-decreasing cost. The telecommunications industry tends to make decisions to help satisfy both of these forces simultaneously.

The TN began as a manual network with labor intensive call routing, evolved into an electromechanical network with effective but slow call routing, and then evolved into a computerized network with fast and efficient call routing. The first phase of the TN deployment required that call routing be handled by a multitude of human operators with the number of operators for a particular call dependent upon how far the call was to be sent. A sole operator could use an electrical patch cord to connect one party to another as long as their telephone circuits were collocated within a single switch panel to which the operator has access. However, if the call setup required connecting to a remote switch panel, then another operator was required to route the interconnecting patch cord at the remote location. Eventually, with enough patience and labor, a point-to-point electrical connection would establish the desired communications channel for the conversation. This channel consisted of an analog circuit that was very susceptible to noise interference that increased proportionally with the distance of the circuit. As a result, long distance telecommunications transmissions left much to be desired.

The next phase for the TN consisted of developing and deploying a network of interconnected electromechanical relays for call routing. These relays essentially removed the human operator from the process. The setup of a call was achieved by generating electrical current pulses by making and breaking the telephone circuit using rotary or pulse dialing telephones. These signals would trigger the electromechanical relays in the switching equipment to setup the point-to-point electrical connection to establish the communications channel for the conversation. This process was much less labor intensive than the manual process, but it still exhibited the problems of susceptibility to noise interference and common failure of the electromechanical relays. These problems were virtually eliminated upon the advent and deployment of computerized digital cross-connect switches in the TN.

The current phase of the TN consists of a dual-planed digital switching network that utilizes a circuit-switched transport plane for the communications channel and a packet-switched control plane for the call management. The transport plane consists of a multitude of digital cross-connect switches that create a circuit-switched transport network. This network uses digital sampling technology to enable voice conversations to traverse vast distances without experiencing the problems of noise interference that plagued long-distance analog telephone conversations many years ago. The control plane of the TN is the Signaling System No. 7 (SS7) network. It provides the backbone

signaling for the TN and is paving the way for the “Intelligent Network” that includes a plethora of new value-added services. The most important reason for deploying the SS7 network throughout the world was to enable telephone companies to share subscriber information and perform efficient call signaling procedures.

2.2.1 Circuit-Switched vs. Packet-Switched Networks

The TN utilizes both circuit-switched[†] and packet-switched network technologies. A circuit-switched network establishes a communications channel that persists throughout the duration of the call, regardless of activity on the circuit. The top portion of Figure 1 shows a typical circuit-switched network with the green lines representing the physical circuit from one endpoint to the other. Alternatively, a packet-switched network does not create a persistent communications channel for the duration of a call. Packet-switched networks deliver individual packets of data across a network from source to destination without establishing a persistent signal path. In a route-diverse network, packets traveling from source to destination may traverse different paths depending on traffic congestion or load balancing requirements. Network resources are not set aside for exclusive use by a single connection. The bottom portion of Figure 1 shows a typical packet-switched network with the maroon squares representing packets traveling between the two nodes. As can be seen from the figure, the maroon packets share the network with other packets and do not always take the same path.

[†] Although circuit-switched technology is commonly used for the transport plane of the TN, an emerging trend exists to evolve the transport plane using packet-switched technology.

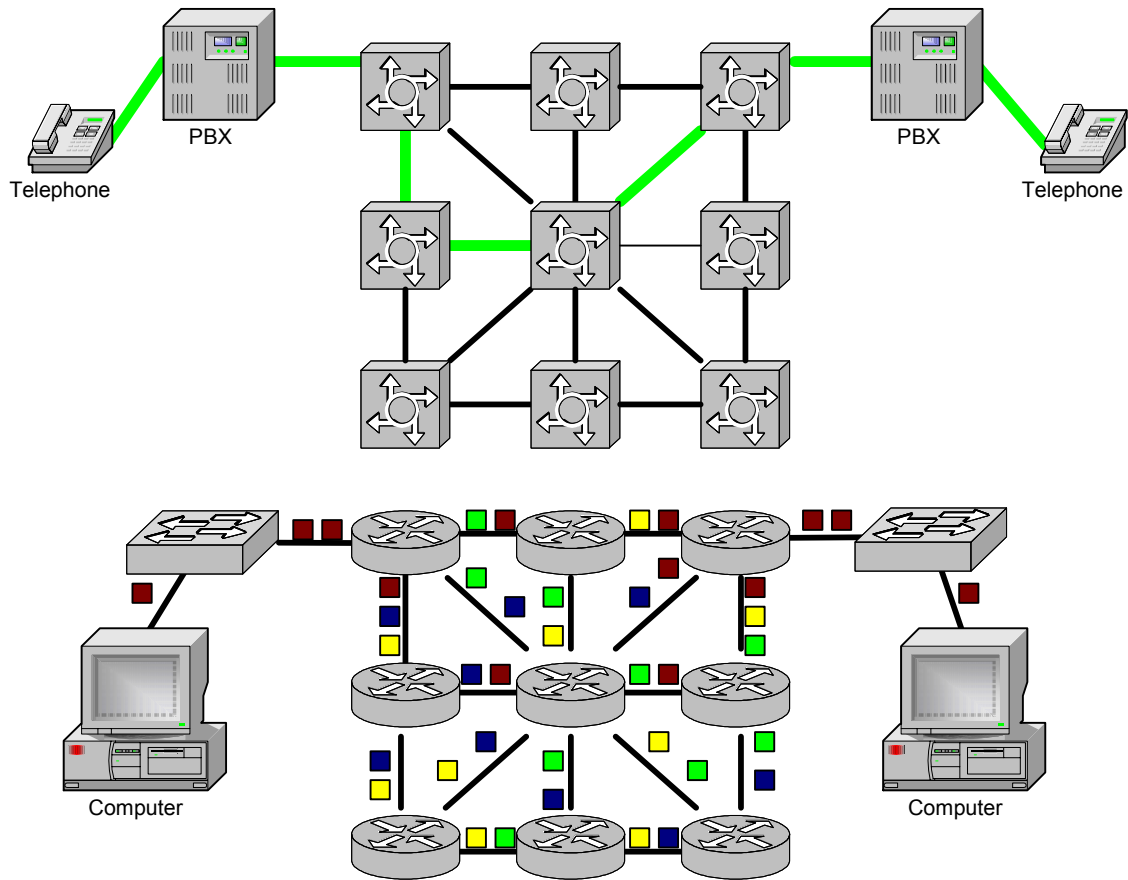


Figure 1: Circuit-Switched Network vs. Packet-Switched Network

2.2.2 Transport Plane vs. Control Plane

The transport plane of the TN is based on circuit-switched technology, and the control plane of the TN is based on packet-switched technology. When a user makes a call, digital cross-connect switches align circuit paths to provide a continuous circuit-switched path between the caller and the called party. The circuit exists for the duration of the call, regardless of activity on the circuit. Call participants are guaranteed a consistent level of performance once the call has been established. The packet-switched control plane establishes call routing for the transport plane. A more detailed discussion of the SS7 control plane is included in Section 3.2.1.1.1.

The vast complexities of the computerized TN necessitate the need for a tool to manage the network. This tool is the Telecommunications Management Network.

2.3 Telecommunications Management Network Architecture

ITU-T Recommendation M.3010 states that “the basic concept behind a TMN is to provide an organized architecture to achieve the interconnection between various types of OSs and/or telecommunications equipment for the exchange of management information

using an agreed architecture with standardized interfaces including protocols and messages.” As such, the TMN is not a part of the TN, but rather a separate entity that is used to collect data from the TN or to send data to the TN.

The ITU-T Recommendation M.3000 provides an overview of the TMN related recommendations within the purview of the ITU-T that describes the principles, architecture, definitions, and specifications necessary to implement all types of TMNs. Table 1 identifies the TMN subject areas as listed in ITU-T Recommendation M.3000. Note that this paper focuses predominantly on the architecture of the TMN and the state of security in the TMN.

Table 1. TMN Subject Areas (SA)

TMN Subject Area	Description
SA-1	Architecture
SA-2	Interface Specification Methodology
SA-3	Management Services
SA-4	Management Functions
SA-5	Management Information Models and Catalogue
SA-6	Management Information Registration
SA-7	Communication Protocols
SA-8	Systems Management Services and Management Messages
SA-9	International Standardized Profiles
SA-10	Conformance
SA-11	Terminology
SA-12	Security

The three basic elements of the TMN architecture as listed in ITU-T Recommendation M.3010 are:

- TMN Functional Architecture,
- TMN Information Architecture, and
- TMN Physical Architecture.

These architectures make up the blueprint of the TMN without which the complete understanding of the TMN would be difficult to comprehend.

2.3.1 TMN Functional Architecture

The TMN Functional Architecture describes how functional blocks may be segregated and how they interact with each other. Within the TMN Functional Architecture there exists support for the following four elements:

- Operations systems function blocks,

- Network element function blocks,
- Workstation function blocks, and
- Transformation function blocks.

Each of these four elements may be used throughout the TMN or on the edge of the TMN to bridge the gap between other entities and the TMN. For example, a transformation function block device operating on the edge of the TMN will essentially connect two functional entities with incompatible communication protocols. One entity will be the trusted TMN, and the other entity may be a foreign TMN of unknown trustworthiness. In the case of the latter, special security precautions must be taken to ensure the trustworthiness of communications traffic from the foreign TMN. In essence, all connections to entities beyond the scope of the trusted TMN must be scrutinized and effectively blocked if the security is in question. Security procedures and protocols such as those described by ITU-T Recommendation M.3016 should be implemented.

The five main Management Functional Areas (MFAs) of the TMN as identified by Rosenblit [2] include:

- **Performance Management:** Typical tasks for the Performance Management area are deciding on service parameters, monitoring service performance, monitoring network performance, instructing NEs on how to report performance data, and responding to requests for performance data.
- **Fault Management:** Typical tasks for the Fault Management area are deciding on repair priorities, processing customer trouble reports, performing root cause analyses, managing NE testing, and responding to test requests.
- **Configuration Management:** Typical tasks for the Configuration Management area include deciding on new services, processing service requests, mapping the service into network nodes, configuring the NEs to support the service, and responding to configuration requests.
- **Accounting Management:** Typical tasks for the Accounting Management area include deciding on service pricing, negotiating prices with customers, collecting and correlating usage data, instructing NEs on how to collect usage data, and responding to requests for collecting usage data.
- **Security Management:** Typical tasks for the Security Management area include formulating new security policies, managing certification paths, distributing internal security keys, managing security audit trails in NEs, and responding to requests for security audit trail changes.

2.3.2 TMN Information Architecture

The TMN Information Architecture describes an open protocol for shared data between management applications in order to support interoperability between different architectures. In general, the TMN specifications do not prescribe specific data protocols. Rather, standardized data protocols are used for communicating information between management applications. Since the management application plays a critical role in the TMN, the security of the data over the managed interfaces is vital. Care must

be taken to authenticate the data as it is shared between management applications. Access to non-authenticated data must not be allowed.

2.3.3 TMN Physical Architecture

The TMN Physical Architecture describes the physical components and the physical interfaces between components in order to help ensure interoperability between different components. The physical components include the Operations System (OS), the Adaptation Transformation Device (AD), the Mediation Transformation Device (MD), the Network Element (NE), the Workstation (WS), and the Data Communication Network (DCN).

The OS is a system that is capable of controlling the TMN and the elements within the TMN. It provides automated or user initiated operation and maintenance functions and must be subject to the security policies of the TMN. For example, if an OS communicates directly with another OS or a NE, it can utilize encryption algorithms within the control of the TMN. Additionally, the OS commonly assumes that the relative placement of it with respect to a NE is static, and thus the network address does not change. It is always a security weakness to assume that a network address is valid simply because it is static. If the device was disabled and the network address spoofed, then a security breach may be attempted.

The AD provides translation of data from a non-TMN physical entity to a NE or an OS within the TMN. The AD poses a unique security threat, since it commonly communicates to non-TMN entities that may not use a compatible interface protocol. Thus, the protocol used by the non-TMN entity must be fully understood by the AD to prevent an inadvertent lapse of security.

The MD converts protocols and transforms data received from TMN devices such as NEs that use incompatible communications protocols. Additionally, the MD may make decisions concerning the data and trigger alarms based upon whether the data from a NE crosses a threshold. Commonly the MD is a program or a small OS.

A NE may be any device or group of devices that provide network switching and data transport functions. A digital cross-connect switch is an example of a NE. A NE typically interfaces the TN to the TMN, and as such, is partly subject to the security policies of the TMN and partly subject to the security policies of the TN.

The WS performs the functions of translating information into a displayable format or graphical interface on a user terminal. Portions of the WS may be inside the TMN and portions may be outside. In particular, the WS portion that collects and translates data is inside the TMN and is subject to the security policies. Alternatively, the graphical interface is not within the TMN and therefore not subject to the security policies. Displaying information on a screen is not inherently risky as far as security of the TMN is concerned. The basic information on the screen cannot affect the operations and performance of the TMN; it would need to be used by a human in an unscrupulous manner to present a security threat.

The DCN is a support service that connects the OS to the NE or the MD. It essentially provides a path for data flow between physical blocks in the TMN. In many cases, the DCN is a packet-switched X.25 or frame-relay type of network and may consist of

multiple interconnected sub networks. Being within the TMN, the DCN is subject to all the physical and logical security policies of the TMN.

3.0 THE PHANTOM MENACE

Although a service disruption of telecommunication services would prove only a minor nuisance for most individuals, there are many cases where lost connectivity can have profound economic, social, or even national impact. Telecommunication services are no longer limited to simple point-to-point phone conversations. The role of telecommunication carriers has expanded to include a myriad of services encompassing many kinds of information exchange. More and more, the nation has come to depend on telecommunication providers for all of our communication needs, from telephones to computers.

As the networks that tie the world together have grown in complexity, so too has the technology that keeps the system operating. An army of technicians, engineers, and scientists work tirelessly to provide ever more useful and reliable services to the public. The United States is coming to rely on these systems for critical functions, but as these networks grow and evolve, they become increasingly difficult to protect. Security experts even suggest that while arbitrary individual components of the system can be protected, the aggregate will always have security deficiencies. In any system, there must be allowances made for control of the network. These allowances offer a source of access to friend and foe alike. The struggle for security is that of attempting to reconcile security and functionality. Security is a job that is never complete. It requires constant attention and vigilance in an effort to simultaneously allow network access to those that legitimately require it, while shutting out threats from those that do not belong [3].

All systems face threats. These threats increase with the importance, scale, and connectivity of the system. When a system is a critical, massive, and by definition connected entity such as the TN, it is a truly awesome target. The TN, in particular, has several unique vulnerabilities which require special attention. Additionally, while many of the threats that exist for TNs are quite generic and apply to most systems and networks, the specific context of TNs greatly amplifies those generic threats [2]. In the pages that follow, an exploration of these networks and their vulnerabilities will be presented. The topics discussed within this report should not be taken as an exhaustive list. An effort to compile such a list would prove futile in the face of an evolving industry with evolving threats. On the contrary, the topics discussed herein are offered up as an illustration of the general types of issues that the telecommunications system faces on the cyber security front.

3.1 Threats Explored

Before exploring the specific vulnerabilities present, it is useful to understand the potential attacks themselves. Identifying the potential attackers, possible attack types/methods, and subsequent consequences of an attack is arguably just as important as recognizing how the attacks would be carried out. Accurately assessing these issues helps in developing an effective security plan and dedicating resources where they are needed most. This section examines these aspects of the attacks which are likely to be encountered in telecommunication systems.

3.1.1 Attacker Groups

The first threat area to examine is that of who the potential attackers are likely to be. There are four basic groups with the motivation and general potential to perpetrate an attack on TNs. (For a more detailed exploration see Ragsdale and Grim. [4])

- **Hostile Nation-States:** As the superiority of the United States military services continues to grow, enemy states will undoubtedly seek out other methods for attacking our nation. Cyber warfare is undoubtedly an attractive tool to serve as amplification for limited resources and an alternative to conventional warfare.
- **Hackers/Hacktivism:** Whether attacking for reasons as varied as recreation to social/political motivation, this group represents a wide-range of skills and intent. Hackers quite likely represent the most common type of attacker a TN will face.
- **Cyber Terrorists:** With the heightened concern for terrorism of all types, this group has gained the most attention recently. This group attacks with the intent of creating the most high-profile, prominent, and chaotic incidents possible.
- **Disgruntled Employees:** Current or former employees with a grudge often represent the hardest attacker type to defend against. This group leaves TNs at a huge disadvantage due to their specialized knowledge of the intricate details of TN operations and vulnerabilities.

3.1.2 Attacker Type

An attacker can be classified by the skills that they bring to the attack. Each classification of attacker requires unique considerations in preparing an appropriate defense [2]:

- **External Intruder with Low-Level Skills:** These so-called “script kiddies” are usually the least threatening. They employ ready-made tools that exploit commonly known vulnerabilities. Often these vulnerabilities are due to software bugs that have been addressed through the issuance of a patch provided by the software vendor. These threats should not be overlooked. However, as is discussed in Section 3.2.2.2.2, software patches present dilemmas to system administrators that are not easily overcome. A system unprotected from these vulnerabilities can represent a serious threat posed by this group.
- **Sophisticated Intruder with High-Level Skills:** This is a higher class of an intruder. They use advanced technical knowledge and skills to attack a system using vulnerabilities not widely known to the public and possibly discovered by their own investigation.
- **Physical Intruder:** While the previous two classes of attackers try to gain access to systems from outside of the normal operational setup, this class establishes a physical presence on the inside of the system. In this case, the attacker can operate in what are often less restrictive environments behind a system’s external defenses.

- **Trusted Client:** This class employs access that would not otherwise be available to the general public by becoming a client or otherwise affiliated entity with the service provider being targeted for an attack.
- **Insider:** The most difficult class of attack comes from the inside. This attack springs from someone that is a trusted part of the system's operational activities. Such an individual does not need to defeat many security measures because they have been given authorized access to system resources.

3.1.3 Attack Type

Almost all successful attacks on TNs rely on one of several broad types. These types are distinguished by the underlying system vulnerability that is being exploited to make the attack successful [5]:

- **Misauthentication:** These attacks are those that undermine the authentication mechanisms present (or in some cases not present) in a network. An attacker somehow is able to convince the network security measures that they are an entity that should be allowed access to the system. There are many technologies that can be employed to prevent or deter these kinds of attacks by strengthening authentication methods (see discussions on encryption, digital signatures, and certificates in Section 4.1 below).
- **System Malfunction:** Attacks of this kind exploit some accidental deficiency in the system, such as software bugs, misconfigured equipment, or insecure protocols. Much harder to protect against than the former, these attacks prey on unintended operational behavior. The only way to prevent this attack is to design, develop, and deploy bug-free network tools, a task which has proved to be a long-standing challenge.
- **Abuse of Privilege:** The most dangerous type of attack comes from an attacker who has been willfully given access within a system and then proceeds to abuse those privileges for their own purposes.

3.1.4 Attack Activities

After an attacker successfully breaches the security of a system, there are several classes of activities that an intruder can utilize to accomplish their goal [2]:

- **Unauthorized Access:** An attacker can gain access to billing information, personal information, or other information that is not meant for public disclosure.
- **Information Modification:** The unrestricted access to private data can be used to modify records. Information integrity cannot be trusted after a system has been compromised.
- **Eavesdropping:** With sufficient access to a data network, all of the communicated contents (private data, telephone conversations, etc.) can become available to an attacker.
- **Masquerade:** An intruder can use their control of the system to employ deceptions for any number of schemes. Playing upon the trust that is placed in

proper network operation, attackers can reconfigure the switch as they see fit to serve their purposes.

- **Repudiation:** Activities on a system are typically monitored allowing all actions to be traced if later required for audits. If a system's security has been breached, actions can be taken for which there are no records or for which records have been modified. This would allow changes to be made or services to be received with no record of them ever taking place.
- **System Modification:** An attacker could wreak havoc by reconfiguring a system for utter chaos or other devious intentions. Sufficiently compromised systems could be modified to replay, reroute, misroute, delete messages, or prevent connection. Imagine the security implications if sensitive communications were retransmitted to a hostile entity.
- **Network Flooding:** A network could be brought down by the creation of superfluous traffic, clogging and congesting the pathways for data. Mass confusion would result.

3.1.5 Attack Classification

As a result of any manner of combination of these types of attacks, certain types of consequences can be experienced in a system [2]:

- **Theft of Information:** Sensitive, important, or otherwise private data can be stolen during the course of an attack. Internal information can be priceless to an entity and devastating in the wrong hands.
- **Unauthorized Use of Resources:** Involves the use of resources to which an attacker is not entitled (such as bandwidth).
- **Theft of Service:** Probably the most commonly perpetrated type of attack in telephony. It involves the use of resources for which there is no compensation (e.g. free long distance services).
- **Denial of Service:** Quickly growing in occurrence, Denial of Service (DoS) occurs when a system does not provide the function for which it is intended. This can occur due to reconfiguration or, more commonly, due to a maliciously overloaded system.

3.2 Two Households

From the humble beginnings in the original Bell laboratory, the telecommunication system has developed into a complex entity. No longer relegated to mere voice traffic (telephony), it has since branched out to carrying data as well. Originally carried over simple phone lines, expanding data transport needs have seen an entire infrastructure developed around it. Indeed much of the modern telecommunication system holds voice and data network controls in isolation, each with its own independent control and monitoring system. These systems have diverged so significantly that they each require independent consideration.

3.2.1 Telephony Networks

It all began with voice. As discussed, the advent of new technology aided the telephone system in shifting from employing human telephone operators to the use of more and more automation for control and monitoring. Telecommunications has been a major driving factor in the development of such technology and has produced some truly amazing equipment to handle the unique set of requirements offered up by the services they undertake.

3.2.1.1 Control and Data Acquisition Systems

The phone system has moved beyond the days when it was a set of mechanical switches making physical connections of copper loops connecting every phone in the country. As it has developed it has added many valuable services, such as toll-free numbers, call forwarding, network-based programmable call distribution, conference calling, and message delivery. The development of the underlying systems necessary to provide these services and offer ever increasing flexibility has caused a corresponding increase in the complexity of the system. And as any system becomes more complex, it becomes harder to secure [2].

3.2.1.1.1 Signaling System No. 7 (SS7)

Technophiles who pursued an interest in telephony came to be known as “phreaks”. Phreaks are a dedicated group quite talented at discovering oddities in and manipulating the telephone system. They were even ingenious enough to learn how to make free long distance calls using a toy whistle out of a Captain Crunch cereal box. However, for the phreak not inclined to eat sweet cereal, there was an active trade in information on the construction of several (arbitrarily) color-coded boxes that could be used for various purposes (e.g. blue box – free long distance calls, red box – free payphone calls, etc.) [6]. Phreakers were able to do these things because the signaling used to control the calls was transmitted on the same line used for the voice transmission employing in-band multiple frequency (MF) signaling tones.

All communication between modern central-office switches now takes place over “out-of-band” signaling using the SS7 industry standard. Out-of-band refers to the fact that these signals are carried on a separate communications channel than the one that they are controlling. SS7 was developed as an out-of-band protocol partially to help prevent the fraud being perpetrated by phreakers that was becoming increasingly prevalent [2]. By separating the two systems which respectively provided voice services and call management, TNs were able to more effectively restrict access to would-be phreaks. Along with additional security, out-of-band signaling provided faster setup times in comparison with in-band based MF tones and more efficient use of voice circuits [7].

In fact, SS7 was so efficient that when it was initially deployed, call setup delays dropped from multiple seconds to one second or less. As a result, many people who were used to waiting for the called extension to begin ringing didn’t believe that their outgoing call could be setup so quickly. They thought that some type of error must have occurred and would hang-up and dial again. To help ease this “problem” with SS7, call setup delays were artificially introduced into the system and systematically reduced over several

months. People were gradually eased into accepting the new fast service that SS7 provided.

The SS7 control network functions primarily for basic call setup, management, and tear down. But SS7 has also proved essential to the widespread adoption of common features such as wireless roaming services, local number portability (LNP), toll-free (800/888), toll (900), and enhanced telephony features (call forwarding, caller ID, three-way calling, etc.) [7].

The topology of the SS7 network includes three main network elements as described below [8]:

- **Service Switching Point (SSP):** SSPs are the endpoints of the SS7 network. They are typically part of a Public Switched Telephone Network (PSTN) end office and are the SS7 network's connection to the voice network. SSPs can either initiate SS7 signaling messages or be the intended destination for them.
- **Signal Transfer Point (STP):** Serving a similar function as routers in an Internet Protocol (IP) network, STP network elements route SS7 signaling message traffic through the SS7 network and collect traffic measurements. If an STP does not have sufficient information to determine how a call should be processed, it must call upon the third network element, an SCP.
- **Service Control Point (SCP):** The SCP network element's primary role is to provide value-added services. Upon receiving a request, the SCP provides database access for any number of services such as LNP, three-way calling, caller ID, etc.

Service provider domains consist of many network elements managed by a centralized SS7 network management system called the Service Management System (SMS). Overall, SS7 provides a rather impressively redundant and reliable network that has proven very fault tolerant. For a detailed exploration of the SS7 network operation please see Ragsdale[8].

3.2.1.1.2 Telecommunications Management Network

While SS7 is designed for the control and data acquisition for telecommunication services, there remains the need to monitor and configure the equipment upon which both the telecommunication services and the SS7 network rely. In response to this need, the telecommunication industry has provided a myriad of different options from which service providers can choose in implementing a TMN. These options range from employing an industry vendor's ready-made solution, such as Telcordia's Network Monitoring and Analysis (NMA) system, to developing custom tools that rely on open protocols, such as Simple Network Management Protocol (SNMP) [9]. Fortunately, in almost all cases, these solutions reduce to data networks, which are further covered in Section 3.2.2.

3.2.1.2 Vulnerability Assessment

Telephony systems have become renowned for their remarkably reliable systems. Often marketing their services as reaching a level of reliability known as "five nines," referring to 99.999% system availability, telephone service providers have developed a base of

customers that expect an unprecedented consistency in service. Americans are fairly accustomed to occasional outages in their electricity, cable/satellite television, and even the water supply, but always expect a dial tone to be present when they pick up the phone to lodge a complaint about other services. Indeed, telephone service suppliers that are able to live up to “five nines” availability provide service that may be disrupted for less than six minutes out of every year!

This kind of reliability comes as a result of extensive investment in creating a system with the necessary redundancy and flexibility to adapt to the various factors that can take a telephone system down. The commitment to security displayed by telephony providers is equally impressive. Industry insiders are exceedingly tight-lipped when it comes to specific details about the systems they represent. This was very strongly encountered when attempting to conduct face-to-face interviews during the course of research for this paper. The industry enjoys a very healthy culture of distrust for outsiders, and this proves particularly important in defending against the surprisingly effective use of social engineering [9].

3.2.1.2.1 Imperfect Past

However, even the telephone system is not bullet-proof, and exterior meddling with telecommunication systems is not unprecedented. For many years most TN companies operated under the assumption that their systems were untouched by outsiders. But a prank pulled on June 13, 1989 brought such illusions crashing to a halt. Callers to the Palm Beach County Probation Department were surprised to have reached not a probation officer, but an adult-oriented phone service attendant named Tina instead. The simple call-forwarding hack had been setup by a 16-year-old that used the alias “Fry Guy.” Fry Guy’s tomfoolery blew open the doors on what had otherwise been a quiet underground scene of phone system enthusiasts [10].

The incident triggered an alarmed BellSouth Regional Bell Operating Company (RBOC) to perform an exhaustive investigation of their system. No less than 42 BellSouth employees worked 12 hour shifts around the clock examining records and monitoring systems for signs of unauthorized intrusion. The “Intrusion Task Force” findings astonished the industry. There was clear evidence of manipulated databases and mysterious phone numbers with no associated user names or addresses (and no accompanying revenue stream). Even more alarming was the discovery that their new digital ReMOB (Remote Observation) diagnostic feature had been extensively hacked, allowing intruders to listen to any switch-routed calls at will [10].

Understandably, these discoveries caused a great deal of alarm. Many critical services relied upon a telephone system that lacked integrity. Furthermore, the trusted phone system was clearly vulnerable to many forms of mischief and abuse. Prior to this event, users of the phone systems had no reason to question the concept of a phone number reliably mapping to an expected location. Indeed, further investigation of Fry Guy revealed that he had used these expectations to defraud Western Union and its customers of money in various credit card scams involving the remapping of telephone numbers [10].

Incidents of this nature illustrate how vulnerabilities can spring from seemingly benign additions to a system. New features themselves can lend themselves to mischief and

misuse, as was the case with call forwarding in this example. With this ability callers could no longer be assured that their calls reached the location they had intended, and likewise, recipients could not be sure that they were the intended recipient of a call. Indeed, a large-scale remapping of phone lines could cause exactly the kind of chaos that terrorist organizations seek in their attacks [11].

3.2.1.2.2 Toll Fraud

Evidence suggests that the preponderance of attacks on telephony systems, public and private alike, involve attempts at toll fraud. The industry has grudgingly come to accept a certain level of toll fraud as unavoidable, as they do not find it viable to commit the resources necessary to eliminate it [5]. Most private companies and institutions devote very little effort to securing their telephone systems, choosing instead to focus security efforts on their data networks. This practice is fueled by the more prominent presence of reports indicating attacks on data networks. Toll and PBX fraud goes much further back into history and does not provoke the same response as news of the latest crippling worm wreaking havoc on data networks. Unfortunately, incidents of high-volume toll fraud appear to be on the rise, and this has started to attract the interest of the savvy Information Technology (IT) administrators [12].

Telephony providers have had much success at detecting mischief by employing automated traffic analysis mechanisms that can flag abnormal activities for further investigation. Such efforts are wise as, depending on the methods being used to perpetrate toll fraud, complacency can be a dubious and risky practice. An intruder with access to the TN's backend functionality has the power to expose an organization to serious legal liabilities, damaging public image issues and large financial burdens simply by maliciously manipulating the system [12]. In general, it is good practice for any unauthorized control plane access in telephony systems to be treated with zero tolerance [5].

3.2.1.2.3 Signaling System No. 7

The adoption of SS7 was an important part in the modernization of the world's TNs. As mentioned, SS7 traffic travels over an entirely separate channel than the communications network. Moving these critical signaling functions out of the easily assessable communication channels was a crucial step in securing the phone system. In fact, in the United States this separate channel is often carried over a completely separate network in an effort to further increase the security and integrity of system control [13]. However, it is significant to note that this is a case where new security measures themselves can actually create new vulnerabilities. The adoption of such an architecture means that there are now two mutually dependant but completely separate systems that rely upon each other for any functionality. One operating without the other is useless. The signaling system itself can be targeted, allowing an attack to disable phone service even when there is nothing at all wrong with the telephony network [2].

Furthermore, while SS7 was designed to be highly flexible and redundant, it is still limited by the network structure of the underlying voice network. The nation's telecommunications grid forms a loose hierarchy, and because telecommunications equipment has proven so reliable, the system often relies heavily upon relatively few large switches to provide nationwide connectivity. If strategically selected switches were

brought down in a cyber attack, the nation's telecommunication networks could become isolated [14].

The biggest threats to SS7 come from its increasing interconnection with an ever-growing number of network entities. Regulatory mandates have brought many new players into the telecommunications sector. Due to this, the once tightly controlled signaling network has come under the influence of a large number of relatively new players in the industry, exposing it to the many vulnerabilities of its less experienced brethren [14]. Interconnections are the weak points common to almost any communication system, even when implemented in the most secure fashion possible by both parties; it represents yet another crack through which an attacker can slip. Unfortunately, due to the fact that the two parties involved in these interconnections often are direct competitors of each other, it can prove particularly difficult to establish the trust and communication necessary for successful interagency security [10].

3.2.1.2.4 Bugs

As discussed in Section 3.1.3, some vulnerabilities are present in a system even if its configuration is perfect. Such threats are due to flaws in the communication protocol, hardware, or software. On January 15, 1990 service to a large contingent of AT&T customers went dead due to such a flaw. A misplaced "break" statement in C computer language code caused a massive cascading failure. The crash lasted 9 hours, thus disrupting phone service for around 60 thousand people and causing approximately 70 million phone calls to go unconnected. AT&T estimated \$60 million dollars in lost revenue and damages from a tarnished reputation. The damage to their reputation was further amplified by an ironic marketing campaign mounted concurrent to the outage which focused on AT&T's superior reliability. However, these monetary loss estimates account only for the losses of AT&T and do not attempt to quantify the losses suffered by their clients or the critical services knocked out as a result of the outage [15].

The widespread system fault occurred despite conscientious efforts at designing an extremely fault-tolerant and robust system. A malicious attack was seriously considered when trying to track down the cause of the failure. Although subsequent investigations came to reveal that the outage could have been easily triggered by an attacker, in this case there was no evidence of foul play [15].

It can only be assumed that similar kinds of vulnerabilities still exist throughout the telecommunications networks in operation today. The complexity of the systems is such that imperfections seem unavoidable. Further complicating the issue is the fact that even when a vulnerability has been identified, the course of action is not clear. Fixes for software flaws are very commonly released in the form of software patches, but the application of these patches has proven rife with incidents where the patch creates further security problems or other system incompatibilities. Testing the patches is even more difficult, as testing cannot safely be done on production systems, and it is hard to adequately simulate them. Hardware bugs and problems with the underlying protocols are even harder to combat, as the costs involved in fixing the problems are much greater.

3.2.1.2.5 Threats

The ability of telecommunication companies to monitor and control their systems has vastly improved the level of service that they are able to offer. However, the conveniences provided by the TMN have opened up their own set of generic vulnerabilities [2]:

- **Remote Management:** Increased automation and functional centralization in the TMN is accompanied by the dangers opened by increases in remote management capabilities. As human influence over the network retreats to more centralized posts, the capabilities to affect the network remotely, if insufficiently secured, can be utilized by attackers as well.
- **External Entities:** Interactions with external entities often increase, opening yet more avenues to facilitate an intruder's task.
- **Standard Interface:** As the technology for network management matures, standardization of the control system increases and leads to greater availability of information on the communication protocols used. Indeed detailed information often can be easily obtained on the Internet.
- **Open System Interfaces:** Protocols become increasingly abstracted from the equipment upon which they run. Whereas attackers may have needed to know specific information about a system, such as the operating systems running on connected devices, now the system operation depends less on such details.
- **Transfer Syntax:** Management systems are increasingly using common transfer syntax, such as Transmission Control Protocol/Internet Protocol (TCP/IP), which lends itself to easier decoding and interpretation by an intruder.
- **Scope and Filtering:** In an effort to produce more efficiently managed networks, many management systems allow for massive system reconfiguration to be deployed with relatively few system commands. In the past, reconfiguring large portions of a system involved individual polling and commanding each network element. Modern interfaces sometimes allow multiple elements to be addressed via a single command or query. With greater impact coming from fewer commands, not only is it easier to produce large effects on a network, but it becomes harder to detect such actions.

Along with the vulnerabilities that are generic in TMN, there are issues that are specific to the regulatory environment within which telecommunication companies must work. The Telecommunications Act of 1996, which included efforts to create competition in previously monopolistic telecommunication markets, fostered the arrival of many new telephone service providers known as Competitive Local Exchange Carriers (CLECs) [16]. Among the regulatory changes were provisions that mandated cooperation between Incumbent Local Exchange Carriers (ILECs) and the CLECs. The resulting electronic interfaces between the two create an Inter-Carrier Electronic Commerce (ICEC) that carries unique security issues [2]:

- **Exposure:** The well developed ILEC control systems are exposed to external entities, increasing pathways into the system. As is a consistent theme in network security, increased connectivity implicitly decreases the level of security.
- **Competition:** As competition has mounted, there are significant cases of unethical practices performed by competing entities. Practices such as “slamming,” the illegal and unauthorized modification of a customer’s preferred interexchange carrier of record.
- **Interfaces:** The necessary interfaces between ILEC and CLEC sometimes must travel over data networks not under the control of either party. This leaves the LECs dependent upon external agencies to provide the level of security they require.
- **Weakest Link:** All LECs participating in the ICEC are potentially exposed to the vulnerabilities presented by the weakest link in the group. This means that even a LEC employing excellent security practices can be made vulnerable by an agency outside of their control.
- **Criminal Front:** It is very possible for a criminal organization, or other malicious group, to set up its own CLEC as a front with no intentions other than committing theft, fraud, or mischief. In these cases even legitimate traffic from the CLEC could have harmful consequences.

3.2.2 Data Networks

Soon after phone users got used to the idea of communication over distances, they began to seek services beyond voice. This, coupled with the rise in use of computers, led to a natural extension of the far-reaching communications network to include the transport of data. While initially piggy-backed onto existing voice networks, data communication systems developed on their own into sophisticated high speed networks. As these networks developed, data and voice networks moved further apart, diverging significantly in their methods of delivery. Whereas telephony has stuck close by circuit-switched roots of using a dedicated and guaranteed circuit from endpoint to endpoint, data networks have experimented with packet-switched networks. Indeed the predominant data network in existence today, the Internet, has driven widespread adoption of the completely opposite mode of information transport found in TCP/IP packet based networks. Because of their prominence, it is these types of data networks upon which this paper will focus.

3.2.2.1 Control and Data Acquisition Systems

The largest and most relevant data network in existence is the Internet. Because of the almost ubiquitous acceptance of the technologies that drive the Internet, it has laid the foundation for data networks across the nation. The security concerns of the public Internet mirror those of private data networks throughout the world. The Internet is formed by the interconnection of many smaller networks. Driven by the underlying TCP/IP twin protocols, the Internet consists of many autonomous systems collaborating to provide universal connectivity using dynamic paths from one node to another. This multi-network collaboration is not owned or operated by any sole entity. Several organizations have been created to guide its development and help keep order. However,

control of the network still rests in the hands of the system administrators that oversee the many individual systems connected to it. These administrators work collaboratively to keep the Internet running by maintaining the critical components discussed below.

3.2.2.1.1 Routing

Due to its decentralized and ever-changing topology, the Internet was designed to function in a best effort system consisting of a multitude of hosts, communication lines, and routers. These elements work collectively to guide individual packets towards their intended destination, with no guarantee of the path that will be taken or even that they will indeed ever arrive. Hosts act as endpoints, sending out data on connected communication lines that make their way through their own sub-network. If the packets are destined for a host beyond the local network, they are sent to the decision makers of the Internet: routers. A router acts as a bridge between the network segments that are connected to it. Its job is simply to take in a packet and then determine which outgoing communication network should be used to send the packet on its way. No router can have a complete map of the Internet, but routers actively seek to determine the very best path to any destination by cooperative communication with neighboring routers. A router is constantly collecting information on the link health and host availability related to all of its connected communication links, and this allows the Internet to quickly adapt to changing network conditions.

Routers are the enabling technology that has allowed the Internet to exist as the connection of a multitude of smaller networks. They have permitted the Internet to scale remarkably well, and it is through their configuration that the greatest control can be asserted over the system as a whole. Efficient route selection is crucial to smooth operation, and routers communicate using a variety of routing protocols which differ in the method and type of information they share about the networks to which they are connected.

3.2.2.1.2 Domain Name System

In general, humans prefer to work with words rather than numbers, whereas for computers, numbers are the easier paradigm. The developers of the Internet understood this, and the Domain Name System (DNS) was developed to allow a numerical addressing scheme to coexist with a more human-friendly text-based system. DNS exists to take the familiar host names such as `www.google.com` or `www.amazon.com` and map them to the numerical IP addresses (`64.233.187.104` and `207.171.175.29` respectively) required for transport on an IP network.

Early implementations of IP networks used a centrally maintained host file to map host names to IP addresses, but changes in a host's IP address or the arrival of additional hosts to networks would not be recognized until the host file was updated and redistributed. Growth in the size of data networks strained the host file server and called for a more scalable solution. DNS was developed in response to this need. DNS, in effect, is a massive distributed database that works by hierarchically distributing the load to child name servers.

DNS operation is most easily explained using an example. When an application seeks information from a host on the network, it will request the IP address from the operating system's DNS client. The DNS client then checks its own cache (described in more detail later) to see if it already knows the IP address of the requested host. If it does not, it will submit a request to a local DNS server. The DNS server can be a server on the local network, or it is often provided by the network's Internet Service Provider (ISP). Upon receiving a request, the DNS server checks its own cache to see if it already knows the IP address of the requested host. If it does not know the current IP address, then it will start its search by making a request to a root DNS server. At this point it is useful to further explain host names.

Host names consists of one or more names (called labels) separated by dots. A typical host name, such as `www.google.com`, has three labels. Each label will help narrow the search for a domain name server which can provide the required IP address. When a local DNS server determines that it must search for the IP address, it will ask a root DNS server for the IP address. Root DNS server IP addresses are known and change very infrequently. Their IP addresses are programmed into local DNS servers (there are currently 13). The local DNS server sends its request to a root DNS server asking, for example, for the IP address of `www.google.com`. The root server responds by saying that although it does not know the IP address for that specific host, it does know the IP address for a DNS server which keeps track of information for `.com` addresses.

This first level, `.com`, is known as a top level domain (TLD). Other TLDs include `.net`, `.gov`, `.edu`, etc. The local DNS server would then proceed recursively, requesting the desired host's IP address from the `.com` DNS server who would then redirect it to the google subdomain's DNS server. At this point, when the google DNS server is asked to provide the IP address for `www.google.com`, the correct address is finally retrieved.

At several points in this process the opportunity for caching can make the system more efficient. If the DNS client on the machine that runs the application has recently requested the address, then it does not need to trigger the whole procedure to run again. Likewise at any other step, if the information at a given level is available, such as the case where the DNS server for `.com` addresses is known, the DNS server is not required to repetitively request it each time it is needed. Indeed, such unnecessary queries are actively discouraged in order to limit wasteful traffic. To ensure that inconsistencies don't linger when IP addresses change, the DNS specifies a time to live (TTL) for each cached query response. This effectively starts a clock on the information retrieved. When the clock expires, the request must be resubmitted.

3.2.2.1.3 Simple Network Management Protocol

SCADA functionality for data networks is found in the popular and extensively deployed Simple Network Management Protocol (SNMP). Development of SNMP provides a unified monitoring and configuration protocol for IP networks. SNMP based network management tools act as clients which communicate with an agent running on an SNMP capable network element. SNMP works by interacting with values identified in a Management Information Base (MIB). These values, referred to as SNMP objects, are comprised of many different predefined types, including text fields, timer values, IP addresses, etc. A core MIB is defined by the standard, but SNMP is flexible and allows

for custom objects to be defined and added to the MIB maintained by management tools. It is this flexibility that has allowed SNMP to enjoy such widespread adoption [17].

As the name would imply, the foundation of the protocol is quite simple. SNMP devices are monitored and configured using one of four message types [17]:

- **Get Request:** This message is used by the network manager to fetch a MIB value. It can be used for polling network device status, performance and settings. Get requests are followed by a get response from the agent.
- **Get Next Request:** This message walks through successive object entries in the MIB. Repetitive use of this message is useful for obtaining large amounts of information from the device.
- **Set Request:** The only message which actually changes values in the MIB, this message is sent by the network manager to trigger an action or reconfigure a device.
- **Trap Message:** The only message originated from an SNMP agent instead of the network manager, this message is sent by a network device that seeks immediate reaction to an event or problem. Using a trap message, a network device can trigger an alarm or indicate some other issue that needs an urgent response. SNMP agents must be programmed with the network host to which traps should be sent.

SNMP is an extremely widespread network management protocol in use throughout data networks. But its use has not been without problems. Several iterations have been developed, primarily due to security concerns:

- **Version 1:** The original iteration which suffered much criticism for its nearly non-existent security. Authentication was limited to a “community string,” which was in effect a simple password sent in clear text over the network.
- **Version 2:** The first attempt at adding security to the otherwise accepted SNMP protocol. This iteration was never widely adopted due to concerns about the overly complicated security scheme it employed. Several sub-versions were developed that sought to balance the gained security with the simplicity of version 1.
- **Version 3:** Recognized as the current standard by the Internet Engineering Task Force (IETF), this version supplanted earlier versions by offering enhanced security without the high complexity found in version 2. Version 3 includes support for data encryption and authentication. Many SNMP agents support multiple versions of the protocol for backwards compatibility. This capability is covered in IETF Request for Comments (RFC) 3584.

3.2.2.2 Vulnerability Assessment

Although the data networks based upon TCP/IP technologies have proven to scale amazingly well, their decentralized and adaptive nature makes it very difficult, if not impossible, to ensure that operations will continue smoothly for an indefinite period of

time. TCP/IP networks take effort to secure from the numerous vulnerabilities inherent to their nature. These vulnerabilities are discussed below [5].

3.2.2.2.1 Architectural Concerns

Modern data networks are vast and complex entities using many different layers of abstraction to form a functioning network for transport. These layers build, one upon the other, to offer increasingly complex services. The elements of this architecture give rise to architecturally related concerns which are covered in detail by Ragsdale and Grim [4] and are briefly reviewed here:

- **Open Standards:** Industry has gravitated toward using open standards protocols in data networks due to the significant value they offer in increased security and interoperability. Overall, this is a benefit to the networks that use them. But the same intensive review to which open systems are subjected also exposes them to the documented vulnerabilities that are found in the public review process. As vulnerabilities are found, the protocols are nearly always adapted to be more secure. This reinforces the notion that system administrators must remain vigilant in keeping their systems up to date in order to avoid system exploitation.
- **Ethernet:** Data systems make extensive use of Ethernet networks for IP transport because of its low cost and high compatibility. But the use of Ethernet opens some security concerns as well. Ethernet systems were originally designed for trusted environments, where all hosts on the system were expected to be friendly. As such, data sent over Ethernet systems share a common medium, and data visibility is not limited to only the sender and receiver. Switched Ethernet systems add some level of protection, limiting the hosts that receive the data, but even these systems can be tricked into distributing data to third parties.
- **Wireless:** Wireless communication is extremely attractive for the reduced infrastructure costs. But use of wireless communication means actively broadcasting information over an inherently insecure medium. Because the medium cannot be secured, steps must be taken to protect the transferred data by obscuring the information broadcasted. Encryption technology is essential for this protection to be possible, but previous attempts to add this protection to wireless communication have proven vulnerable to exploits.
- **External Connections:** Data networks are growing ever more interconnected. Every connection that reaches beyond the system administrator's control is a doorway into the system. These doorways prove to be inherently weak points in the security of networks. These weak points are difficult to strengthen. If the connected network is the Internet, then the external connection exposes a system to an extraordinarily hostile environment.
- **Weakest Link:** The strongest of security can be cracked by the weakest link. There are numerous examples where a conscientious and comprehensively secured system was foiled by a trivial vulnerability.

3.2.2.2.2 Software

Millions of computer terminals across the globe are active participants in the health of the data networks to which they are connected. They can often represent the weakest links in the system. Unfortunately the current state of computer software running on these hosts is plagued with bugs and security issues. While there are intensive efforts at improving these problems, the reality is that these vulnerable systems pose a huge threat to data networks.

Much notoriety has been given to the high profile “worms” that have been unleashed on the Internet. Experts estimate that the devastating Structured Query Language (SQL) Slammer worm, after originating somewhere in East Asia, quickly spread throughout the world, doubling in infection rate every 8.5 seconds and affecting 90% of all vulnerable machines in under 10 minutes [18]. The traffic these worms generate is enormous and quickly overwhelms the capacity of the Internet. The best-effort methodology used by IP networks cannot effectively cope with a situation where vastly greater amounts of traffic are generated than the system can handle. The congestion that follows brings communication to a painfully slow crawl.

In contrast to the highly visible effects of network flooding worms, recent efforts by security researchers highlight that more than a million computers on the Internet have been compromised and act as silent “zombies,” pumping out spam and viruses. The group conducting the research, The HoneyNet project, worked for months tracking what happened to so-called “honey-pots,” computers put on the Internet with the sole intention of attracting hackers. Hackers latched onto the honey-pots with surprising speed. The HoneyNet researchers found that the longest one of their machines existed on the network before being found by a remote automated attack tool was merely a few minutes, with some being found in seconds. Once found, attackers went to work exploiting well-known vulnerabilities in the operating system. Computers not kept up to date with the latest patches and security updates, as these computers intentionally lacked, are quickly compromised. This sheds light on the fairly common practice of attackers actively amassing large armies of compromised computers on the Internet, representing an impressive pool of computational resources and bandwidth with which to carry out their bidding [19].

The intentions driving the procurement of these vast numbers of compromised computers seem to represent a wide variety of purposes. The researchers found that the computer networks were [19]:

- aiding in the relay of spam messages, routing unwanted advertisements to a multitude of email boxes,
- assisting the propagation of computer viruses,
- abusing pay-per-click advertising schemes, producing profit from fraudulent click-through traffic, and
- acquiring sensitive personal information by hosting fake websites meant to appear as legitimate websites (such as a bank).

These exploits rely on weaknesses or bugs in faulty software to propagate, and they do so with remarkable success. The necessity for increased security in network endpoint systems has, thankfully, received much needed attention from software developers. Industry is cautiously optimistic that future software releases will show the evidence of these efforts. Until then, prudent IT departments are focusing on keeping systems under their control up to date with the latest patches (when possible) and protecting their networks with strict firewalls and security policies.

3.2.2.2.3 In-band Management

Many of data network's vulnerabilities spring from the fact that in most cases the networks employ in-band management and control services. Because the control and monitoring traffic travels over the very network which it is serving, it is much easier for a cyber attacker to exploit the control systems for their own gain. Furthermore, because this critical traffic shares its cyberspace with data traffic, the vulnerabilities of the network and its control systems collide. Security risks of both are one in the same with issues in both domains affecting operations of the other. To effectively evaluate the existing vulnerabilities requires exploration of the network as a whole, as is found in this report.

A good illustration of this codependent relationship is seen in the DNS. As discussed in Section 3.2.2.2.2, IP network's endpoints represent its weakest components. Since network management takes place over in-band communications, crucial services such as DNS are added to this list of vulnerable endpoints. Furthermore, since DNS is provided by servers which typically run on bug-ridden commercial operating systems, they inherit all the vulnerabilities that use of this software entails. The DNS allows for a lot of flexibility in the system. IP addresses can change; indeed the entire underlying structure of the network can drastically be altered with complete transparency for its users. But if a DNS server is compromised, this flexibility can prove an alarming security threat [11].

Although IP networks can function without a DNS, because most users have come to rely on it, DNS is now absolutely critical to the operation of the Internet. If an attacker is able to compromise a name server, they can effectively disable all communications in networks that depend upon that server. By preventing a DNS server from responding to client requests for IP resolutions, the attacker has successfully executed a denial of service attack. Disruption of network communications can be an extremely effective attack given the circumstances, but control of DNS servers also provides a much more salacious and potentially dangerous possibility.

As discussed, DNS maps host names to IP addresses in a manner completely transparent to applications which use the service. The IP address received in reply to a translation request is used to carry out the actual communications. Attackers can exploit this by manipulating the DNS to provide the wrong IP address. False information can be injected in several ways. The DNS makes heavy use of caching in many levels of the database hierarchy. These caches can be manipulated either by hacking into the name servers themselves, providing false information to a DNS query, or by modifying the locally cached copies of DNS responses in end stations.

The result of such manipulation, known as DNS cache poisoning, is that a network client can be fooled into initiating a communication session with a hacker's computer under the

guise that they are communicating with some other server. This obviously can have undesirable consequences, such as the unintentional divulgement of sensitive information. So-called “phishing” is a common attack where the user is fooled, for example, into thinking they are logging into their bank’s online system or online auction site only to have inadvertently revealed their login information to a third party. DNS poisoning also allows for man-in-the-middle attacks, allowing an attacker to act as a relay between the user and their intended server, all the while monitoring and collecting the transferred data.

Other in-band management functions particularly vulnerable to exploit are the routing protocols used to distribute network link state and route information. Most IP networks rely heavily on trust. The reliance on trusted relationships, a decision founded upon functional assumptions made during earlier days of the Internet, has increasingly led to growing pains [11]. Due to this trust, route discovery can fall prey to just about any router (or an entity masquerading as a router) that provides false information regarding the best path to network destinations. This would be an effective way of intercepting, blocking, or modifying traffic to that destination. Many of these protocols involve the router trusting information it has received from external sources. These kinds of issues have necessitated a constant evaluation between the balance of trust and performance in Internet protocols and practices.

For example, in April of 1997, a small ISP’s routers propagated information incorrectly indicating that it had the best route to most of the Internet. Internet routing was disrupted for several hours as upstream routers trusted this erroneous assertion and pushed overwhelming amounts of data through the small, unprepared ISP. Although this problem was a fluke caused by a human misconfiguration, it serves as an effective example of wide scale disruptions in the Internet being caused by a local event [11].

These technologies, such as DNS, routers, and other network infrastructures, can be exploited because, in general, access to these subsystems is not limited within data networks. Data network security could benefit greatly from the separation of these critical systems from the general data path as the SS7 network did for the TN. Although such a separation may not be practical, at the very least strong authentication and access authorization mechanisms should be in place and functional.

3.2.2.2.4 Human Factor

The router misconfiguration presented in the previous section brings discussion to yet another large contributor to the overall security of data systems. Networks are a tool, and like most tools they serve to amplify the abilities of the humans they assist. But as with any tool, the actions of the user are amplified without discretion toward the good or bad consequences of the deed. Whether it is unintentional mistakes made by those that use and manage the system, or the calculated efforts of a mischief-maker, undesirable behavior routinely makes its way into the operations of data networks.

Attackers can prey upon the fact that there are still human factors involved in the process. An operator sitting in a network operations center at a telecommunications company must rely upon his own interpretation of the situation to decide what should be done and to determine what the effects of his actions will be without direct knowledge of either. In these circumstances, even the most scrutinized decisions can have unexpected results [5].

Likewise, an attacker can glean a remarkable amount of useful information directly from the individuals involved with networks. So-called social engineering is an underappreciated vulnerability. There are repeated reports in the literature of extremely disturbing cases where researchers are easily able to socially engineer information from their targets. Such as evidenced in a 2005 United States Treasury department report that indicated that internal auditors were able to convince over a third of the contacted Internal Revenue Service (IRS) employees and managers to disclose their network login information.

Internal auditors contacted 100 individuals employed by the IRS and portrayed themselves as personnel from the IT helpdesk trying to remedy a network problem. They requested that the employees provide their network login username and temporarily change their password to one they suggested. A stunning 35 of the individuals contacted complied with the requests. In follow-up interviews, those that had provided the information gave a variety of reasons for disclosing their passwords in violation of IRS rules. Some were not aware of the hacking technique and wished to be as helpful as possible to the computer technicians; the thought of foul play never entered their minds. Others went as far as to attempt looking up the caller's name in the IRS global employee directory, but gave the information anyway, while others initially hesitated but received approval from their managers to cooperate [20].

In the case of the IRS, the social engineer could have easily used the information obtained to access taxpayer information or to otherwise affect the IRS data network [20]. In a broader sense, social engineering allows an attacker to gain access reserved for authorized users. Resolving this vulnerability depends upon a broad awareness of the problem. All users of a network, particularly users with significant access, should be trained to recognize and respond to social engineering attempts. Timely reporting of a suspected incident can be very useful as an indication of an impending attack.

Network security is also vulnerable to changing human alliances. Today's system administrator can easily become tomorrow's disgruntled employee. For this reason it is desirable to implement role-based security. Each user is given only the authorizations necessary to perform his job. If his role changes, so does his access. This practice, which is highly advisable, proves useful in mitigating other human related risks as well, since it allows some limits on how much damage can be done by a user.

Unfortunately, much of the existing telecommunication equipment used today does not offer the level of access control granularity necessary for role-based security. Furthermore, individually configuring each element is cumbersome in large networks. Because of this difficulty, role-based security is often implemented in a network management tool. This tool adds an interface between users and the equipment with which they are working. Equipment access information is kept a tightly guarded secret and is provided only to the network management tool along with a list of who is authorized to do what. Users perform all actions through the tool, which confirms the user's credentials and then performs the requested action only if the user is authorized to do so [21].

3.3 Network Convergence

Telecommunications infrastructure has developed into massive twin networks that carry data and voice traffic respectively. Originally an offshoot of the voice network, data networks have grown into their own right. Customer premises nationwide have two ports: one for voice service and one for data, but this configuration is changing. The redundancy of building and maintaining both these networks is pushing many in the industry to consider consolidation. Convergence of all traffic into a unified communications network is indeed an attractive concept.

When deciding how to consolidate these networks, the inherent versatility of data networks to transport a wide range of services makes it the initial obvious choice. This consideration, coupled with the notoriously high costs associated with the development and maintenance of telephone networks, has brought many proponents to call for system consolidation to be built upon the cheaper and more accessible data networks employing IP technology. Indeed there is already a group of IP telephony services known collectively as Voice Over Internet Protocol (VOIP) which aim to provide for a unified system.

Overall, network convergence has advantages beyond mere financial incentives. It allows industry efforts to be more focused and will improve both the security and functionality of the resulting merged network in the long run. But the path to a unified communication network is not without its own technological difficulties and security challenges.

3.3.1 Difficulties

The public switched telephone network (PSTN) and Internet share many commonalities with each other. They are a collaborative body involving large numbers of subsystems operated by many different organizations. Because these systems are collaborations, there exist many interfaces at the boundaries of subsystems, and these interfaces greatly increase the complexity of the system. Indeed, data and telephony networks have never been entirely separate entities; the telephone system has long depended upon data networks for control and management, whereas a large amount of data traffic flows over the leased lines of telephone companies [5].

As briefly discussed already, IP networks work in a fundamentally different communications paradigm than those of telephony. Voice conversations have benefitted from the advantages provided by a circuit-switched dedicated communications link. As voice services are moving towards packet switched IP implementations, they are now faced with the challenges of varying and unpredictable packet arrival that traditional telephony never had to take into account. In a best effort communications protocol such as IP, the reliability that customers have come to expect can be challenged by varying network conditions such as congestion.

Migration to a unified communications network must also take into consideration the significant investments that have been made in traditional telephony. The extensive infrastructure that telecommunications providers, along with a multitude of private companies, own and operate necessitates continuing support for many years to come and must be included in a new consolidated network. New IP telephony therefore must

coexist seamlessly with the existing systems. This is crucial for it to enjoy widespread adoption and to prevent the further splintering of communication networks.

Adding to the various difficulties in network convergence is the regulatory environment currently in place for telephony networks. The unique history of telephony services has given rise to a system heavily managed by government regulations. These regulations include very specific and sometimes costly requirements on telephony providers, such as emergency (9-1-1) service access and law enforcement wiretap provisions, etc. The emergence of VOIP services traveling over the public Internet has operated largely outside of these regulations, causing traditional telephony providers to cry “foul” as cheaper alternatives become available through the Internet.

New technologies often bring with them considerations that confound existing laws, and it takes time for legislation to be reworked to include them. VOIP’s arrival in the telephony industry calls for such legislative change, and it is understandable that regulation takes its time to assess the considerations that are unique to VOIP. However, since VOIP itself is still being developed, the sooner that regulators put in place clear requirements and expectations, the better. Incorporation of such guidelines early in VOIP development is much easier than spending additional efforts trying to add it later. Furthermore, regulators must be careful that the guidelines they provide do not stifle emerging VOIP efforts.

3.3.2 Security Considerations

Government regulation also plays a large role in the security considerations of a converged network. Regulators have been placing increasingly more privacy and security responsibilities on the shoulders of the networks that carry sensitive data. Comprehensive legislation such as the Health Insurance Portability and Accountability Act (HIPAA) regulating healthcare related data, the Gramm-Leach-Bliley Act (GLBA) governing financial services industries, and Title 21 Code of Federal Regulations (CFR) Part 11 mandating requirements for electronic record security all place stringent legal responsibilities on any networks that carry these types of data. The expectations mandated in these articles of legislation cannot be satisfied by the rudimentary security capabilities of an out-of-the-box network. Sophisticated management tools and practices must be employed. System administrators must prove not only that their networks are configured securely in the first place, but that the configuration has not been altered in a way that would allow sensitive data to be compromised [21].

Unified communications networks will find that privacy is an important and tricky issue for which legal considerations cannot be neglected. Legislative efforts to improve the security on data networks can be expected to continue. This trend has led many in the industry to warn that IT-based industries are likely the next group to be targeted in liability lawsuits as tobacco litigation winds down. As more liability comes to rest on telecommunication and IT professionals it will be essential that they can testify that they have made appropriate security decisions and exercised due-diligence in both voice and data communication to [22]:

- guarantee the integrity of customer transactions,
- anticipate and address new threats, and

- ensure compliance to privacy and security laws.

Additional security considerations come from the need to develop SCADA-like functionality for a unified communications system. Even the best secured telecom services are wide open to threats posed by their management systems. Centralized or inadequately protected management systems act as vulnerability multipliers. Protection of these systems is critical. Many telephony providers would likely be uncomfortable employing the in-band control and monitoring often found in IP networks. Therefore, as the networks are consolidated, system designers will need to find some way to reconcile the differences between the two networks' current methods of control that will be found acceptable to both parties. This security concern provides an opportunity to develop a system that improves upon both networks' current implementation.

Network convergence is a good idea. It will, however, take considerable effort to develop an effective and timely roadmap. For further exploration of topics related to traditional telephony and VOIP see Ragsdale [8].

4.0 Recommendations

Overall, when it comes to control system security, the national telecommunication infrastructure is leaps and bounds ahead of other critical infrastructure providers, such as natural gas, water, and electricity. But the security measures that they use definitely leave room for improvement. This section will focus on the various security tools, services, practices, and research that are recommended for all telecommunications companies to consider.

4.1 Security Tools

Security often involves a cocktail of many different elements working together to tighten a net of protection around a system. Telecommunications providers seeking to secure their monitoring and control abilities have a variety of mechanisms at their disposal from which they can pick and choose to create an appropriate security plan for their system. These elements work together to form a gestalt system; that is, a system whose sum is greater than its parts. These basic mechanisms and technologies form the foundations of security services and are discussed by Rosenblit [2]. Some common security tools and capabilities include hashing, encryption, digital signatures, and certificates.

4.1.1 Hashing

Hashing takes an input of arbitrary length and produces a fixed-length, short message digest. Hashing is useful for detecting transmission errors and to some extent ensures that the transmitted data has not been altered. But it is more commonly utilized as the basis for other security measures and is rarely used as a standalone security mechanism. A hashing function is considered a secure, one-way function if it satisfies the following conditions [2]:

- **Secure Property:** Any change to the initial bit string changes the message digest completely.
- **Second Preimage Resistance Property:** Even when all aspects (hashing function, message and digest) are known, it is practically impossible to construct another message with the same digest.
- **One-Way Property:** It is practically impossible to derive the original message from its digest, even if the hashing function is known.
- **Collision Free:** It is computationally infeasible to find any pair of messages that have the same hash value.

No hashing application has been proven to meet all of these requirements, but there are many that have not been proven insecure either. Because of this, the variety of hashing protocols that are currently popular, such as Message-Digest algorithm 5 (MD5) or the Secure Hashing Algorithm (SHA), could abruptly become insecure in light of cutting edge research. Indeed researchers have already shown some collision and preimage weaknesses in MD5. But up until now, these algorithms have proven sufficiently secure for most uses [2].

4.1.2 Encryption

Encryption is the term used to describe the process of obscuring or encoding a message so that it can only be read after it is decoded using some form of a “key.” The key, which is often a number or some other unknown property, is provided to authorize users to decipher the message. There are two types of encryption: symmetric and asymmetric [2], of which asymmetric encryption is more recent.

Symmetric encryption uses the same key to encrypt information as it does to decrypt the information. This form of encryption usually uses a publicly known algorithm for encryption and, as such, symmetric encryption has absolute dependence on the key remaining a secret. A popular implementation of symmetric encryption is found in the Data Encryption Standard (DES), which is based on the Data Encryption Algorithm (DEA) [2].

Symmetric key encryption is susceptible to brute force attacks where an attacker attempts to decode a message by trying all possible keys. The DES uses a numerical key composed of 56 random bits. Keys of this size have over 72 trillion (72,000,000,000,000) possible unique keys. This is a staggering amount of possibilities, and yet there are systems available that are able to correctly decode DES messages in a matter of hours [24]. As computation power, availability, and strength increase, so does the need for longer keys. In general, as the number of bits in the key increases, the difficulty to compromise the encryption increases exponentially [2].

Complications in the use of symmetric encryption algorithms arise from its dependence upon the use of a secret key. The distribution of this key must be done in a secure manner to maintain secrecy. Secure distribution of the key requires the very service that encryption is in place to provide, which means the key must be transmitted by some other protected method (e.g. hand-carried).

Asymmetric encryption addresses the difficulty of key distribution that is prevalent with the use of symmetric encryption. Asymmetric encryption uses one key to encrypt the data, called the public key, and another, a private key, to decrypt it. This method works well because the public key can be freely distributed to anyone wishing secure communications. The private key is kept as a closely guarded secret by its owner. The message to be sent is encrypted using the public key of the intended receiver, and once encrypted, the message can only be decrypted with the corresponding private key. Since it doesn't matter who obtains the public key, it can be transmitted in the clear on the network [2].

Removing the obstacle of key distribution has brought encryption services into the mainstream, making it a much more accessible technology. Because of this availability, it has enjoyed widespread adoption on networks. Popular and available algorithms such as the pervasive Rivest-Shamir-Adelman's (RSA) algorithm have allowed secure communications in applications varying from e-commerce to network management [2]. Telecommunications providers should use encryption whenever possible to protect both the content and the control data that passes through their networks.

4.1.3 Digital Signatures

The development of electronic communications has given rise to the need for a method to verify the sender of a message. To meet this need, a clever application of asymmetric encryption is used. Asymmetric encryption algorithms such as RSA have the property that encryption and decryption are interchangeable. In other words, just as a message encrypted with the public key can only be decrypted with the private key, so too can messages encrypted with the private key only be decrypted with the public key. This property can be used to digitally sign a message as shown in the following example.

Alice is using the asymmetric encryption algorithm RSA. As such, she has a private key and public key. The public key has been distributed to Bob to whom she wishes to send a digitally signed message. Alice sends a message to Bob. She then takes the message she wishes to sign and uses her private key to encrypt either the message in its entirety, or a message digest formed using a secure hashing algorithm. Message digests are often used to save computational or network resources, and assuming a secure hashing protocol is used, security is not sacrificed. Alice then sends the encrypted message, known as a digital signature, to Bob who in turn decrypts the transmission using Alice's public key. If the decrypted text agrees with the message sent by Alice, then Bob can be assured that only someone with Alice's private key could have generated the digital signature [25].

Digital signatures are valuable in telecommunications monitoring and control networks because they can be used in providing assurance for network equipment that commands are originating from an authorized network controller. It also finds important uses in a business context. Telecommunications providers, even competing entities such as ILECs and CLECs, are required to work cooperatively in the everyday business of keeping the telecommunications network running. This cooperation often requires them to make requests or otherwise enter into business agreements that are greatly aided by the ability to digitally sign communications. Such digital signatures mimic their real-world paper signature counterpart in their ability to hold the senders accountable for their actions and agreements. If necessary, they can even be used as evidence for a third party, such as a court of law [2].

4.1.4 Certificates

Both asymmetric encryption and its use in digital signatures suffer from a subtle but noteworthy weakness. They rely on the accurate correlation between a public key and its corresponding private key owner. That is, if Bob has a public key that he associates with Alice, how can he be sure that he has received Alice's actual public key. Asymmetric encryption can fall prey to man-in-the-middle attacks, where a third party, say Carly, is able to sit in-between communications linking Alice to Bob. Carly can potentially trick Bob into thinking a public key belongs to Alice when in fact she has supplied a public key for which she has the corresponding private key. Carly could then intercept communications between the two decoding message from Bob with her private key and then re-encode them with Alice's real public key to be sent on to Alice. This could occur without either realizing that their messages were being intercepted.

To combat this kind of attack, a public key infrastructure (PKI) has been developed. The PKI allows users to have a trusted third party certificate authority (CA) issue a digital

certificate which contains their public key and packages their credentials such as name, organization, etc. along with it. This certificate is digitally signed by the CA and is used by Bob to verify that he has the proper public key for Alice. The savvy reader would notice that such a system would require that Bob know for certain that he has the correct public key for the CA. Indeed, Bob must have established some basis for trusting a certificate coming from a CA. This can be accomplished ahead of time, or can be obtained through some reliable medium [26]. Large entities such as those often found in telecommunications can even choose to setup their own CA to provide assurances for public key certificates.

4.2 Security Services

Using these tools discussed in Section 4.1, telecommunication providers can design a system which offers services that are resilient and resistant to attack. This section focuses on a core set of security services that all system designers should consider when designing their own security plans [2].

4.2.1 Connection Access Control

Connection access control acts as the first line of defense. Usually implemented by specialized equipment placed at interconnect boundaries on the network, connection access control devices monitor all traffic passing through these boundaries. Implemented in Closed User Groups (CUGs) over X.25 networks and firewalls in IP systems, any traffic that does not fit the profile of allowed network communications is discarded. Connection access control compares the incoming traffic to internal configurations outlining the source addresses that are allowed to communicate across the boundaries and the type of services that the network should allow.

Connection access control won't typically prevent a determined intruder from finding a way into the network. But it can usually remove a large amount of attacks from less sophisticated attackers and can prevent the network from even having to deal with the additional unwanted traffic that would otherwise flood the system [2]. Telecommunication implementations can benefit most from placing these types of services at the interconnections between cooperating but separate entities. Connection access control is especially important to block out the pervasive vulnerability probes that are experienced by any systems attached to the Internet.

4.2.2 Peer Entity Authentication

If an attacker is able to bypass connection access control, his next obstacle will likely be defeating the peer entity authentication that is in place. Peer authentication is the process that is used to initially set up a communications relationship between a client and a server. The network operations center (NOC) authenticates itself to network elements when beginning a configuration setup. During this authentication, the operations center will provide credentials that establish the capabilities that should be granted to it for the remainder of the session. Peer entity authentication is a prime candidate for such services as the digital signatures mechanism described above [2].

4.2.3 Data Origin Authentication

Authentication should not stop after the initial connection is established. Some form of continuing authentication service should be in place to prevent an attacker from hijacking a connection after it has been set up. This authentication can be a continuous or periodic process that verifies that the communication is indeed coming from the purported sender [2]. Again, such authentication can make use of mechanisms such as those described in the digital signatures discussion.

4.2.4 Integrity

Network elements should not rely merely on assurances that the sender of data is legitimate, but should also assure that the data has not been modified during transport. The integrity of a message can be verified using a hashing algorithm as discussed in Section 4.1.1. Integrity should take into account missing messages as well as the modification of message contents [2].

4.2.5 Confidentiality

The aforementioned services help to prevent active attacks. Sometimes passive attacks, during which an attacker merely observes the network, can also be dangerous since telecommunications systems often transport sensitive data across their communication lines. Effective encryption works well to protect the data from eavesdropping and as such should be used whenever possible. Trickier still are situations where merely the presence or absence of traffic can be useful to an intruder, even if the transmissions are encrypted. An example of this situation could be an application where the presence of traffic indicates a corresponding presence of individuals or the indication that certain events are taking place. In instances where this is a concern, traffic can be shaped to always be present, even when necessary communication is not taking place [2].

4.2.6 Non-repudiation

In business environments such as those often found in telecommunications management systems, it is important that services are set up so that an entity cannot falsely deny it has sent a message. For example, if a CLEC puts in an electronic request for 1,000 circuits, mechanisms must exist to prevent the CLEC from later claiming that it placed no such order, or that the order was for only 10 circuits. Such a service is known as non-repudiation. With a non-repudiation service in place, the ILEC will have the electronic equivalent of a signed contract proving the existence and authenticity of the original service request. As the name would imply, digital signatures are very effective at providing this service, certifying both the content and the sender of a message [2].

4.2.7 Security Alarm

Telecommunication systems should also be equipped with a service that is able to monitor the network for suspicious activity. For example, it is advisable to continuously probe the network for unauthorized changes. This can be accomplished by commonly (along the order of minutes) reviewing log records for evidence of an administrative login. Such logins are required for a configuration change to take place within the

equipment. When a login is found, then the complete configuration data can be compared to the configuration data backup that is stored elsewhere [21]. Other alarms can be triggered by monitoring traffic patterns and communication transactions for irregular activities.

If an intrusion is detected, then security alarms should be generated notifying monitoring agents, such as a NOC or system administrators, of the situation so that they can respond. Additionally, the alarms should be sent to connected systems, warning them of the existence of an irregularity and alerting them to possible issues that could arise from their interconnection. Since a compromised system can hardly be relied upon to produce alarms without fail, connected systems should also monitor their connections for irregular activity occurring over the connection. It is also wise for systems either receiving or generating a security alarm to take precautions that automatically react to the situation, entering “panic modes” that actively address the condition and limit its impact as much as possible [2].

4.2.8 Security Audit Trail

Finally, all telecommunication systems should provide extensive logs to allow for forensic analysis of an attack. While not an active defense against attacks, the existence of the logs can be invaluable in tracking down both the culprit and the vulnerability that was exploited. This knowledge can be used to strengthen the system against future attacks against the identical vulnerability. Additionally, the mere existence of a security audit trail can act as a particularly useful deterrence against attacks and provides general accountability for all actions performed on the network [2]. It is, therefore, essential that the logs themselves be guarded by security measures making them difficult to alter. Otherwise, they cannot be trusted to provide an accurate source of information in the aftermath of an attack.

4.3 Utility Security Recommendations

While telecommunication networks have a monitoring and control system that surpasses that of other utility companies in areas of security and sophistication, there are many commonalities between their needs and security issues. As such, the general recommendations relevant for infrastructures such as water and natural gas suppliers are equally valid for telecommunication networks. For a detailed study of these recommendations, which include considerations on topics varying from control center locations to government-based security incentives, see Ragsdale and Grim [4].

4.4 Research Areas

The ever evolving nature of the networks used in telecommunication systems means that security systems must continuously adapt and innovate as well. This innovation does not come without a focused effort on the part of research and development teams in both industry and academia. This section explores the various research topics that should be investigated to better equip the nation’s telecommunications providers with networks that are secure.

The telecommunications industry is notoriously tight-lipped about security, which is an inherent security policy itself. Therefore, a portion of the problem in securing telecommunications networks springs from the fact that those charged with protecting telecommunication networks suffer from an insufficient understanding of their potential attackers. Industry experts point to the fact that an adequate categorization of a threat model does not exist. The current level of research in this area is clearly minimal and many organizations are understandably reluctant to discuss known vulnerabilities. More importantly, these organizations are even less willing to discuss the attacks that they have experienced [9], which was a primary difficulty encountered during the research phase of preparing this report.

Research should be conducted to more clearly define who launches specific types of attacks. This knowledge could prove extremely helpful to security professionals, allowing them to more effectively and efficiently tailor the security systems around these considerations [3]. Furthermore, it can be assumed that a majority of attacks are never detected and that these are perhaps the more important types of attacks in need of additional scrutiny. However, it is in the interest of the industry as a whole to perform, facilitate, and share the results of such research.

Another important area for research is improvement in one of the primary sources of vulnerabilities in these systems: software bugs. Fortunately, the wave of high-profile security problems that have caused noticeable disruptions to the Internet has led to a renewed commitment and focus by software developers to produce secure code. While the complete elimination of these bugs is likely impossible, it must continue to be the focus of intense effort. Research in this area can teach software designers effective methods for writing good software and developing secure systems from insecure components, similar to how reliable computer systems can be built from unreliable electronic parts [3].

The industry also could benefit greatly from the development of a formal framework for use in assessing the strength of a security system. Just as an engineer can evaluate how much weight a bridge can hold, so too should there be a method for performing qualitative analysis on system security [3]. Such a benchmark would be an extremely effective tool for evaluating current systems, assessing the impact of changes, and developing new security plans.

Other possible topics for research include the expansion of studies exploring the new challenges, vulnerabilities and security concerns brought on by the emergence of VoIP and other network convergence technologies. Industry is also encouraged to continue seeking better ways to collect, aggregate, mine, and dispense information on developing threats. Hand in hand with this pooling of threat information, it is important that we find a way to combat the denial and complacency of telecommunication service providers who refuse to believe that attacks can happen to them [22]. It is essential that all telecommunications providers realize that as their data networks become more and more prevalent, and as their systems become ever more globally interlocked, that these are the digital frontlines of a new borderless battleground. System administration is an atypical research topic, but quite likely stands to benefit the most from further exploration. Much can be done to ease the load on a profession that is all too often over-stressed and under-appreciated [3].

Government can help motivate research by continuing its support of telecommunications security research. These research investments should include [22]:

- the establishment of mechanisms to reach community consensus about telecommunications security requirements,
- the documentation of such requirements in common ways such as provided by standards like the International Organization for Standardization's (ISO) Common Criteria,
- the establishment of security incentives like government "venture capital" for rapid prototyping,
- the strengthening of deterrents to malicious attacks on the telecommunications infrastructure,
- the expansion of the number of students and faculty pursuing telecom security, and
- the continuation of efforts to expand information sharing.

Most important, however, is the fact that while research is indeed needed, there is a great body of research not yet implemented in practice. For example, there is far more cryptographic science present than there are network protocols that use them. This is likely due to a lack of consideration for the human factors involved in the adoption of new security technology. There is evidence that suggests that many security technologies are not employed because they are too difficult or cumbersome to use. Considerable effort should be given to bringing new technologies out of the lab and into practice. But even beyond usability issues, a security theory that has been realized in a form user-friendly enough to be widely deployed is still up against an overwhelming case of operational inertia. In order for new technologies to be embraced and adopted, there has to be an undeniable incentive for telecommunications companies to do so [3].

5.0 CONCLUSION

The convenience and ubiquity of modern communications has precipitated the advent of the information age. It contracts distances and blurs borders. The connectivity enables humans to interact in ways never before possible or imagined. But our reliance on these new capabilities has left us vulnerable if they were to suddenly cease operation. A large scale system outage would have colossal financial and emotional impact on the nation. These impacts could be further amplified in conjunction with a separate physical attack. These are precisely the criteria sought by terrorists planning strikes. This threat cannot be ignored and calls for a focused and concerted effort to prevent such an occurrence.

Securing a network with the size, complexity, and accessibility found in telecommunication networks is by no means a simple matter. This report has endeavored to provide insight for those considering the challenges that such a task involves. Fortunately, the security problems facing the telecommunications industry are similar, if not identical, to those facing the computer and networking industries. Telecom will be able to benefit tremendously from the constant improvements in security and security procedures that are developed for computers and networks, but it is essential that they be evaluated in the context of telecommunication networks.

Care must be given to tailor the security plan for a given network to the specific needs of that system, and because of this it is important to constantly appraise the security and potential threats in a network. This is particularly crucial as voice and data networks continue to converge, bringing new challenges and unexpected security issues. Developing legal requirements also present a liability that necessitates a commitment to security. Fortunately, telecommunications networks have demonstrated a history of considering security that far exceeds other infrastructure entities, and this puts them well ahead of the game.

6.0 LIST OF REFERENCES

- [1] Public Broadcasting Service, “More about Bell,” American Experience – The Telephone. <http://www.pbs.org/wgbh/amex/telephone/peopleevents/mabell.html> (Mar. 10, 2005).
- [2] M. Rozenblit, *Security for Telecommunications Network Management*, New York, NY: IEEE Press 2000.
- [3] S. Bellovin, “House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development: Hearing on ‘Cybersecurity—Getting it Right’,” July 22, 2003. <http://hsc.house.gov/files/testimony%20bellovin.doc> (March 1, 2005).
- [4] G. Ragsdale and E. Grim, “Cyber Vulnerabilities within the National Infrastructure’s Supervisory Control and Data Acquisition Systems: Cyber Vulnerabilities in Energy Infrastructure’s Supervisory Control and Data Acquisition Systems. Draft NCS TIB, September 2004.
- [5] F. Schneider et al., “Critical Infrastructures You Can Trust: Where Telecommunications Fits,” 26th Annual Telecommunications Policy Research Conference. www.tprc.org/abstracts98/schneider.pdf (March 4, 2005).
- [6] “Phreaking,” Wikipedia Entry. <http://en.wikipedia.org/wiki/Phreaking> (April 7, 2005).
- [7] Performance Technologies, “Tutorial on Signaling System 7 (SS&),” www.pt.com/tutorials/ss7_tutorial_091503v2.pdf (March 14, 2005).
- [8] G. Ragsdale et al., “The Convergence of Signaling System 7 and Voice-over-IP,” NCS TIB 00-8, September 2000.
- [9] M. Raschke, “Telecommunications Network Operating Center Meeting and Tour Notes – November 9, 2004,” Southwest Research Institute, Project No. 10.10403, October 15, 2004.
- [10] B. Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, New York, NY: Bantam Books, 1992.
- [11] Committee on Information Systems Trustworthiness, *Trust in Cyberspace*, National Research Council, Washington D.C.: National Academy Press, 1999.
- [12] C. Hing, “A Telecommunications Access Control Policy,” SANS Institute. http://www.giac.org/certified_professionals/practicals/gsec/3296.php (March 3, 2005).
- [13] “Signalling System 7,” Wikipedia Entry. <http://en.wikipedia.org/wiki/SS7> (April 7, 2005).

- [14] National Research Council, Committee on Science and Technology for Countering Terrorism, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, The National Academies Press, Washington DC, 2002.
- [15] N. Borisov, "AT&T Failure of January 15, 1990." <http://www.cs.berkeley.edu/~nikitab/courses/cs294-8/hw1.html> (July 20, 2004).
- [16] "Competitive Local Exchange Carrier," Wikipedia Entry. http://en.wikipedia.org/wiki/Competitive_local_exchange_carrier (April 7, 2005).
- [17] "An Introductory Overview of SNMP," Diversified Data Resources, Inc., 1999. http://www-t.zhwin.ch/it/ksy/Block07/SNMP_Overview.pdf (March 21, 2005).
- [18] S. Gorman et al., "Least Effort Strategies for Cybersecurity," School of Public Policy, George Mason University. <http://arxiv.org/ftp/cond-mat/papers/0306/0306002.pdf> (March 3, 2005).
- [19] "Have hackers recruited your PC?," BBC News, March 17, 2005. <http://news.bbc.co.uk/2/hi/technology/4354109.stm> (March 17, 2005).
- [20] M. Dalrymple, "Auditors Find IRS Workers Prone to Hackers," Associated Press, March 16, 2005. <http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2005/03/16/national/w162055S07.DTL> (March 17, 2005).
- [21] D. Jones, "The Definitive Guide To Enterprise Network Configuration and Change Management," Voyence/realtimepublishers.com, 2004. http://library.telecommagazine.com/data/detail?id=1073659113_535&type=RES&x=1331944679 (March 7, 2005).
- [22] P. Brusil et al., "Critical Telecommunications Infrastructures Demand Security," *Journal of Network and Systems Management*, Vol. 9, No. 1, 2001.
- [23] "Competitive Local Exchange Carrier," Wikipedia Entry. http://en.wikipedia.org/wiki/Data_Encryption_Standard (April 7, 2005).
- [24] "Data Encryption Standard," Wikipedia Entry. http://en.wikipedia.org/wiki/Data_Encryption_Standard (April 7, 2005).
- [25] "Digital Signature," Wikipedia Entry. http://en.wikipedia.org/wiki/Digital_signatures (April 7, 2005).
- [26] "Certificate Authority," Wikipedia Entry. http://en.wikipedia.org/wiki/Certificate_Authority (April 7, 2005).