USING THE TECHNIQUES OF A SECURITY ASSESSMENT TO GUIDE TECHNOLOGY DEVELOPMENT IN EDUCATION

A Thesis
Submitted to the Faculty of
Purdue University

by Stephanie Ann Miller
CERIAS TR 1999-12

Center for Education and Research in
Information Assurance and Security,
Purdue University
December 1999

USING THE TECHNIQUES OF A SECURITY ASSESSMENT TO GUIDE TECHNOLOGY DEVELOPMENT IN EDUCATION

A Thesis

Submitted to the Faculty

of

Purdue University

by

Stephanie Ann Miller

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

December 1999

ACKNOWLEDGMENTS

I wish to express my gratitude to the many people who have been involved in my growth and development both personally and professionally.

I thank my family for their continued support through each major juncture of my life. They have taught me how to learn and grow from every adventure I pursue. From them I derive my strengths, motivations, and dreams.

I thank Saleem Chaudhary, that special someone who entered my life when I needed him the most. He has been there through all of the triumphs and struggles of graduate school and supported me at each step of the way.

I thank Steve Hare for his time, guidance, ideas, and support through the IASEP project. I also thank the entire IASEP team for their contributions, ideas, and willingness to learn as we have all worked together to promote greater security focus for education projects.

I thank all of the guys and gals of CERIAS as well as my entering class at Purdue. Somehow we all did survive our first year of graduate school here, and the resulting friendships have made it all worth everything. Thank you all for keeping me sane and for teaching me so much about computer science and about life!

Finally, I thank Professor Gene Spafford, my advisor, for his amazing guidance during this experience. He has been a wonderful source of inspiration academically, professionally, and personally. His spirit and dedication has created an exciting envi-

ronment for research and learning in information security that the entire community can share. I am thrilled to have been a part of the CERIAS experience and to have worked with such a dynamic personality as "Spaf".

TABLE OF CONTENTS

Page

Page

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Miller, Stephanie Ann. M.S., Purdue University, December, 1999. Using the Techniques of a Security Assessment to Guide Technology Development in Education. Major Professor: Eugene H. Spafford.

The goal of this thesis is to structure and present the complete process involved in implementing a security assessment. Our objective is to capture the essence of a successful security assessment. We will not only document best practices, but will outline such an assessment for a project underway in the School of Education and funded by the State of Indiana. That project promotes improved evaluation of special needs students.

The result of this work has been a concrete example of a security assessment methodology as well as a documented process that can be utilized as a template in future assessments. The assessment techniques we recommend in this thesis include project examination, threat analysis, modeling of data flows, and development of a security architecture.

Other topics we will address throughout the document include fundamental security precautions, such as ensuring confidentiality, integrity, and availability.

We will offer insight on dissemination of results to project sponsors and users to encourage the effectiveness of the deliverables produced during a security assessment.

1. INTRODUCTION

Over the past several years there has been increasing realization of the need to protect information assets. While the definition of risk means different things to different organizations, the willingness to mitigate that risk is evident among top executives.

In a 1997 survey (see [21]) over 74% of senior executives responded that their information security risks had increased over the last two years. That same survey revealed that 82% of the respondents recognized the importance of information security and 75% indicated that their use of the Internet for business would expand if the risks inherent to that medium were reduced. This survey was supported by other studies who express the growing requirements for information security protection in most areas of technological development. Figure 1.1 provides further evidence surrounding the severity of the problem in protecting information assets. The attacks measured in that figure are real concerns for any type of computer technology usage.

The purpose of this document is to share experiences in the security assessment project that was undertaken throughout the 1999 calendar year with a technology development team associated with the School of Education (SOE) at Purdue University. This report documents how we actively pursued the security concerns that the team had already realized for their technology project. In doing so we were able to

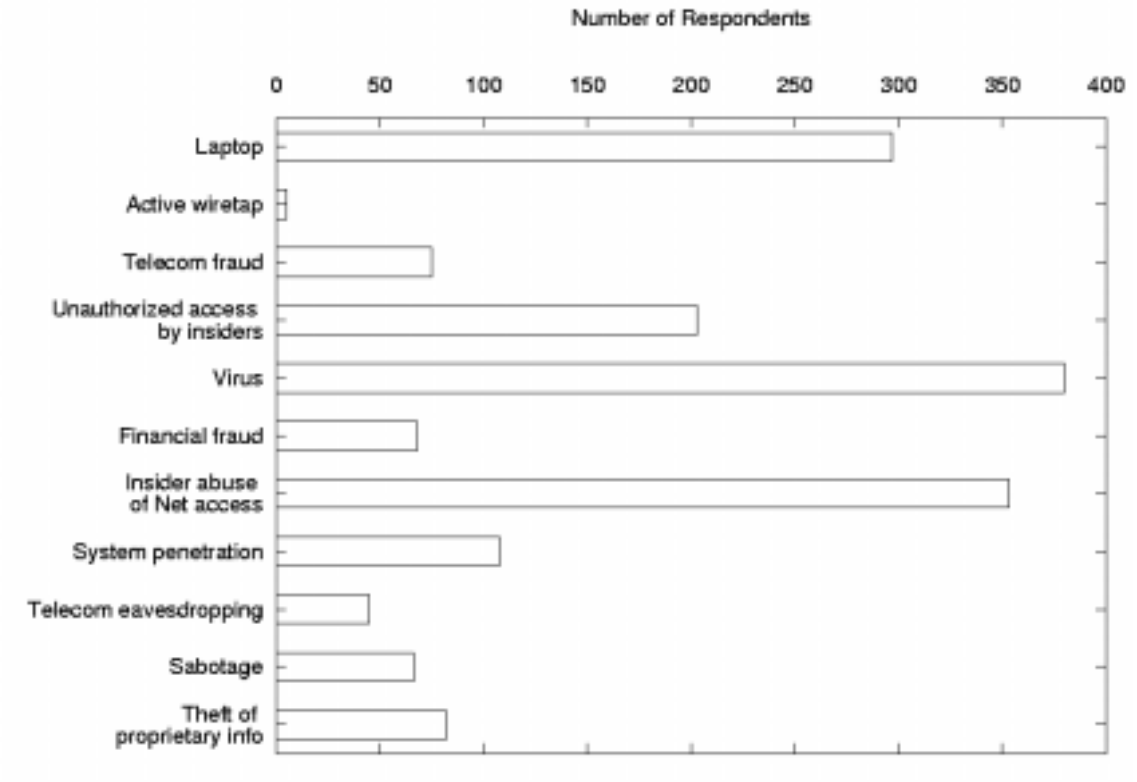

Figure 1.1. Types of Attack Detected Within 12 Months (Source: CSI/FBI Computer Crime Survey 1998)

introduce additional security topics affecting the project. We worked closely with the project team to understand their needs, their backgrounds, and their expectations for the security piece of that initiative. The content of this document will give an overview of the interaction between CERIAS (Center for Education and Research in Information Assurance and Security) and the SOE project team, consisting of representatives from Purdue University and the Indiana Department of Education. We

will highlight the results that were accomplished during the course of the security assessment.

The security assessment we performed was realized through a series of steps as presented in figure 1.2. The initial phase of the assessment was to learn as much about the project under evaluation as possible. Taking that knowledge, we formulated a data model for the technology as well as a threat analysis. We then used the recognized threats as a guide for overlaying the security architecture on the data model.

During each phase of the security assessment we worked closely with the project team to explain the security topics under consideration. In doing so we were able to educate the participants in the rationale for each security measure that was recommended.

In this thesis we will carefully document each of the assessment activities. Before delving into the specifics of our security assessment however, we will first provide background on the IASEP project and then provide background in general security awareness through the presentation of many widely used security concepts.

The contribution of this thesis is to capture the various elements of security into a cohesive package that is useful for many parties: the security assessment methodology. We engaged this structured methodology to ensure each dimension of the evaluated project was considered. We were able to bring together the various issues addressed in security through the presentation of a collection of deliverables that captured all of the essential security components that emerged during the assessment. We unveiled an interaction between assessment phases that provided a logical flow of input and output

through the process. This outcome closely relates to the Framework for Interpreting Risk in eCommerce Security (PFIRES)[11] effort. PFIRES promotes a life-cycle of activities to develop and execute a comprehensive security policy. We will show our assessment process to be a realistic approach for securing technology using the evaluation of the IASEP project as a case study.

1.1 Intended Audience

The anticipated audience for this thesis can be divided into two categories. We are writing with a focus on the needs of security professionals who have the need to conduct similar security assessments as a part of their work responsibilities. We hope to augment their efforts in this area by detailing the methodology we utilized and justifying the effectiveness of each step through the specific details of the IASEP security project. However, we do not want to ignore the project team who may be interested in independently adding security functionality to the technology they are developing. They may not have the resources or time-line for a dedicated security professional to understand the new technology they are building to conduct a thorough assessment of it. For that team we hope this document will provide basic guidelines that they can follow to address their need for improved security focus. Development teams cannot ignore the implications of threats on most technology-driven projects. By reviewing the details of the IASEP security assessment, insight can be gained about possible relationships and similarities to other projects where security should be considered.

1.2 Document Organization

The basic structure of this document is as follows. Section 2 will describe the project that was evaluated during our research. It will highlight the context for which our assessment methodology was created as well as point out future work to be completed for that project team as a follow-up to the results of this assessment. Section 3 gives an overview of security requirements and directs the discussion to the particular concerns for security in education programs. Section 4 offers the details for the actual assessment involving the IASEP project. That section dissects each critical stage of our process and documents the resulting deliverables. Section 5 reviews the methodology followed during the course of that assessment from a generic perspective and can serve as a guideline for future assessments. Section 6 summarizes the challenges and contributions of this thesis project. The appendices offer specific documents produced during the assessment as well as a brief tutorial on cryptography.

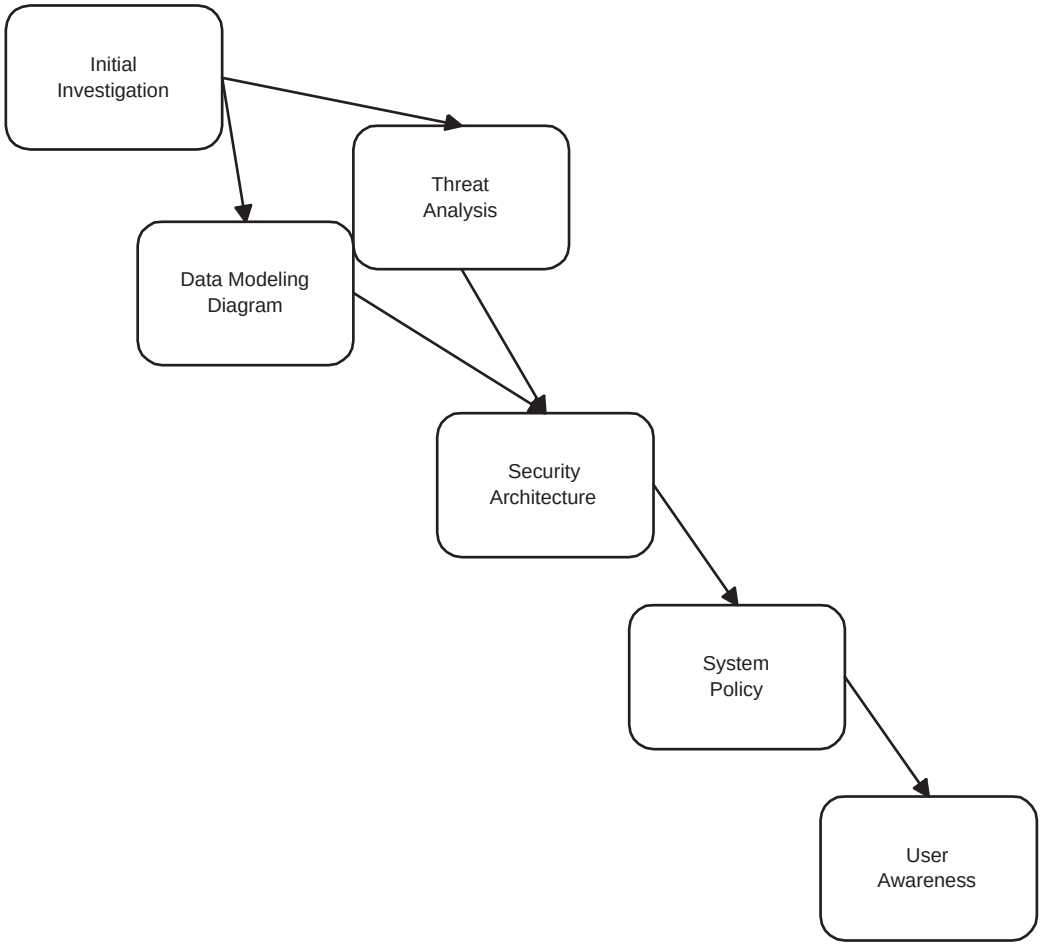

Figure 1.2. Model of the Security
Assessment Phases

2. SETTING THE STAGE: INTRODUCING IASEP

2.1 General Background

The name of the project under review is the Indiana Assessment System of Educational Proficiencies (IASEP). This is an assessment tool to be used by educators throughout the state of Indiana in the evaluation of students with special needs. The motivation for the development of such a tool stems from the difficulty in adapting traditional accountability methods that are sensitive to the educational progress of all students. The reauthorization of the Individuals with Disabilities Education Act (Public Law 105-17, 1997) required that these challenges be overcome.[12]

The researchers and developers in the School of Education at Purdue University underwent a software development process sponsored by the Indiana Department of Education (IDOE) whereby they created a new method of testing students the goes beyond the Federal mandate. This new way of generating test results, including video, audio, and electronic image materials, has been well received both by original stakeholders in the development of the tools as well as the teachers and parents directly involved in using the technology. Using more of the multimedia utilities widely available and used in other industry segments, the developers were able to create an assessment process that more accurately represents the true achievements of a student in multiple dimensions. For example, handwriting samples from the

student can be scanned and included in the assessment report along with an audio clip of that same student demonstrating improved vocabulary usage.

The multimedia documentation is compiled along with the teacher's rating of the student, which is collected with the new IASEP software piece, to provide an overall evaluation package. An assessment in this format allows for interactive feedback from teachers, parents, support staff, and other documentation systems. The IASEP assessment system is based upon the principles of effective instruction, which suggest that the evaluation of student progress should be multi-dimensional, continuous, and be responsive to individual growth.[12]

There are many challenges to overcome when introducing such a radically new way of testing student performance. The heavy emphasis on technology introduces many of the software and hardware maintenance, asset management, and user interface issues that many corporate institutions have been dealing with for some time. Compared to most other states in the United States, the IASEP student assessment system is advanced, and as such is a pioneer in solving many of these traditional and emerging challenges in the setting of a primary educational institution. The requirements for protecting the accumulated data, along with the individual it represents, have become a significant component of the overall development effort. Originally thought by the team to be a topic of minor significance, data security within the overall effort has become an integral piece for the success of the project.

Some of the most severe threats we uncovered in the threat analysis were issues related to confidentiality of student-specific information and system misuse. In par-

ticular we wanted to uncover many of the vulnerabilities in the system that arise from granting Internet access privileges to the users as well as to re-engineer poorly designed protections for the data of interest.

2.2 Brief History of IASEP

The IASEP research and development project began in November 1997. The mission of the team was to construct a tool for student assessment that utilized many forms of electronic documentation and a means of bundling this documentation into a single report that conveyed the student's progress. The rationale behind a computer-based data management system was to aid the teachers with a set of comprehensive documentation formats covering goals and measurements of educational progress of their pupils. The team set out to build a platform to be distributed to teachers throughout the state that would empower them to do that. The platform of choice was an Intel-based laptop system running the Windows 95/98 operating system. Custom software was written to perform the student evaluations. The utilities for collecting the multimedia documents were commercially available; many were bundled with the operating system itself. The integration of all of these technology pieces within the system went into pilot use at the start of the 1998-1999 school year.

Along with the technological developments that were being implemented, many user and administrative processes had to be defined to handle the testing data itself; from collection of data through transmission to district entities and eventually on to the State Department of Education for review. The procedures for manipulating the data had to be easy to use, yet would not lead to misuse of the system either

intentionally or unintentionally. All of the issues surrounding the collection, storage, and transmission of data were engaged as the security assessment got underway.

The security assessment portion of the project was initiated in late December 1998. By this time the IASEP project was already in pilot deployment and the system as a whole was in the hands of the end users. At this point most of the development of software and integration efforts had been completed and the integration of security requirements was left as a last step in the process.[14]

The time-line followed by the team is common of many projects. Unfortunately, adding security reviews as a wrap-up exercise adds an additional set of challenges to overcome in future roll-out of the security enhanced system. However, we discovered some benefit in letting the pilot users handle the system as the security analysis was taking place. Real data and user activities could be observed and that review could become part of the assessment input. Having actual scenarios arise during the pilot project gave us a means to prioritize the perceived threats and measure the consequences and recovery effort more accurately. This situation also provided a baseline on user experience and system usage by which to adjust our final recommendations.

2.3 Assessment Impact

The impact of the security assessment on the IASEP research project, as a whole, was significant. Deliverables from the assessment have been adapted into training workbooks and presentations. We have filmed a video highlighting scenarios in security, as they relate to our threat analysis, that are of most interest for the individuals who will use the system regularly.[39]

Many IASEP system users are excited about having the laptop platform available for their classroom and home use. Yet users are becoming increasingly cautious of the warnings about privacy and system corruption that they hear in the media. There can be serious consequences related to liability issues resulting from a compromised system. Our goal was to predict and ultimately prevent these situations. Given this overall increased security awareness throughout an increasing number of user communities, we have been able to promote and achieve good practices and safeguards as advocated throughout the assessment deliverables.

2.4 Team Composition

From the beginning there have been several individuals focused on the data security element of the IASEP project. The purpose of this section is to describe that group. These descriptions provide information about the types of roles involved during the data security endeavor.

Representing the School of Education at Purdue University as the committee chair, with the duty of overseeing the entire IASEP research campaign, was Deborah Bennett. Dr. Bennett is a faculty member in the School of Education and has led the entire team through the formation and implementation of the IASEP program. Working with her are three individuals who have been involved in the entire IASEP research initiative from the beginning. Mel Davis is a graduate student in the School of Education, with the role of program coordinator on the project team. Ms. Davis was in charge of organizing initial data collection and running of the pilot, among other activities throughout the roll-out. Another graduate student from the School

of Education focused on IASEP research and development was Helen Arvidson. Ms. Arvidson was instrumental in the development of the training guide and other documentation pieces throughout the effort. The primary software developer involved in IASEP was John Cunningham. He was contracted by Purdue University to handle the application development and overall technology integration for the system. He provided the team expertise in developing educational systems.

Representing CERIAS (Center for Education Research in Information Assurance and Security) was Stephanie Miller and Steve Hare. Ms. Miller, the author of this document, is a graduate student in the Computer Sciences Department with research interests focused on many topics within the realm of information security. She was asked to join the project, leveraging past experience with security consulting engagements in industry, to guide the team through the security assessment process. Steve Hare, managing director of CERIAS, helped with the development of deliverable materials. Mr. Hare was instrumental in providing recommendations on the security assessment process as it developed.

Several stakeholders from the Department of Education in the State of Indiana (IDOE) were regularly involved in the team activities. They were Steve Stafford, education consultant in the Division of Special Education; Duane James, policy analyst in the Division of School Finance and Educational Information; and Darcy Hopco, a special education legal consultant. Ms. Hopco produced an outline of "Confidentiality Reminders" that describes parents rights, when parent consent is required, the legal definitions of "educational record," the "personally identifiable information," as

well as a number of other critical points for teachers to keep in mind when using the IASEP system.[13] Everybody from the IDOE provided insightful points for further investigation as well as views into the state's organizational resources and recent work related to the project requirements.

Additional people joined the team as the need arose. We had one teacher, Karen Stein, from the pilot group who was actively involved in the IASEP data security project. Her input about the system was extremely beneficial as we discussed ideas in meetings and gauged how users would likely react to our proposals. Eric Davis, legal counsel with a focus on intellectual property and copyright for Purdue University, provided legal advice related to the specific intellectual property and copyright protection concerns. These have become important issues for the team as inquiries are being made for the licensing of the software and related tools in areas beyond the initial development focus. Karen Dodson participated in one of our data security meetings to provide awareness regarding parental concerns surrounding the technology. As a parent already involved in the pilot study, her insight was extremely valuable to the team. Kevin McDowell, also from IDOE, was indirectly involved during much of our endeavor. He offered examples of past work he has performed related to data privacy matters as well as advice on particulars of the education systems and programs in Indiana. Candace Person is handling the security protocol development that will be discussed in the next section. Her background is as a specialist in cyberlaw and she brings expertise in interpreting case law related to electronic privacy and the interfaces among web technology, confidentiality, and First Amendment issues. All of

these experiences combine as she works in a consultative capacity as the team explores the development of comprehensive procedures to guide the collection, storage, and transmittal of electronic data both for the individual laptop assessment procedures and through the web-based procedures that are envisioned for the future.[13]

2.5 Project Scope

The IASEP system was initially designed for use as an assessment tool for special needs students in public schools within the state of Indiana. The interest in this technology has since grown as news about the tool and its many possible uses has spread beyond Indiana. The system reached the end of the pilot deployment phase the Fall of 1999. According to [12], the number of participants in the pilot effort consisted of 60 teachers who represented 370 students in nine locations. This number increased after full roll-out and deployment to approximately 1000 teachers in the 1999-2000 school year. Each teacher was given his or her own laptop configured with the necessary software. Scanner equipment, as well as video and audio capture devices, is shared by multiple instructors.

Technology coordinators are available to handle system problems and upgrades once the project is in full production. There are approximately 170 technology coordinators who are trained for the IASEP system.[42] They will be supporting teachers throughout the local districts.

The first large-scale transmission of the assessment data will occur in May 2000. District and state level technology teams are making preparations to accept the data and perform the aggregations for analysis.

Use of the student assessment system beyond this initial focus area is not yet finalized.

2.6 Future Work for IASEP

Everyone who participated in the collaborative security assessment realized a heightened sense of responsibility surrounding issues of data protection. Many activities are underway to promote this new-found revelation about security with users of the current platform as well as to future projects intended to bring more technologies into the hands of the educators in Indiana and other locations.

As the security assessment matured, we all soon realized a significant gap exists in most state programs related to issues of information security in technology. Therefore a new project team has emerged to research the exact situation in state education departments throughout the country. The mission of this team is to develop a security protocol to be embraced by similar education technology projects in the future. The project goal as stated in [8] is to develop a general prototype for the management of all electronic educational data that complies with state and Federal laws. The resulting objectives have been outlined in table 2.1.

This project team has been actively engaged since early July 1999 and is working towards a comprehensive document to fulfill these objectives.[17]

Additionally, efforts are underway to address inquires for expanding the use of the IASEP system beyond its initial purpose, that of assessment for students with severe disabilities. There has been talk about using the system and software in preschool en-

Table 2.1
Protocol Objectives

1. Identify current data security policies and procedures and develop a set of protocols that will impact how data is entered, stored, transmitted and reported in Indiana.
2. Team with CERIAS, state educational and legal consultants to expand the security work underway with the current IASEP system (the topic of this thesis)
3. Develop a set of schematics to display the information compiled and written so that readers and practitioners can readily visualize and understand how the protocol elements fit together and how they could be used to implement the protocol
4. Develop a training protocol to disseminate critical information

vironments, as well as licensing the technology for the benefit of other states interested in the tools that have been developed. Negotiations are pending with Massachusetts, Rhode Island, Kentucky, New York, Michigan, Nevada, and South Carolina currently. Likewise several task-forces have been created to investigate uses for the technology of IASEP in various other environments. These groups are ECAS (Early Childhood Assessment System), addressing the needs of younger children and DIAS (Documenting Indiana's Academic Standards), addressing the needs of "gap" students, who represent up to 40% of the student population and have milder disabilities.[18] These are students who find difficulty with traditional standardized testing.

2.7 Chapter Summary

IASEP is a dynamic project exhibiting most of the critical security requirements that emerge in new technology projects. The IASEP project has brought new tech-

nology to teachers in the classroom and the resulting challenges are ground-breaking in many ways, not the least of which is the integration of security considerations for education environments.

There are a variety of factors present in this project that have added to the task of the security assessment process. The utilities encompassing the assessment had to be integrated seamlessly with the assessment application. In many instances computer technology was new to the end users and the IASEP team wished to increase the comfort level of those users with the platform while providing the necessary mechanisms to harden the system against attack or misuse. There is a balance to be realized when building a system for user flexibility and solid security safeguards simultaneously. The security assessment that will be presented in chapter 4 was intended to accomplish this balance.

3. FUNDAMENTALS OF COMPUTER SECURITY

3.1 Overview

The fundamental goals of information security rely on trusting a computer system to preserve and protect its data and resources. Terms like security protection and privacy often carry different meanings to different people. However the underlying definition is that a secure system should be dependable and behave as expected.[1] Some of the most common concerns in security protection are confidentiality, integrity, and availability. However additional requirements in authentication, access control, authorization, and non-repudiation are also significant when implementing security controls. All project developers must account for the unique blend of requirements they must manage to adequately protect valuable resources and information in a computer system.

The role of a security assessment is to measure the degree to which these requirements are met in a project and to then make recommendations for increasing the amount of trust in the system. A security assessment can be thought of as a technique for determining how much money to spend to protect information resources, and how to spend that money.[9] The graph in figure 3.1 depicts the balance between security implementation decisions and cost controls. The most important and significant contribution to making these determinations should be to implement the same

types of baseline security controls and practices as other prudent information owners in similar circumstances.[9]

This chapter will dissect many of the security requirements commonly identified in security assessment work. There are a variety of requirement classifications often presented in discussions of security; in this section we will highlight some of the common topics. Each aspect of security will be defined according to how information can be compromised, followed by frequently suggested mechanisms to ensure information protection against this type of compromise. Finally, for each definition, we will present examples to point out the specific applications of these requirements to education-related procedures and practices.

3.2 Confidentiality

The requirement of confidentiality is closely tied to the need for privacy. The idea is to allow communication between entities in such a way that the participant identity and/or message content are accessible only for reading by authorized parties. This type of access includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object.[34]

The most common approach taken to fulfill confidentiality requirements is to use techniques of cryptography. By scrambling all data contained in an object through a function known as encryption (where an object can be a message, file, or similar piece of information) privacy for information owners is obtained. The result is that only appropriate parties can retrieve the information. In addition to encipherment newpage of data, confidentiality is sometimes achieved by traffic padding. However this is a much weaker means of ensuring privacy.

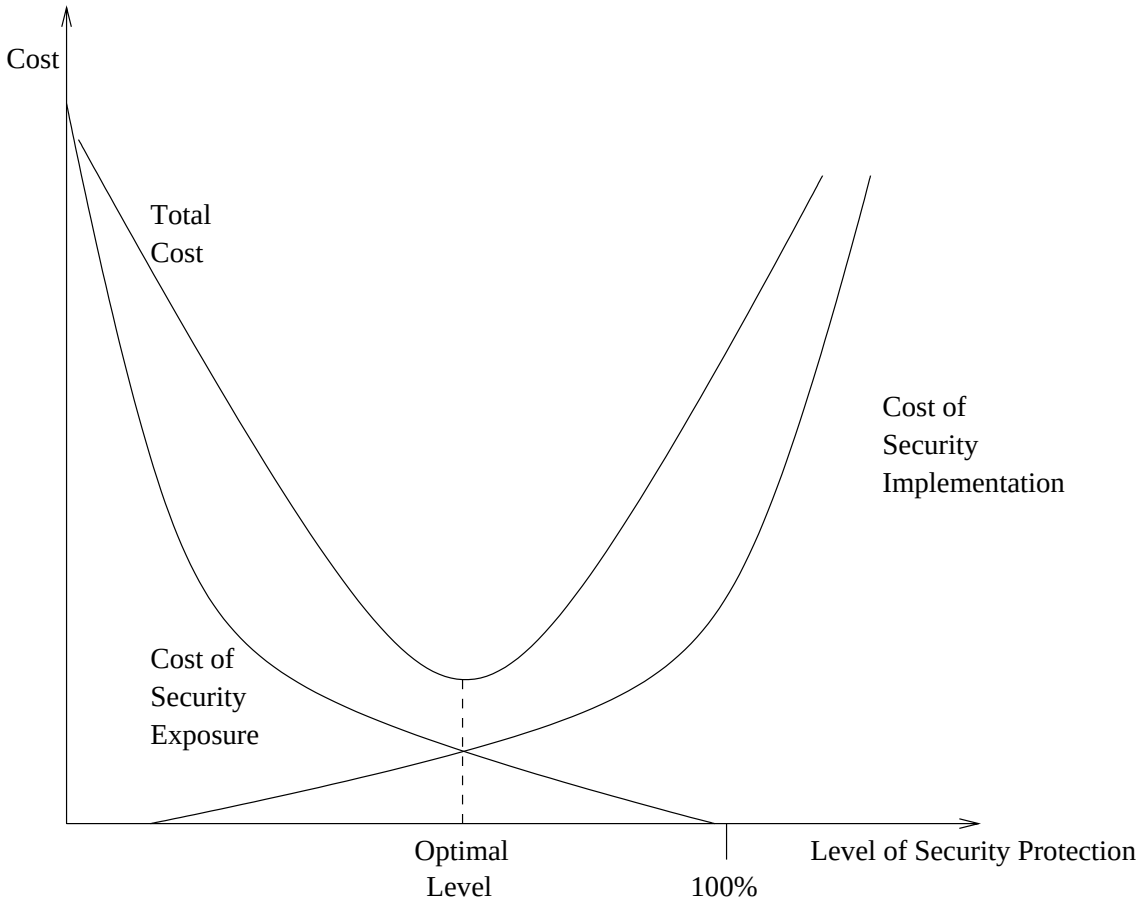

Figure 3.1. The security cost "function" [2, 36]

The primary violation of confidentiality is disclosure, but modification can also be a violation. Compromise is often the result of malicious activity whereby active efforts (cryptanalysis) are employed to break the code for the enciphered message, but that is not always the case. Errors can also occur during transmission of the message. This leads to the requirement for most mechanisms to detect and attempt to correct such modifications. With the use of encryption, additional precautions should be taken to protect the security of the cryptographic keys stored in host machines. Compromise of the keys directly effects the privacy of information being protected by those keys.

Confidentiality is a critical component for protecting student data. FERPA, the Family Educational Rights and Privacy Act, states that its purpose is to set out requirements for the protection of privacy of parents and students under section 438 of the General Education Provisions Act, as amended.[23] FERPA dictates a specific set of standards for information disclosure that are designed for protection of student and parental rights. If any type of student information maintained by an educational institution is leaked or accidentally transmitted by electronic means, it is important that anybody intercepting the data is not able to interpret the meaning or value it contains. Encryption fulfills this requirement.

Appendix A provides further details on the basic terminology and mechanisms driving the field of encryption.

3.3 Integrity

The idea behind integrity in information security is that when a user moves or communicates information, that information starts and ends in the same state of

wholeness, unimpaired condition, and completeness. No fraction of the information is missing or concatenated, encrypted, or converted in any unanticipated ways.[10] We all need the ability to trust the computer systems we use to handle our information properly. Integrity requirements are critical in the field of security to establish this sense of trust that an object still contains the same unaltered information it was intended to provide.

One possible technique used to ensure integrity of messages is to utilize secure one-way hash functions. When a secret key is used along with the message, the function is known as a Message Authentication Code (MAC).[34] Other names used for this class of technique include cryptographic checksums, message digests, or fingerprints.

Unlike encryption, in which decryption is the reverse operation, a one-way hash function works in one direction: It is easy to compute a hash value from the message, but it is hard to generate a message that hashes to a particular value.[4]

Examples of these techniques include MD4, MD5, and SHA. These algorithms generate a small fixed-size block of data that is appended to the message.[34] The two communicating parties can share a common key. The checksum is then generated by the sender as a function of the message and key. The entire message is transformed into anywhere from 128 to 256 bits in most practical cryptographic checksums. The receiver of the data can then use the same algorithm to again generate a hash of the message and compare it against the one that was provided. If the hash values differ, it is evident that the message has been altered. Additionally, sequence numbers, digital signatures, and time stamps can be considered as mechanisms for integrity validation.

A compromise to integrity occurs when the message itself has been altered or the mechanism for ensuring integrity has been tampered. This occurs when an unauthorized party not only gains access to but tampers with an asset. Examples of such activity include changing values in a data file, altering a program to perform differently, or modifying the content of a message as it passes through a network.[34]

In education there is a strong need for data integrity. Any type of alteration to student performance records should be immediately evident to school administrators. Falsification of information such as student grades or financial assistance details is a serious concern in educational institutions. The use of computer systems should not make it easier to access and change records. If such an attempt were made, school authorities should be notified immediately by the system.

3.4 Availability

Availability is the capacity to guarantee that system resources such as operating systems, networks, and applications are accessible when they are needed. More concisely it is defined as the state of being present, accessible, or obtainable; capable of use for a purpose, immediately utilizable.[10] This property is a cornerstone of security. If one cannot use his or her computer, there is no way of knowing if other security requirements are being followed. The requirement for continuous system availability is critical, and many businesses today would not function if access to computing resources were denied to customers, partners, or suppliers.

The loss of availability is known as denial of service (DoS). Denial of service results if a machine is no longer responding because of overloaded resources or power failure. Denial of service can also happen when the method for accessing the machine

is removed or modified (such as a changed password). DoS is a serious threat for computer systems today, especially those with permanent connections to the Internet.

One approach to ensuring availability of resources is to maintain redundancy in a system. Through redundancy several systems can share the same role so that in the event of failure of any one device, an auxiliary resource automatically becomes available. Other mechanisms used for protection of system availability are careful system administration and sound system design [5]. In addition, protection from physical harm is also encouraged. Good system administration practices include active monitoring of usage as well as careful backup procedures along with recovery planning.

In education environments, there are specific time-lines for completion of student testing and evaluation. The introduction of new technology for this purpose brings to bear the absolute need for availability of the system during that period of time. If system availability is lost, important deadlines could be missed with severe consequences for a corporation.

3.5 Authentication

Authentication is a means of proving ones identity to another. This is a requirement for most types of computer access. When a user "logs on" to a system, he or she is authenticating himself/herself as a legitimate user of the computer.

This aspect of security is one most individuals engage in daily. Common mechanisms for achieving authentication include:

- Something I know (such as a password)
- Something I have (such as a smart card, or digital certificate)
- Something I am (such as fingerprint or retinal scan)

An additional method of authenticating oneself could require the use of a third party (e.g., a notary service) to validate identity.

Authentication is used as a way to prevent masquerading. The degree of prevention depends on the strength of mechanism employed.

This security requirement exists in almost any use of technology being developed. In our particular case study, all users are required to authenticate themselves to the IASEP rating system as part of launching the application. This mandate works to prevent the entry of data into the system without properly identifying oneself as the instructor whom the program recognizes.

3.6 Authorization

Once a successful authentication dialogue has taken place for a system, authorization enters the picture. Authorization can be characterized as a set of polices, rules and procedures in the most general sense. It is a process of granting certain rights to users once they have satisfactorily identified themselves (such as with a name and password combination). On some systems, a master user (often known as root or administrator) has full authorization on the system. That user has access to any information or activity running on the computer. Other users have varying degrees of authorizations as defined by the actual controls being used.

Mechanisms for determining authorized privileges include access control lists, and role definitions. It should be possible to define new authorizations as needed or to remove excessive authorizations. Effective authentication is a requirement for proper functionality for the authorization controls that are established for an internal user at login time.

Authorization has been compromised when an unprivileged user has gained rights to protected data or activities. Authorization is a means for improving security by increasing internal user accountability and limiting overuse of authorized access.[41] Many statistics indicate that over half of all computer security breaches occur from the inside by the trusted users. This is often the result of granting them more authorization than they need. For example, granting a backup operator full administrative privileges to perform that simple duty could lead to abuse of the excessive privilege.

In education, the property of authorization is demonstrated by the different responsibilities identified for different roles in the administration. For example, an aide may be authorized to manipulate attendance records in the computer system but does not have the authority to view or change a student's grades. The authorization for this task is granted solely to the classroom instructor. This type of administrative policy is enforced in the computer using the necessary mechanisms to grant the prescribed authorizations.

3.7 Access Control

The property of access control works closely with that of authorization to protect against forbidden use of resources. The basic technique in this area is to grant subjects (users, processes) access to objects (files, memory blocks) based on access rights.

The access rights describe privileges of the subject and state under what conditions those entities can access an object and how the access is to be allowed[2]. This is a process that occurs automatically without user interaction. A system administrator or another user wishing to grant access to particular data sets the access privileges accordingly. Internally the system acquires a user identity (the name he or she authenticated with), verifies that identity, checks rights of that user before granting access, and optionally logs and monitors user activity with the resource.

The two primary policies of access control are discretionary access control (DAC) and mandatory access control (MAC). In DAC, the owner of an object has the option to protect an object against access from other entities on a need-to-know basis. In MAC, the system always checks an entity's rights to access an object. Neither an entity nor the owner of an object can ever override or change the decision made by the system.[2]

Access controls can be defined for network access, system access and resource access.[11] Mechanisms popularly used for this purpose include access control lists, network perimeter devices, security labels, time of day/duration limits or filters. Users are typically combined into groups as an additional method for granting access privileges. The various mechanisms are used as a means of controlling what information is accessible to the user or group and how the information may be accessed. Such controls can restrict read, write, and execute privileges on objects for particular users.

The property of access control is particularly useful in the implementation of IASEP that was analyzed. Users with different responsibilities required access to the same rating program. However, the access privileges they possessed differed based on their role in the classroom. Instructors needed full read / write access to all data in the system for student assessment. However classroom support staff only had a need to access restricted areas of the software. Based on user identification that separation of roles could be achieved in the software.

Note, the definitions of authorization and access control are closely coupled. One can think of access controls as the means for granting authorized activities. In many documents the differences are so small that these security properties are often combined. They are separated for the purpose of this thesis to provide information on a wider spectrum of security related terminology.

3.8 Non-Repudiation

There are many perspectives to consider when it comes to non-repudiation. Generically this property ensures that a message or transaction was initiated by the identified sender and received by the identified receiver. It protects against later denying responsibility for involvement in a communication. A combination of four services: proof of origin of data, proof of original content, proof of delivery, and proof of original content received, encompass non-repudiation.[2] Together these services ensure that neither the sender nor the receiver can deny having sent/received a message or deny the contents of that message. Non-repudiation can be used to provide legal evidence of a user's actions.

Mechanisms for ensuring this security property include use of digital signatures, a notary service (also known as an arbitrated signature), or time stamping among other options. A digital signature is analogous to a handwritten signature, but more powerful in the context of trying to counterfeit it. Digital signatures are based on techniques of public key cryptography (as detailed in Appendix A) and can be directly used between the communicating parties or through the services of an arbitrator. The basic functionality of a digital signature is to generate a hash of the data to be signed, and then encrypt that hash with the private key of the person issuing the signature. Once the signature has been checked using that same person's public key, the authenticity has been confirmed. The essence of a digital signature is that the receiver must be able to prove that a message originated with a given sender, but must not be able to construct the signed message. Thus the sender requires secret information to construct the signed message, and the receiver must be able to access public information to use in the validation of the message.[41]

Compromise of non-repudiation functionality occurs when an individual who is cheating the mechanism is able to claim to have sent to a receiver (at a specified time) information that was not sent (or was sent at a different time). Another approach would be to claim to have received from some other user information that the cheater created.[34]

In education, a problem could arise if a student were able to deny receiving a reprimand electronically. Likewise one may be able to claim that a research report

was submitted and received prior to a deadline using non-repudiation techniques if that submission were questioned.

3.9 Audit

Having some or all of the above security measures implemented is not sufficient to ensure complete protection. The definition of an audit is an independent review and examination of system records and activities to test for accuracy of system controls, to ensure compliance with established policy and operational procedures and to detect breaches in security.[41]

One mechanism available for performing an audit is system logging. Making a record or log of system activity is necessary to detect malicious usage occurrences. Along with logging of data, mechanisms for data reduction, and data filtering are employed to help in the identification of malicious activity.

A compromise to audit functionality is the alteration of the log entries that are generated. Alterations could include removal of particular log entries or timestamp changes.

In educational environments, the need exists to keep track of who is granted access to specific student information. Not only should access be controlled for that sensitive information, but it should also be documented by the system. Documenting file access is not a new process in education – the precedent has existed for some time in the paper file cabinet environment. With new technology emerging, there is the ability for more reliable auditing capability. Careful planning needs to be done to ensure the same documentation standards are being realized electronically.

3.10 Summary

For the sake of simplification and summary, table 3.1 has been provided to accumulate some of the security mechanisms that were identified in this chapter. Combined, these techniques provide a toolset by which to establish the desired amount and type of security protection. Some of the components from this table will be used when we discuss the generation of the security architecture.

Ultimately, the three primary concerns of confidentiality, integrity, and availability (CIA), are essential in the protection of student records and must be implemented for any new technology dealing with that type of data.

The remaining security requirements that were outlined in this section are necessary in varying degrees of magnitude for the protection of student data. They compliment the CIA principles and will also be highlighted in our discussions of the security architecture later in the thesis.

Table 3.1
A Partial List of Common Information Protection Mechanisms

- Digital Signature
- Access Control List
- License and/or certification
- Signature
- Witnessing (notarization)
- Liability
- Certification of origination and/or receipt
- Audit Trail
- Checksum
- Access
- Validation
- Time of occurrence
- Authenticity – software and/or files
- Ownership
- Registration

4. THE ASSESSMENT DETAILS

4.1 Introduction

A security assessment process is defined by taking all of the requirements for protection into account and recommending appropriate safeguards. According to Webster,[37] the action of assessing involves making a determination of the importance, size, or value of an item. An assessment provides a systematic method for reviewing each requirement in the setting of the project at hand to ensure every possible project component is analyzed and understood.

This section will detail the activities that occurred during the security assessment of the IASEP project. At each step of the process we had to remain conscious of challenges related to aspects of people, process, and technology issues. Awareness must be raised among the administrators and user population regarding security. Furthermore accountability for activities must exist among all users of the system. Process issues relate to areas of policy, audit, and management. These topics should not be overlooked as they are essential for maintaining the level of protection implemented by the technology components. Finally, technology considerations can be handled in architectural designs, customized frameworks, and product selections. All of these focus areas will be addressed during the course of the assessment.

From start to finish, the IASEP project has provided a system for adapting security models and practices into newly evolving research and technology in the field of education and associated technological developments. We anticipate that our work here will serve as a springboard for future integration projects concerning security in education technologies.

4.2 Project Review

4.2.1 Overview

We began the task of understanding the IASEP system platform fully, as well as user processes and overall requirements of the system, upon our initial contact with the project team. Our first goal was to understand how the system was to be used by teachers and the functionality it possessed. Following that analysis, our objective of integrating specific security requirements into the project could be undertaken.

4.2.2 Initial Investigations

Prior to meeting with the IASEP project team for the first time, a small amount of overview material was provided to share background information on the project. By reading this document we had a better understanding of the goals for the overall research effort and initial progress it had achieved. Using this information we began contemplating the various forms of security controls that would apply to the software being discussed. Our ideas revolved around the platform used to develop the software, a Windows based notebook computer, as well as the nature of the information being collected. The basic features we perceived would be most relevant to this setting were

virus protection, physical security of the hardware, and confidentiality of data on the system. With this mind-set and knowledge that additional information would need to be gathered, we met with the IASEP development team for the first time.

That first meeting with the IASEP team took place on December 4, 1998. [14] The purpose of this meeting was to introduce key players in the project and to begin to describe how the project had evolved to the current state as well as to explain where the concerns for security had been introduced. Following this initial probe, we were then able to better understand the purpose behind the technology being deployed. In addition, during this first interaction, we began a series of discussions about security requirements in general. These on-going tutorials provided familiarity related to common security definitions and purpose for the educational benefit everybody involved in this security assessment.

During our project discovery time we learned about the software development tool, a product named Clarion TopSpeed [38], being employed by the team and the capabilities it had for enabling encryption algorithms. We received our initial glimpse of the rating software that had been developed. We also learned that this project had significant scalability concerns as discussion proceeded about the pilot deployment and roll-out expectations. Finally, during this time we learned that it was unclear who would have the final responsibility for the project once the researchers from Purdue had finished development. All of these topics required further investigation as the assessment ensued.

Following basic conversations about the project and the need for addressing security concerns that had arisen, a demonstration of the newly developed software took place

along with a description of how the multimedia documentation pieces were integrated into the tool. For a more complete description of the software package refer to [29]. This demonstration gave us the opportunity to observe not only the tool to be used by the classroom instructors but also some of the underlying processes that drive the whole system. These usage processes prescribed how a teacher interacts with the system during data collection, data storage, and data transmission.

The screen shots in figures 4.1 and 4.2 are presented to provide context for the reader regarding the technology and software being evaluated.

4.2.3 System Analysis

The next focus of security assessment review was to understand how data flowed among all entities in a high level view of the IASEP rating tool. Through a series of discussions, we captured the essence of the overall tool usage. Before any student assessment-specific data is collected, the teacher must enter basic information about each student. The teacher then collects the student's assessment data (including multimedia documentation pieces and rating calculations) in a classroom setting. From that point the information accumulated on the laptop has to be passed to the school district for aggregation, and finally on to the state department for analysis. The initial plan is for data transfers to take place using Zip disks; future plans call for data transmission over the Internet.[13, 14, 15]

Our next step was to gather information about the established student data access procedures within school districts. We also needed to obtain legal information to better understand the confidentiality rules and regulations surrounding this type of

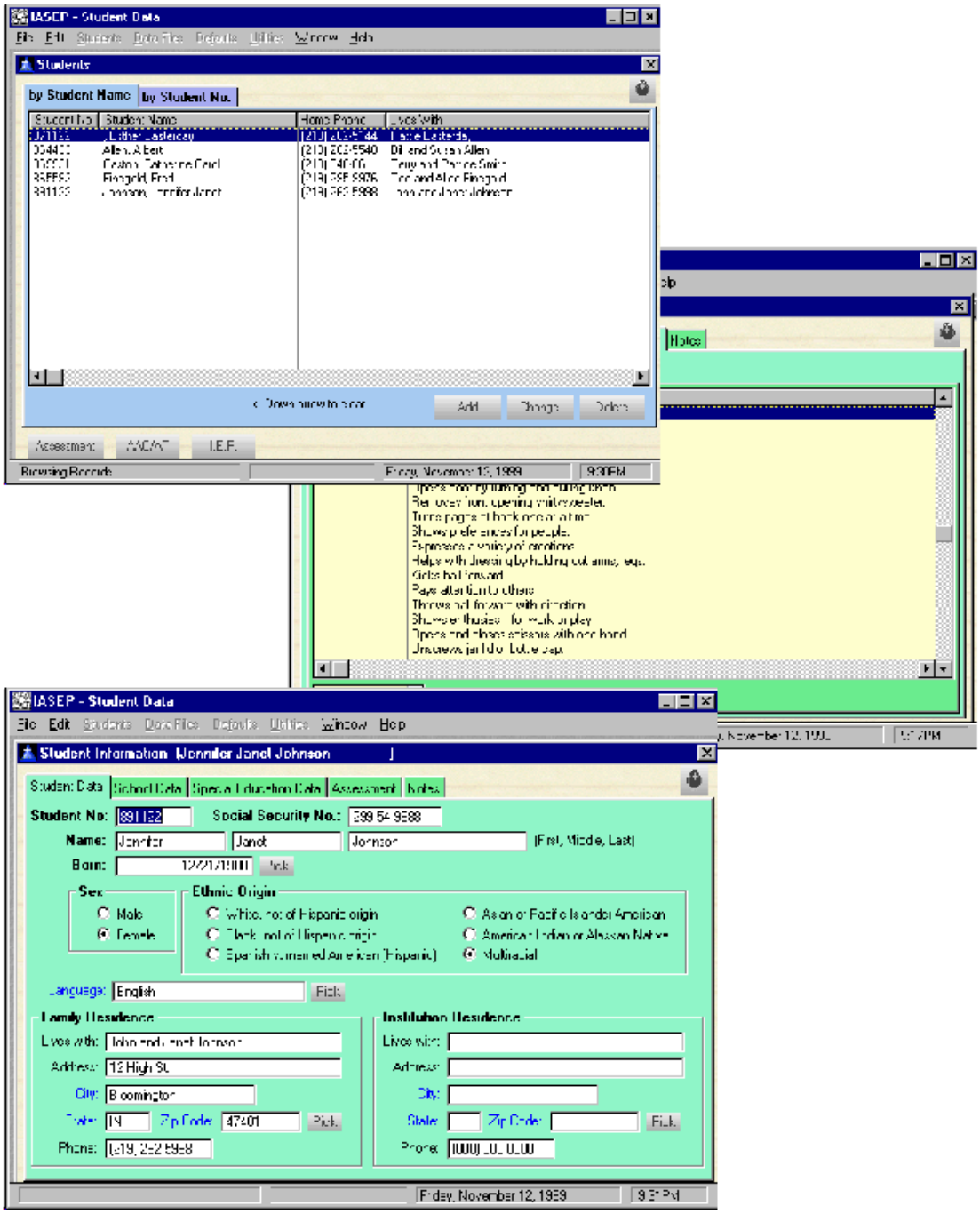

Figure 4.1. IASEP Screen Shots

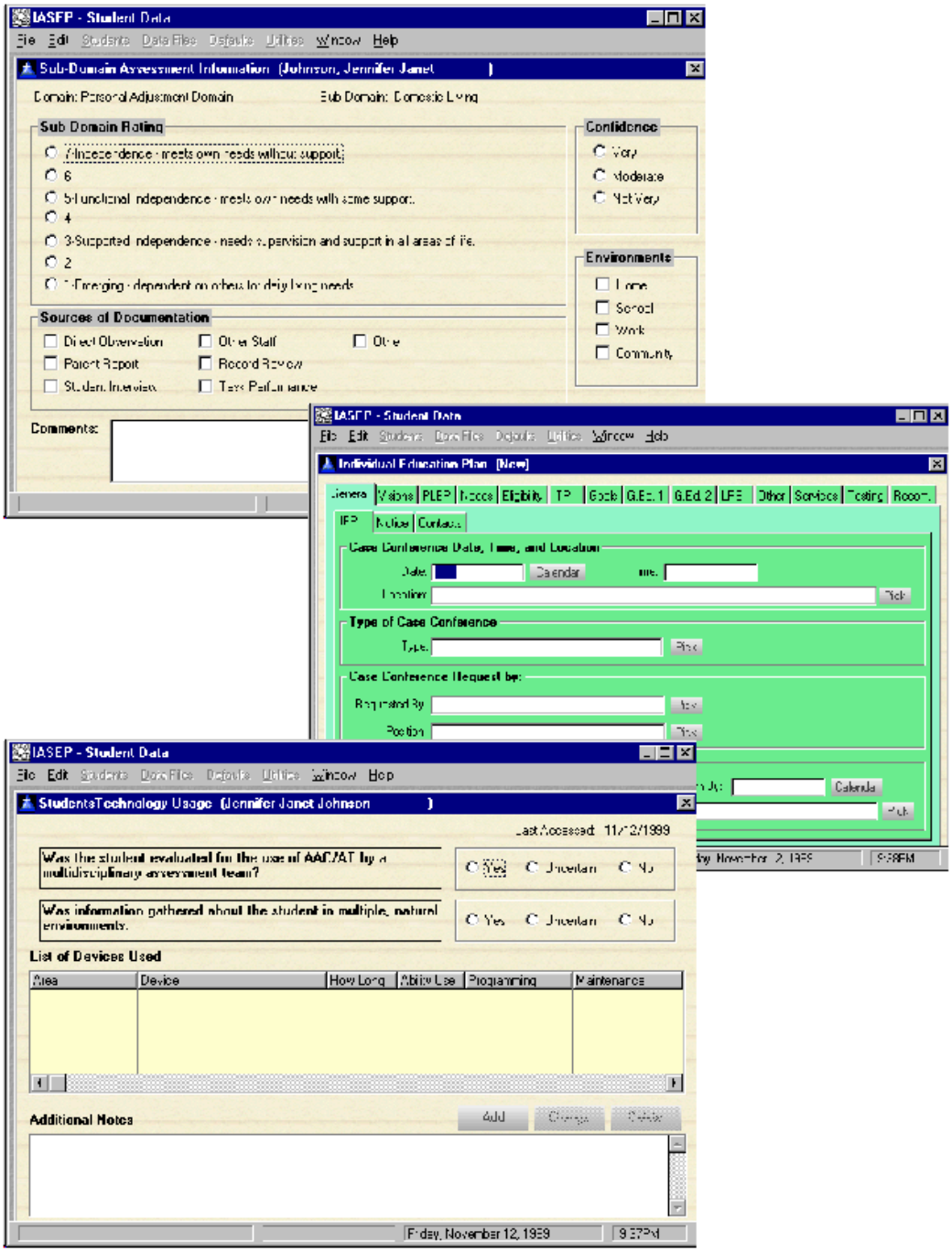

Figure 4.2. IASEP Screen Shots, cont'd

data. We discovered that nearly all regulations in current use have been written for the paper cabinet model of a student file. Therefore it has become one of our duties to help the team adapt that set of precedents to the electronic file model. That was a specific task handled by Ms. Hopco. Her work has also uncovered some of the Internet acceptable use policies implemented in school corporations currently.[40] Those documents were utilized during the policy development described in section 4.8.

Moving past the procedural elements of the project, we began to focus on the technology being implemented. We obtained a copy of the software and installed it locally on a CERIAS machine to learn more about how the system could be used and abused. Our initial discoveries are outlined in table 4.1. These observations were shared with the developer who then worked to incorporate better security standards into the software.

4.2.4 Ongoing Investigations

The remainder of our initial learning in the project occurred over several meetings.[14, 15, 16, 17] We would gather security related points of interest from the team, and then returned with additional questions and recommendations for the team to address. During the course of multiple discussions with the team around specific concerns in the project, we were able to devise a list of the most critical issues to handle during the development of our security strategy. Table 4.2 highlights those areas.

Some of the specific details related to the concerns in the above table involve differentiating a specific student's data in the documentation pieces. Each multimedia

Table 4.1
Installation Notes

- A standard password is used for every new install (which is provided in the documentation). There is no forced change to a fresh, individual password upon starting the tool. That option is available within the menu system if the user chooses to reset the password on their own.
- The software package always installs to the same location; no option is provided to choose a different location using the installer.
- It was unclear from the binaries provided which fields of data were being encrypted. This is an area requiring further investigation.
- All data files are stored in a single directory location. We were unable to determine if this location is configurable by the user.
- Unsure what "housekeeping process" is doing. The developer needs to have strong control over automatic maintenance activities which the system performs.

segment should only capture a particular student. This requirement will be a challenge to enforce as videos are collected in a classroom environment.

Also the state has strict mandates regarding the ability to associate an individual student to unique test data. There is currently work being done to address the problem of proper translation between an identifier kept with data and the student it represents. This is a very delicate subject with legislators and there does not seem to be resolution to the problem in the near future.

These are just a few of the specific concerns raised by the IASEP project team and stakeholders. Each issue identified in the table will need to be addressed in turn. Some, like the two mentioned above, are out of the scope for this security assessment. We continued to learn about the IASEP program as the security assessment progressed. This list of topics provided in table 4.2 accumulated primarily in these

Table 4.2
Principle Security Concerns

1. Student identifiable information and translation points. There are guidelines in Indiana that must be followed.
2. Capture of multiple students in documentation pieces is a confidentiality concern, especially among parents.
3. Release of medical information or other highly personal student information kept on the system must be prevented.
4. Password sharing between teachers and aides, especially in ways others can take advantage of (i.e. via chalkboard) needs to be discouraged and/or prevented.
5. The techniques to be used for encryption cannot be too cumbersome. They must be powerful yet easy to use.
6. Need to identify which pieces of data in the system are to be encrypted.
7. Obtaining parental consent to use the system for their child. The parents must trust the technology to protect their interests. This concern was a driving force behind the initiation of the security assessment.
8. Desire to keep track of hardware and software (asset management, configuration management). Need to understand other state processes and adapt to them if they exist or develop our own.
9. Desire to not prohibit teachers from learning more about technology while keeping sensitive information protected. Need to be able to harden system without scaring user from using it to fullest potential
10. Considerations for using the Internet as possible transfer mechanism vs. hundreds of ZIP disks
11. FERPA compliance must exist.
12. Need to document how to recover from system failure, compromise, etc. Along the same lines there is a need to adequately understand a compromise to detect and act swiftly.
13. Interfacing with other systems is necessary for IASEP to be useful and long lived. An example of such a system is called CODA.

early investigation stages of the work, but also matured as we moved into developing a customized security strategy. While we realized it would be an extreme effort to address every point in the table, it has served as a guideline and motivator throughout the assessment endeavor.

4.2.5 Project Review Summary

It took several meetings to work through this data-gathering phase of the assessment. However, by doing so we were able to arrive at a fairly comprehensive view of the IASEP project. Having a clear picture of the project under evaluation enabled us to produce valuable deliverables for the entire team. There were still issues to be uncovered as we progressed through the assessment; that is to be expected. Overall the results of this phase allowed us to move forward through the assessment possessing a good understanding of our mandates and needs.

4.3 Data Flow Diagram

4.3.1 Overview

Using the findings from the project review phase, we were able to devise a visual representation of the flow of data through the system. Our definition of the system for this purpose is the complete use of the tool from data creation on the laptop through collection and processing of results at the state level. Figure 4.3 is the outcome of this phase of the security assessment. Our goal was to establish a convenient model for describing the system in its entirety. We wanted the diagram, which we also call a process map, to abstractly convey the use of the system while being as accurate

as possible. This visualization of the system enabled us to easily demonstrate where critical junctures existed in the system and to later provide a framework for developing the overall security architecture for the project.

4.3.2 Description

In the diagram, the arrows indicate how data traverses through the system and the squares represent significant data processing activities. The oval labeled "Win95/98 shell" signifies that the system is idle and an empty desktop is displayed on the screen with no processes running.

Three generic actions can be initiated from the Win95/98 shell. One, the system may be shutdown and thus end further operation. Two, a user may choose to configure the system. While later we will recommend that configuration options are minimized, the system is fully available for the user to control, for the purpose of the diagram. Possible configuration activities could include installation of new software, entering the control panel to alter parameter settings for various devices, installing a new printer, etc. Any activity that would alter the original system configuration as shipped to the user would fall into this category. Finally number three, the most frequent activity to be performed by the user is the launching of a piece of software installed on the system. Any application falls into this category. For example starting up a word processor, spreadsheet, email client, web browser, or even a game are examples of this action. For the purpose of this discussion we will focus on launch and usage of the IASEP rating software and auxiliary utilities for collecting the multimedia documentation on students. The other applications will be considered as the security

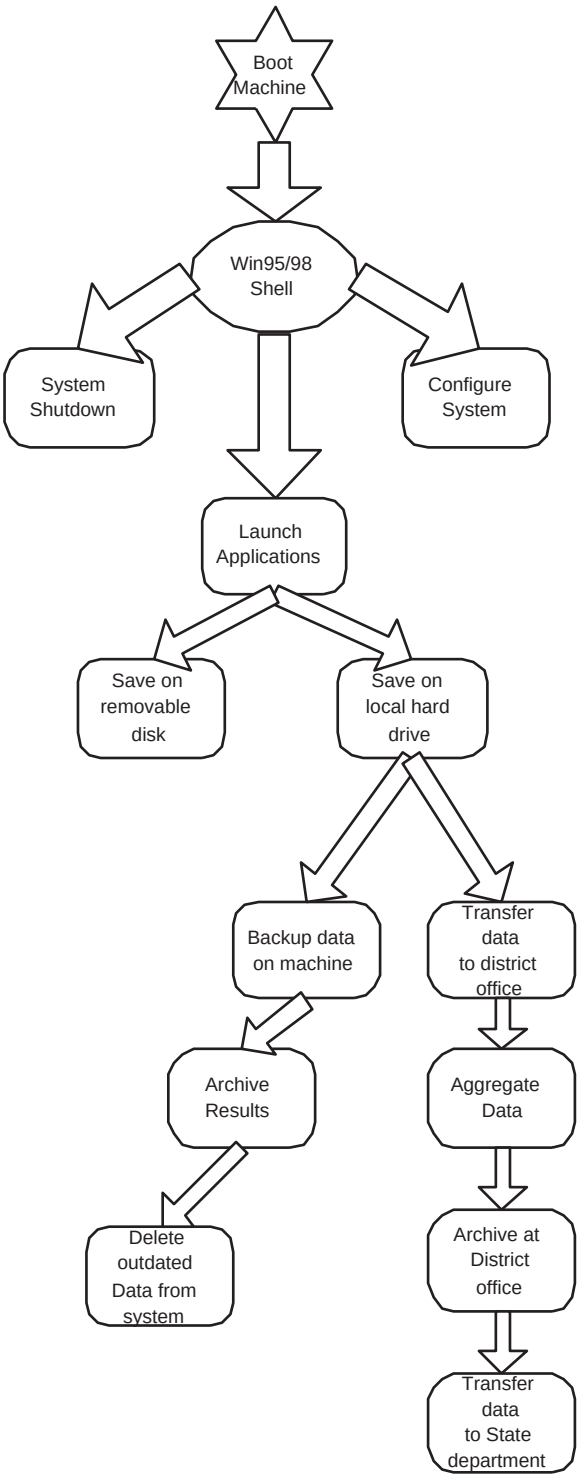

Figure 4.3. IASEP Data Flow Diagram

architecture is developed, but the complexity of the development for the IASEP project is in the rating system and result processing. This is the need that drove the establishment of this data flow diagram.

Using the appropriate applications, data is captured and accumulated into a student file. The default operation is for student files to be stored on the hard drive of the machine. The user has the freedom to save files to an external medium such as floppy diskette or Zip disk. Each laptop is routinely backed up, although the regularity of that routine depends on the discipline of the machine owner. Those backups are necessarily archived and the medium used to store the backups is rotated as will be prescribed by policy. At the end of a school term, a student is no longer the responsibility of the current instructor. At this time each student's data should be purged from the machine.

Ultimately data collected on the individual machines is transferred to the district office for processing. As soon as the data for all instructors of a particular district have submitted their results, the collection of entries is aggregated before submission on to the state department for analysis. The data is archived at the district level and the last transmission of concern is that between the districts and the state department.

4.3.3 Alternative Representation

In addition to the figure 4.3, we also found it helpful to abstract the data flow model and provide finer granularity in the process descriptions. This alternative representation provides a drill-down ability to fine-tune the details at each step of the process (see figure 4.4).

The overall information contained in either representation is the same. This version of the model was not actively pursued during our security assessment. However the creation of this alternate model was a helpful exercise to undertake. Through it we could further demonstrate a well-rounded understanding of the IASEP system and underlying processes. This representation of the model is included here to provide accurate documentation of all efforts in the security assessment, but will not be revisited again during the security architecture phase.

4.4 Asset Identification

This aspect of the assessment was not formalized during the engagement with the IASEP team, but is an important component of any security assessment methodology. For our purposes, the assets we indirectly identified were the student data being collected and the physical media collecting and storing that data. This definition includes the laptop hardware as well as diskettes used during transmission of data. Additionally encryption keys for unlocking sensitive information are also considered as system assets in need of protection. Furthermore we assumed the remaining standard assets identified in this type of security assessment involving computerized systems. Such assets include equipment and supplies, intellectual property (data and programs), computer services and processes, system memory and CPU (central processing unit), and personnel to name a few.[41]

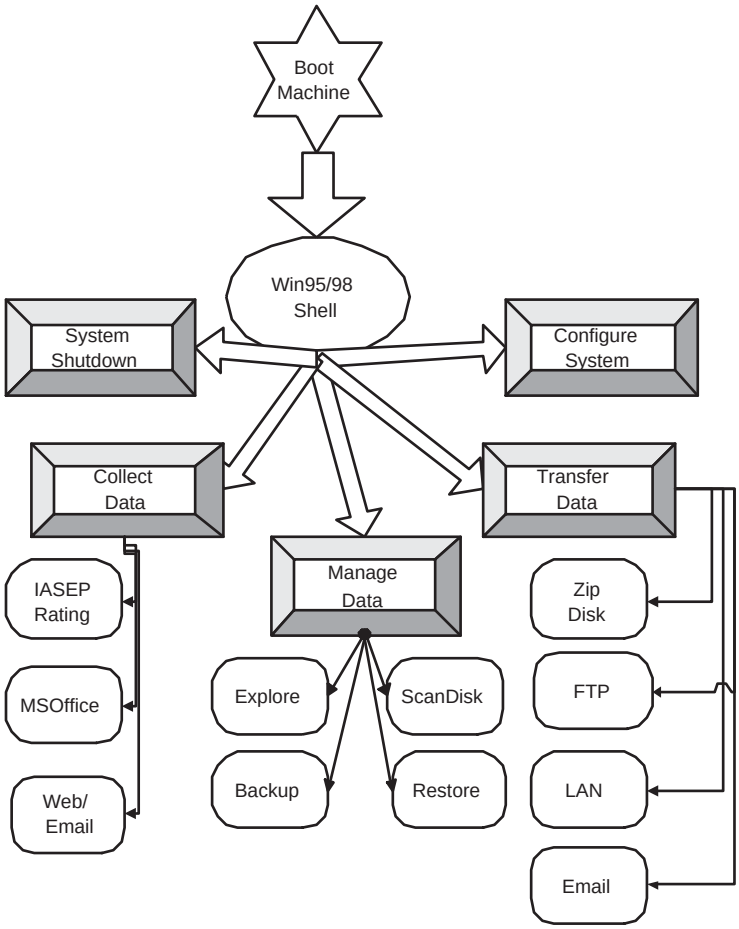

Figure 4.4. IASEP Alternative Data Flow Model

4.5 Threat Analysis

4.5.1 Overview

As we worked with the team we were able to develop a list of real and significant threats to the system that would need to be taken into consideration before final software deployment. Threats can be realized based on accidental occurrences or deliberate system abuse. Accidental situations include natural disasters, extreme temperatures, physical damage, etc. Deliberate malicious activities could include breaking physical security to access a system, or compromising the technical security of the software.[11]

As our threat analysis proceeded we were able to further educate the original project team as well as other stakeholders regarding the need for appropriate protection. Through the threat analysis, we covered the fundamental concerns in security and the vulnerabilities that are faced in a project such as this. Specifically, we had to address issues surrounding Internet access, electronic data storage, and data transmission between administrative entities. The project team understood the threats we envisioned to be a serious matter. This phase of the assessment produced a powerful tool for subsequent adoption of recommendations presented in the security architecture.

4.5.2 The Results

In presenting an initial view of perceived threats to the team, we detected a great amount of apprehension among the developers about the technology that had been produced. We continued to evolve the table of threats and in doing so continued to raise awareness to threats by the developers as they finalized the software.

The actual threat analysis results appear in Appendix B. This analysis categorizes the threats as well as assigns probabilities to occurrence and consequence to each item. Those ratings were based on team discussions of known incidents and current understanding of typical user behavior based on experiences in the pilot deployment. The threat document was then used not only to drive the production of the security architecture, but also in the development of training materials so that the same concerns realized by the developers could be passed along to the end users.

The threats were divided into categories based on the source of the threat. We identified threats related to physical security in the classroom, threats related to vulnerabilities in applications, threats related to vulnerabilities in the operating system, threats related to user error, threats related to network access, and threats related to data transfer as likely areas of concern in the IASEP model.

From those categories, we devised specific examples of the risk involved. For example within threats related to network access, we identified the potential for infection from virus (a form of malicious code which infects other programs by modifying them to include some version of itself [41]) or the introduction of a Trojan horse (a computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiusly exploit the legitimate authorizations [41]) to the system as specific considerations.

4.6 Security Architecture

4.6.1 Overview

A common structure for presenting the security recommendation in an assessment like ours is through the use of a security architecture. A security architecture is abstract by definition, not prescribing specific products and tools, but offering an organized view of secured components in a system. William H. Murray of Deloitte and Touche LLP[33] likens a security architecture to the site plans and blueprints that are used by construction professionals. The architecture is used as a means for coordinating the designers and builders. It permits agreement and acceptance among the parties to avoid future problems. A security architecture serves an analogous purpose. It is used to guide the integration of security controls into the system in such a way that is clearly communicated and understood by all pertinent parties.

4.6.2 Developing the IASEP Security Architecture

The ultimate goal of each of the preceding assessment activities has been to integrate security mechanisms and practices throughout the structure of the IASEP utility. That is the deliverable we have labeled as our security architecture.

Our architecture takes advantage of the structure provided by the process map to identify critical checkpoints in the process flow that will ultimately synthesize with the security needs. Security needs were identified based on the threats accumulated for the project. The level of importance of the threat offered a metric for determining the most important security features to focus on in the project. The resulting architecture is presented in figure 4.5. The creation of such an architecture was easy to accomplish

given the care taken in generating the data flow diagram. Using that model, we were left only with the challenge of mapping threats based on calculated priorities into the architecture. This activity was the primary thrust of the overall assessment.

With a security architecture in place that defined the critical system components, a comprehensive implementation and integration effort could be initiated.

4.6.3 Matching Threats to Security Controls

Within figure 4.2, pointers have been inserted where security controls should be established. This section will provide the rationale for each checkpoint and the corresponding threat(s) it aims to mitigate.

Perhaps the most critical protection for the system is to keep it out of the hands of unauthorized individuals. The primary means of doing so is by use of physical security mechanisms. Example methods of improving physical security include use of hardware locks and storage of the machine in a locked cabinet when not in use. These types of controls aim to prevent machines from being stolen or made available for use other than in the presence of the system owner.

We also recommend using a form of authentication as the system boots up to again ensure it is usable only to a properly identified user. This recommendation is a consequence of threats caused by lack of physical security.

Boot authentication may not always be sufficient. The system owner may leave the system turned on and not monitor it constantly. At this point a different person can take advantage of the system. For this purpose we propose additional system protection measures throughout the security architecture.

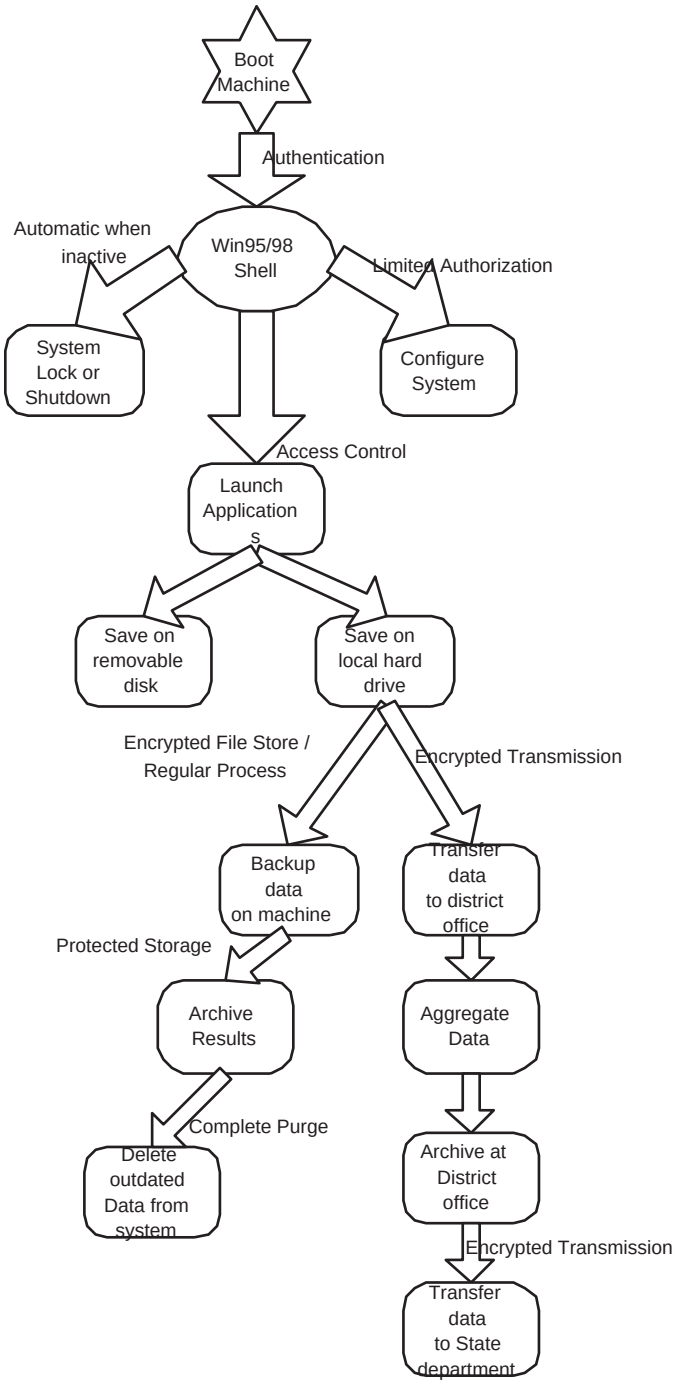

Figure 4.5. IASEP Security Architecture

If a system has been inactive for some period of time – a threshold to be defined by the technical coordinators – it is likely that the authenticated user has walked away from the machine without locking the software. In this event, a password protected screen-saver could automatically be timed to turn on, or the machine could automatically turn itself off. Either occurrence is intended to protect from unauthorized usage while the system owner is away, a solution again designed to mitigate physical security threats.

The limited authorization control(s) are intended to minimize the amount of system mis-configuration resulting from user error. The ability to change system parameters should be restricted to ensure system changes are only issued by an authorized individual (i.e. the technical coordinator during system repair or upgrade).

The most critical software on the system, the IASEP rating program, must provide some amount of access control. Several precautions are in place to ensure only the correct user has access to the machine. The access control(s) implemented at this point are continuing in that line of defense. This control should be a function of the user who has been authenticated to the rating program. This area of the architecture is highlighted to protect from threats enabled by network access. As other applications on the system are launched, there should be additional access control present as defined by the developers.

The remaining security architecture features capture the need to protect the confidentiality of the data being collected and processed by the system. These considerations result from many of the items identified in the application vulnerabilities, the

operating system vulnerabilities, and the data transfer threat categories. Encryption is recommended for files stored on the system as well as on the external media that will be used to submit student evaluation results across administrative domains.

Finally, we recommended that at the end of the school term, the hard drives in the system be completely purged. This control would ensure that if later damage is realized on the system, there is little to no chance of recovering sensitive data on past students by using low level data recovery techniques on the hard disk drive. This is a control that again mitigates threats related to physical security of the machines.

The framing around the security architecture was included to represent the need for overall physical security and virus protection for the system. These are both fundamental precautions to implement for the overall benefit of the architecture.

4.7 Product Recommendations

The recommendations in the security architecture are meaningless without products to implement them. An important component of the security assessment methodology is to present an unbiased collection of potential tools to the team for consideration. The specific utilities we promoted for purchase by the IASEP team included physical locks for the laptops, virus protection, encryption utilities, and optionally an industrial backup package. We were able to accomplish these recommendations by preparing a matrix of potential software options. We presented our findings to the team in the areas of cost, functionality, and features. We reviewed many products including data sheets and demonstration software when available to arrive at realistic information about the products. A significant role played by CERIAS at this stage

of the project has been to interface between product vendors and IASEP project members.

Ultimately the purchasing decision for the best suited package was the responsibility of the project sponsors. The team identified ease of use, reasonable cost, and compatibility with other tools on the system as their criteria for selection. The final decision was made to purchase approximately 1500 licenses for the PGP Desktop Security Suite of products sold by Network Associates. Pretty Good Privacy (PGP) is a utility for public key cryptography. The belief was that ease of use and compatibility would be satisfied with this product given its already widespread use among computer users. The software is sold with a graphical user interface option or with a command line feature. The command line option was a strong selling point for our purpose as it would allow greater flexibility in possible future releases with more of the encryption routines programmed directly into the IASEP software.

Finally, the "suite" of products made the option for improving the IASEP system in the future attractive by providing secured email plugins and VPN capabilities. These features will be investigated further as the transition is made from transmitting data to the school district using Zip disks, as is being currently implemented, to a network based approach.

4.8 Policy Recommendations

With a clearer vision about the security needs of the project along with legal requirements, the need for a clear policy statement could now be addressed. A security policy is a document or a set of documents that spells out responsibilities for the user

surrounding their conduct, privileges and duties. According to [11] it is a set of rules stating what is permitted and what is not permitted in a system during normal operation. It must be embraced throughout a corporation, in our case from the state level all the way through the local school districts and system users. The common components of a security policy include a policy statement, the purpose of the policy, indication of document scope, necessary compliance requirements, and details on how to handle deviations or breakage of policy.

Our first step was to discover the existing policies in use by school corporations and how they related to the needs for IASEP. With the assistance of several stakeholders we were able to obtain copies of various acceptable network use policies [40] used throughout the state as well as the recommendation for policy provided by the Department of Education in Indiana. Each school corporation adopts its own policy, which must be approved by the school board. Upon reviewing many of the established policies, we concluded that most of the policies were based on the State's recommended policy and that they only addressed on acceptable use of the network. Taking this as our starting point and realizing that the IASEP tool would require a policy that encompassed more than network use we developed a list of policy requirements to follow as we set out to generate a policy outline. Those requirements are highlighted in table 4.3.

Our goal during the creation of a new policy for the IASEP application was to ensure we addressed all critical components of the system and how they should and should not be used. The outcome of the security assessment process was to build an outline

Table 4.3
Objectives for the Security Policy

- Meets needs of intended audience. Not exceedingly long.
- Information is properly disseminated.
- High degree of acceptance is achieved.
- Adaptable for use in all corporations and through the lifetime of the technology.
- Meets government requirements (FERPA).

highlighting the top issues for the policy (see Appendix B). That outline was then discussed among the stakeholders and then provided to a legal consultant who would provide the proper policy wording and incorporate our model into the existing school corporation policy styles. The final policy document that will be presented to the school corporations for adoption is a deliverable of the protocol development initiative (see section 2.6).

4.9 Follow-up Activities

There are many activities that should continue to be executed after an initial security assessment. Using our methodology we were able to address a significant number of the security issues uncovered during the assessment. Following the implementation of the recommended controls, periods of review should be scheduled to make necessary modifications and updates to the system to ensure it maintains continued safety for the users.

- Processes that should be run at least annually by the project administrators include a security audit critical components as well as review of the policy.

- Training and communications should be regularly scheduled to keep all users appraised of current trends and vulnerabilities with their system.

- Software upgrades should occur as necessary to patch bugs uncovered in the software or any of the supporting multimedia utilities.

4.10 Delivery Mechanism

The success of our security assessment was realized not only through the enhanced security awareness that grew throughout the IASEP project, but also in our ability to communicate project deliverables easily through Internet based communication mechanisms.

The development of a mailing list and World Wide Web repository, where findings were published and comments shared, helped to keep the entire team informed of updates to material. All of the major deliverables were posted to a World Wide Web site we created. By using the Internet as our delivery tool, we increased the size of our reachable audience. The presence of the security material in web format not only gave improved organization to the overall assessment, but provided interested parties all over the state an opportunity to take part in the process. The existence of the mailing list also helped to facilitate sharing among the team of new ideas in a timely fashion so that milestones could be achieved and shared outside of the monthly status meetings.

Once the deliverables were finalized, their real worth was realized in the training materials that were developed to support the end users of the system. Training sessions focused the user population on the outcomes generated by the assessment both in the threat scenarios presented and the software that was demonstrated.

4.11 Summary of Assessment Results

The results of the security assessment process have appeared in many dimensions. The assessment process has educated all team members about the concepts of security and mechanisms for protection, especially as they apply to education. This occurred by means of regular team meetings where time was spent discussing the concepts of security as they apply to the IASEP software in particular. We have produced deliverable content in HTML format so that the experiences from the assessment can be shared freely among the research community at large. The actual deliverables from the assessment process include a threat analysis for the system, a security architecture, and policy outline.

The threat analysis document has been used to produce training materials and scenario based presentations. After compiling the threats, we then worked to capture the data flow through the system in a "process map" that would enable the whole team to discuss critical function points in the technology and where threats mapped into the system. This process mapping led to the security architecture that was presented to the team as a means of recommending appropriate security controls to mitigate the most dangerous risks. The security architecture was offered to the development team to establish a best practice to be followed to ensure proper protection of the

machines and data. Finally, based on the unique tools, processes, and setting for the project, a policy framework was presented that would address the most critical topics to be later documented formally in a policy statement. Additionally, CERIAS representatives have helped during training sessions in the presentation material in the data security segments.

5. THE ASSESSMENT METHODOLOGY ABSTRACTED

5.1 Overview

The purpose of the previous section was to provide a detailed account of the security assessment that took place on the IASEP project. That engagement can be considered as a specific case study for the general security assessment process we utilized. Our goal for this section is to generalize the security assessment approach so that it can be applied to a broader range of project areas in the future. We will also provide motivation for each recommended phase of the assessment to aid the practitioner in developing a service catered to particular project needs. Our own assessment customizations evolved around the unique requirements, both legal and technical, that are found in educational institutions. One can imagine a plethora of conditions that would necessitate special consideration when engaging some form of security analysis.

Many models have been developed to describe the security assessment process. Often those models are proprietary information for a professional services organization which serve as a key differentiator in their solution offerings. Security assessments are commonly performed by such organizations as a supplemental offering to customers they have already engaged in business. However security assessments should be well understood by the overall technology population. All project teams should

feel empowered to make security conscious decisions given adequate information about performing security assessment activities.

In this section we will outline the fundamental strategy involved in this type of work as well as provide a checklist which we believe to be useful in helping the reader understand the basic techniques.

5.2 High Level Description

From a high-level viewpoint, our security assessment consists of four primary steps. While these activities are generally sequential in priority, there is overlap among the outcomes that are generated. Later in this chapter we will refine our scope of the methodology further to provide more explicit procedures to follow during the assessment.

The first of these four steps involves getting to know the project team, technologies, and processes they are creating. This background check lays the foundation of knowledge that will become the focal point throughout the assessment. Based on this accumulation of information gathered from the team, it is helpful to begin to model the project visually such that there is a consistent view of the way the technology works and how data is manipulated and transferred throughout the system. This is the second phase. The purpose of the visual model is to ensure accurate interpretation of the discussions and ideas among all assessment participants as well as to provide a logical tool for addressing security issues. Independently from building that model, the assessment team will need to document potential threats to the project as phase three. Following the completion of the previous two steps, a security architec-

ture can be designed combining the threats and the system model. The merging of threats and project visualization allows threats to be handled within the most logical locations in the flow diagram. This fourth step of designing the security architecture concludes the final thrust of the assessment. From the architecture additional work can be generated related to policy development and dissemination of the results.

Figure 5.1 provides a conceptualization for the structure and deliverables we followed during this assessment. The outer flow in the figure depicts the activities that were performed while the inner compartments label the deliverables that were produced.

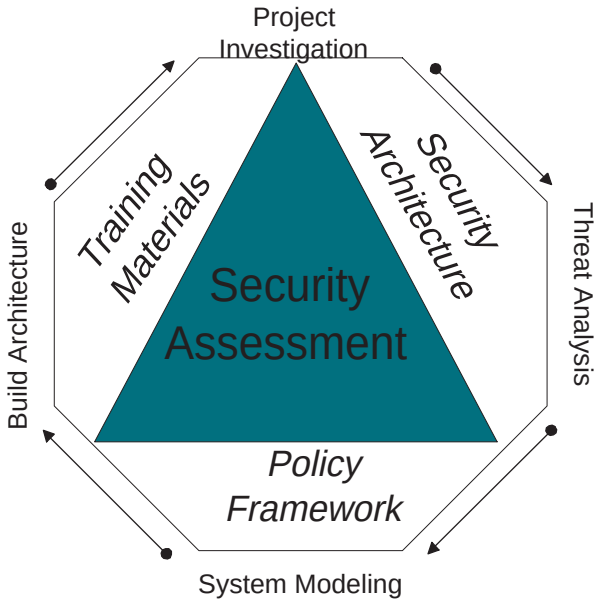

Figure 5.1. A Security Assessment Framework

In the IASEP specific security assessment each step from the figure was executed just once. However, one can imagine situations where several iterations of the cycle may be advantageous.

5.3 Methodology Dissection

The above description provides a very generalized outline of the methodology we developed. It is useful to further detail the effort involved at each phase. Milestones tend to be obvious based on the description of a step, however thorough analysis of the step is critical to ensure individual components are not overlooked. At this point We will expand the definition of each phase to include milestones, deliverables, resources, and specific considerations.

- Get to know the team, their project, their concerns, their expectations, assumptions, and background. This stage could encompass a survey to gain more detailed information plus input from more participants. The respondents can then be interviewed individually in a timely manner to elaborate on information collected in the survey. The motivation here is to ensure a greater chance for success in the final outcomes of the assessment. The goal is to gather as much information as possible so as to avoid making poor assumptions about system operations or sponsor expectations.

- Conduct industry wide research for similar efforts involving the project's technologies, processes, environment, and needs. The motivation for this activity is to learn about current threats and trends relevant to the technology project of

interest. It is here that data can be gathered from various published sources that have focused on a product or process you will be studying during the security assessment.

- Identify assets using a variety of methods. The findings should be well documented and agreed upon by all project participants. The motivation is to avoid wasting time trying to protect system components or data whose value is not worth the cost of protection.

- Formulate threats that effect the project. Threats arise from the technology utilized, application developed, operational environment, user activities. (expand on security requirements to evaluate). The motivation for this step is to steer security controls that will be developed in future phases of the assessment to thwart the real threats to the system. These threats should prioritize the biggest areas for concern, those in need of immediate safeguards.

- Create a visual model of the project if one does not yet exist. This will be used in the development of the security architecture. It also serves to help the team identify other issues in the project as they are better equipped to visualize the system structure. The purpose for this activity is to create an agreed upon representation of the overall system and to emphasize the flows of data through the total system environment.

- Based on the perceived threats (with emphasis on specific probabilities and consequences) begin to insert threat prevention mechanisms into visual model. These will serve as security checkpoints as data flows through the system.

- Determine the most influential / necessary checkpoints (prioritize based on cost / budget, most detrimental risks to prevent, etc.) and make recommendations on implementation along the lines of tools, policy, procedures, etc.

- Document the full deliverable package. Follow-up with critical findings in assessment. This could include assisting in policy generation, training material specific to security, defining higher level security concerns and breaking out as separate effort to solve, etc. Emphasize the importance of dissemination of relevant material so that the effort to secure the system is pro-active and not just an academic exercise.

5.4 Future Work in Methodology Development

There are several areas in security assessment methodology development that are ripe for further research. As an additional phase of the process, one could incorporate usability studies into the recommendation of controls. Research continues in the field of improving usability of security mechanisms, and bringing those ideas into every security assessment performed could provide additional benefit to the project sponsor.

Secondly, one may want to look at ways for formally proving the security specifications are correct. Automated reasoning is an area that has been studied for many years. Incorporating ideas from that research into the realm of a security assessment would offer project sponsors greater sense of value in the recommendations they are offered.

Finally, one might be able to quantitatively analyze the degree to which security requirements are being met by the controls within the security architecture. Providing such measurements would also assist in the proofs of the correctness of the architecture. Further investigation into the methods for quantifying security requirements is needed.

5.5 Summary

The methodology outlined above was developed based on the specific chain of events that occurred in our case study with IASEP. While initially the phases were customized to the actual assessment needs we realized, we believe it can be generalized enough to be helpful in any type of security assessment. The variety of information collected and evaluated at each juncture of the methodology is obtainable in any project scenario. Once a project is assessed in this fashion a more robust understanding of the project scheme can be achieved. This helps not only to make good security decisions, but also helps developers gain a new perspective about their design as a whole. Documentation of anticipated risks becomes available as well as recommendations for mitigating the more critical threats. Most importantly, user acceptance of the final product is likely enhanced by the dedication of the project team to consider security hazards and present competent solutions with the final release.

6. CONCLUSIONS AND LESSONS LEARNED

Our assessment methodology is not unique. However, during our initial research into security assessment methodologies in the literature we discovered that there is a definite lack of structured information. We assume this is because of the often proprietary nature of methodologies, especially among consulting organizations. Additionally, as the security assessment process is generally understood and accepted by the technology community, it is often not the most exciting of research areas for academics to explore. Nevertheless, we felt encouraged by the results of this project and the way it was embraced by the stakeholders involved. The resulting documentation within this thesis is intended to aid future researchers and practitioners through the most significant phases of a security assessment.

6.1 Our Discoveries

No document of this kind would be complete without a look back at the challenges encountered and the lessons we have learned from them. The following is a list of the issues believed to be our greatest hurdles during the course of the security assessment and various suggestions on how to improve the process during subsequent project reviews of this nature.

- Defining and developing a methodology while it is also being utilized can be a blinding experience. We felt disoriented through much of the process. However

we were in essence executing the common stages of an assessment process. While we often felt our approach was haphazard, we enabled ourselves to be guided by the needs and desires of the consumer instead of by a rigid pre-defined process. We believe, looking back, that some amount of blind faith is required of one's abilities to be doing what is best for the customer. By following that intuition, the end result will be well received and likely exhibit greater organization than initially expected.

- We achieved great success in maintaining scope during the course of the project, an achievement that is often overlooked. Granted there are some oversights that are bound to occur in any large undertaking. Examples include miscommunicated assumptions or lack of total user involvement during initial phases. But overall, we were able to keep the security assessment on track. We stayed focused on the system in front of us and the needs of the team as the emerging methodology took shape. We didnot possess a strict assessment model to follow, as such we were focused on the specific needs of the project team. We never felt a need to retrofit this project into an already developed methodology and this allowed us greater agility in providing the best solution possible for the IASEP program

- Along the same principles, we maintained a flexible perspective for suggestions for new approaches to executing a security assessment, as it was a new experience for all parties involved.

- A variety of technical backgrounds was represented among the IASEP team members as well as ultimate system users. Our challenge became one of addressing the security concerns of the engagement while involving the entire audience in discussions that by nature had to maintain a certain degree of technicality. We gained valuable experience in delivering the technical concepts to a less technical audience and allowing everybody to share in the ability to understand and promote security in the technology.

- We were initially uncomfortable with the outcome we were working towards. It was hard for the entire team to articulate a clear statement of expectations prior to progressing through the life-cycle of the security assessment. This circumstance can be avoided in the future with a methodology now in place that aides to drive milestones in the assessment, while being flexible enough to facilitate flexibility in usage as discussed above.

- This effort was long in duration, as we were essentially building our methodology from scratch. In the future, the work load can be shortened slightly using given this overall assessment process that has been better understood and documented

- Timing is an important factor to consider in a security assessment. Effort should be made to ensure the recommended controls can be implemented correctly without last minute tensions that can lead to mistakes. In the IASEP data security assessment, the recommendations were provided early enough so that the security enhanced software was ready for the first major deployment in the Fall of 1999.

- As was discussed in the future work section for IASEP, a security assessment is never complete. The system will continue to evolve and the related security controls and policy will need to evolve with it. While a major change to the system would require a full assessment effort, continued improvements to the baseline model should not require significant changes to the security recommendations. The biggest remaining topic yet to be addressed by the IASEP project team is the migration from data transfer via Zip disks to transfer over a network, perhaps over the public Internet.

6.2 Testimonials of Success

Many people are excited about the work they have seen from the IASEP team and the breakthroughs that have been developing around the security piece of that system. Information security and related topics are new to many educators as they embrace the widely available technologies becoming reality in their institutions. Various testimonials regarding the impact of the security review on the IASEP program have been collected.

Quoting Dr. Deborah Bennett, IASEP Committee Chair, "It has been clear to the IASEP team that educators have not yet acknowledged the problems in securing education data. Our research of current practices across the country suggests that policies and procedures for addressing these issues are scant or nonexistent. CERIAS is currently assisting our research team in creating comprehensive and understandable educational policies for protecting electronic student data and other confidential and

sensitive information. These protocols will have far-reaching impact in the State of Indiana and potentially in other states, as well."

Additionally, Karen Stein, a educator using the system and active participant in the pilot deployment, had these comments. "I feel that the data security portion of program shows teachers, administrators, and parents that we are serious about keeping records secure and that a lot of time and energy was put into making sure that this data will not be exposed to the kinds of threats that are all around us in this age of technology.... The IASEP security team has taken a responsible approach of dealing with security issues before they happen, instead of waiting until something goes wrong."

The IASEP system developer, John Cunningham, stated that "As a result of the input from CERIAS and the data security group, we made substantial changes in the way the IASEP program handled data security issues. We also added a segment of data security training and awareness as part of the regular training for teachers in using the IASEP program."

This collection of comments portrays the value that was realized by selected stakeholders involved in executing the IASEP strategy, particularly focused on the impact of our data security efforts.

6.3 Final Remarks

In short, the experiences gained from seeing the security assessment from creation through completion have been beneficial to everyone involved. Researchers from

CERIAS have learned how to better structure and adapt assessment activities to the situation at hand. We have also learned the value of how to present information related to security such that less experienced individuals can appreciate the techniques and potential hazards related to information technology. In doing so, those individuals are empowered to take full advantage of the recommended safeguards. Purdue has also achieved a tremendous win by integrating the expertise of the newly formed CERIAS center with already established research initiatives throughout the University, such as this one in the School of Education. Most importantly the State of Indiana is now recognized as a leader in the development of new technologies for the classroom which take into practice the wide range of security safeguards that educators require.

APPENDICES

A. CRYPTOGRAPHY TUTORIAL

A fundamental requirement throughout the security architecture built for the IASEP project is confidentiality of student information. The most widely utilized mechanism for enabling confidentiality of data is encryption. The purpose of this tutorial is to provide background information related to basic encryption techniques. Additional resources are noted in section A.4 and in the bibliography if a more extensive study of this field is desired.

A.1 Overview

Cryptography, according to [7], is defined as the art of transforming information to ensure its secrecy or authenticity or both. Cryptanalysis is the art of breaking ciphers. Cryptography is typically presented in terms of the messages it manipulates. The original message is called plaintext or cleartext. After being handled by an encryption algorithm, the resulting message is called ciphertext. The goal of encryption is to encode the contents of a message such that its meaning becomes hidden. The plaintext message can be recovered from the ciphertext using a decryption algorithm. Both algorithms employ the use of keys. A key is a number or other value that is used to mathematically scramble the bits of the message. The length of the key (measured in bits) is a good indicator for the strength of the encryption. The longer the key, the more difficult cryptanlysis becomes.

There are two basic strategies used in cryptography. They are symmetric encryption (also known as secret-key) and asymmetric encryption (also known as public key). Both modes have been widely studied and implemented. Symmetric cryptography uses the same key for encryption and decryption. That key must be a secret shared only by the endpoints of communication. Public key cryptography uses a key pair. One of the keys is held private by the owner of the key pair, while the other key is made public for anybody to use. The requirement in asymmetric cryptography is that the private key cannot be calculated from the public key without great (near-impossible) effort. Public key cryptography is a popular technique for two reasons. First, the requirement for securely sharing a single key among multiple parties is no longer present. Second, public key cryptography is easily used for the digital signature paradigm in addition to data encryption.

A.2 Criteria for Strong Cryptography

There are many points to consider when determining the strength of a cryptosystem. The secrecy of the key to be used should be a dominating principle for the cryptosystem. Relying on secrecy of the algorithm that uses the key is not recommended as a way to improve the strength of the system. A larger key space, as measured by bit length of the key, is also necessary for ensuring the strength of the cryptosystem. The ciphertext that is generated by the cryptographic algorithm should be as random as possible as measured by various statistical tests. All of these factors combine to improve the viability of the cryptography desired and increase resistance to attack.

A.3 Symmetric Key Cryptography

Symmetric key algorithms often fall into a variety of categories. The three primary modes of encrypting data are transposition, where the ciphertext uses the same letters as the plaintext only rearranged; substitution, where different letters are used in the ciphertext that have been derived from the plaintext; and product ciphers, which is a composition of the first two categories. Within each classification one can think of using a block or stream cipher technique. Block ciphers encipher each block of bits with the same key. Stream ciphers encipher a single bit of the message at a time.

Many popular algorithms fall into the realm of symmetric key cryptography. A famous algorithm is DES (the Data Encryption Standard) This algorithm was introduced by IBM and reviewed by the NSA around 1977. It has been used and studied by the best minds in cryptography since that time and has held up well. DES is a block cipher and works in a series of rounds. Other symmetric key ciphers include IDEA, Blowfist, and Skipjack to name a few.

The primary benefit of symmetric key cryptography includes faster performance over public key cryptosystems. A disadvantage of this method is key management. Additionally, this class of cryptography algorithms do not lend themselves to digital signature usage. While finding ways to share a secret key among two parties over a network is challenging, there are protocols that exist to facilitate safe key sharing, for example Diffie Hellman.

A.4 Asymmetric Key Cryptography

The use of public key cryptography is popular for many cryptography purposes, as it can provide authentication, integrity, and non-repudiation in addition to confidentiality.

RSA (Rivest-Shamir-Adleman) is a well-known public key algorithm named after its designers. This algorithm is based on exponentiation in modular arithmetic. Like DES, RSA appeared in the mid-1970s and has been widely implemented since that time. Other algorithms used in public key cryptography include El Gamal, the Diffie Hellman key exchange protocol mentioned above, and Massey-Omura to name a few.

An advantage of public key cryptography is ease in key management. A public key can be distributed on an insecure channel without compromise to the key pair. As noted above, symmetric key algorithms are generally much faster than asymmetric algorithms. In practice the two techniques are used together, so that a public key based algorithm is used to encrypt a randomly generated encryption key (sometimes called a session key). This random key is then used for the encryption of the actual message using a symmetric algorithm.

A.5 Applications of Cryptography

There are many utilities available the make use of the cryptographic techniques described above.

An implementation of the RSA algorithm used by many people is PGP (Pretty Good Privacy). Using this piece of software, each user generates their own key pair then publishes the public key. PGP users can then maintain a key ring of all other

users they plan to communicate with securely. PGP is available on a variety of platforms and provides a straightforward means of encrypting or signing electronic information.

Additional uses of cryptography include electronic contract negotiations, electronic cash implementations, or Kerberos which is an distributed authentication mechanism. There are more uses of cryptography than could be adequately covered in a tutorial of this nature. For further discussion on cryptographic applications refer to the references provided in section A.7 or in the bibliography.

A.6 Attacks on Cryptography

There are many methods used to try to break the code of an enciphered message. These techniques are known as cryptanalysis. The following is a partial list of attack methods.

- Ciphertext-only attack: The attacker only knows the encryption algorithm that was used and the cipher text to be decoded. The attacker has no knowledge about the content of the message, although it is possible to make inferences about the message based on language or communicating parties.

- Known-plaintext attack: This is a situation in which the attacker knows (or can correctly guess) some parts of the plaintext used to produce the ciphertext. The goal is then to decipher the remainder of the message.

- Chosen-plaintext attack: Using this strategy the attacker can provide specific plaintext to the encryption system that is processed with the unknown key.

Having the plaintext and ciphertext combination can aid the attacker in discovering the key.

- Man-in-the-middle attack: This attack occurs when cryptographic communications take place, including key exchange protocols. The attacker is situated between the communicating endpoints in order to passively or actively participate in the communication. This technique is useful if the adversary wishes to communicate as a masqueraded user.

A.7 Specific Cryptography Related Resources

If additional information related to this topic is desired, there are a great many resources available. Applied Cryptography by Bruce Schneirer is a book book containing all of the details of most algorithms and protocols that are known in this field. Cryptography and Data Security by Dorothy Denning is a primer on the mathematical formulations that are at the heart of security. She also provides chapters on many algorithms and usages for cryptography. Practical Unix and Internet Security by Simson Garfinkel and Gene Spafford also has a section on this topic. Most textbooks on security provide at least a chapter or section on the topic of cryptography. These references provide higher level understanding of the field. Finally, the Internet contains a large amount of information related to cryptography and security in general. Many of the fundamental research papers can be found on-line in addition to university course materials and other tutorials.

B. POLICY FRAMEWORK DELIVERABLE

B.1 Security Policy Outline

Topics to be included:

- Policy of the District/State entities
  - Reference Network Acceptable Use policies already in use by corporations
  - Reference Paper records policies
- Policy Purpose
  - Intended Audience
  - How policy will be distributed
- Scope (boundaries of this policy)
  - Technologies it relates to
  - Itemize components of the IASEP system
  - Superceeding policies
- Compliance (how policy exceptions are handled, how to follow policy
  - Periodic review periods
  - Responsibility of all educators (help each other out)

- Consequences of breaking policy
- Relationship of electronic student records to paper files
  - Why this data is to be regarded as sensitive/confidential as others
- User responsibilities
- Physical Security
  - Log-off when not in room
  - Keep laptop locked to furniture if left on desk
  - Lock laptop in cabinet when not in use (after-hours)
- Laptop Usage
  - Primary purpose is testing
  - How other installed applications are to be used
  - Rules on installing personal software (purchased and downloaded)
- Laptop Maintenance
  - Problem detection and reporting
  - Contacting technology department for system maintenance
- Application Access
- Data Access

  - Virus scanner must not be disabled

- Laptop sharing / at home rules
- Internet Access
  - Acceptable Use policy plus special download rules
- Data transfer Procedures
- Backup policy
  - Frequency
  - Rotation of media (using different disks each time and rotating them)
  - Media storage (off-site)
- Protecting student privacy
  - Follow encryption rules
- Legal Issues (FERPA)
- Software copyright
  - Discuss piracy and legalities of licensing
- Addition of new users to system (new teachers hired)
  - Transfer of systems (issues involved)

Policy Objectives:

- Meets needs of intended audience. Not exceedingly long.
- Information is properly disseminated.
- High degree of acceptance is achieved
- Adaptable for use in all corporations and through time
- Meets government requirements (FERPA)

Samples to Reference:

- A Survey of Selected Computer Policies from Institutions of Higher Education (http://www.brown.edu/Research/ Unix_Admin/cuisp/)
- Information Security Policy Guideline(http://spr.das.state.or.us/guidelin/secpol.htm)
- Indiana Department of Education: Recommended Acceptable Network Use Policy (http://www.doe.state.in.us/olr/aup/welcome.html)

C. THREAT ANALYSIS DELIVERABLE

UNDERSTANDING THREATS

What can go wrong during the data flow process?

Table layout

DESCRIPTION in column 1	PROBAB. in column 2	CONSEQ. in column 3

Rating System Guide:

H - High threat of occurring

M - Medium threat of occurring

L - Low threat of occurring

1. Threats because of physical security in classroom

Laptop is stolen. Confidential data is released, the asset is lost, testing is interrupted.	(H)	(H)
Shoulder surfing leads to compromise of system passwords	(L)	(M)
Password Sharing	(H)	(M)

2. Threats because of vulnerability in applications

A vulnerability in the application is discovered after roll-out. A patch would need to be issued and proper instructions on application of the patch or scheduling of trained personnel needs to be done to perform the upgrade.	(L)	(L)
A vulnerability in the overall infrastructure is discovered later in the project.	(L)	(L)
Encryption key is compromised	(L)	(H)
File naming conventions can lead to confusion associating documentation to correct student	(L)	(M)

3. Threats because of vulnerability in operating system

A Windows95 vulnerability is discovered and a service pack is issued	(L)	(L)
Misconfiguration in system leads to unauthorized access	(M)	(M)

4. Threats because of user error

Laptop or data processing machines (servers) become misconfigured in ways that could lead to the machine crashing, or programs are broken. This can occur if anybody other than authorized personnel attempt to troubleshoot the laptop, or non-project related software is used on the system. The overall effect is that work can be lost, time is lost in restoring machine configuration, and data could be lost or damaged in the process.	(H)	(M)
Users try to solve own computer problems, thus changing the standard machine configuration	(H)	(M)
Laptop is used for unintended purposes such as web surfing, or personal software is installed. This can introduce a virus or trojan as mentioned, consumes additional storage space for non-work related material, malicious content could be stored on the machine.	(H)	(L)

5. Threats because of network access

Laptop is trojaned to redirect the collected information. It can be sent to the attacker, or the data can be manipulated.	(L)	(H)
Laptop is infected with a virus. The machine is temporarily unusable, data can be lost, maintenance costs, time to remove virus.	(M)	(M)

6. Threats because of data transfer

Zip disk can become corrupted/damaged in transit. It could be demagnetized, obtain weather damage, media can be torn. If any of the following occur the data on the disk would be lost. The original data needs to be recopied and this delays testing results, and results in the loss of that zip disk as a future resource.	(M)	(L)
Zip disk is lost in transit. It disappears between point A and point B.	(M)	(L)
Data is intercepted in transit. Either the zip disk is stolen and contents read or using the Internet packets can be sniffed.	(L)	(L)

LIST OF REFERENCES

LIST OF REFERENCES

[1] Gene Spafford and Simson Garfinkel. *Practical Unix and Internet Security.* O'Reilly & Associates, Inc, second edition, 1996.

[2] Tomas Olovsson. A Structured Approach to Computer Security. Technical Report 122, Department of Computer Engineering, Chalmers University of Technology Sweden, 1992.

[3] Tom Szuba. *Safeguarding Your Technology.* National Center for Education Statistics, 1998. http://nces.ed.gov.

[4] Bruce Schneier. *Applied Cryptography.* John Wiley and Sons, Inc., second edition, 1996.

[5] Deborah Russell and G.T. Gangemi Sr. *Computer Security Basics.* O'Reilly & Associates, Inc, 1991.

[6] Bradley Lamont. A Guide to Networking A K-12 School District. Master's thesis, University of Illinois, Champagne-Urbana, 1996.

[7] Rita C. Summers. *Secure Computing: Threats and Safeguards.* McGraw-Hill, 1997.

[8] Candace Elliott Person. Electronic educational data security protocol project report, September 1999. Distributed electronically to IASEP stakeholders.

[9] Donn B. Parker. *Fighting Computer Crime: A New Framework for Protecting Information.* John Wiley and Sons, Inc., 1998.

[10] Donn B. Parker. Restating the foundation of information security. In *14th National Computer Security Conference*, volume 2. SRI International, October 1991.

[11] CERIAS and Andersen Consulting. PFIRES: Policy framework for interpreting risk in ecommerce security. Whitepaper on policy frameworks. To appear in SANS2000, 1999.

[12] Deborah E. Bennett, Mel A. Davis, John Cunningham. The development of an alternate assessment system. URL `http://www.soe.purdue.edu/projects/iasep/Papers/AltAssessSystem.htm`, 1999.

[13] Deborah E. Bennett. The development and dissemination of policy and procedures for managing electronic educational data for the State of Indiana. URL `http://www.soe.purdue.edu/projects/iasep/Security/DataControl.htm`, 1999. Statement of Problem.

[14] Stephanie Miller. IASEP December 1998 meeting notes. URL `http://www.cerias.purdue.edu`, December 1998. On project web site.

[15] Stephanie Miller. IASEP Feburary 1999 meeting notes. URL `http://www.cerias.purdue.edu`, Feburary 1999. On project web site.

[16] Stephanie Miller. IASEP April 1999 meeting notes. URL `http://www.cerias.purdue.edu`, Feburary 1999. On project web site.

[17] Stephanie Miller. IASEP July 1999 meeting notes. URL `http://www.cerias.purdue.edu`, July 1999. On project web site.

[18] Stephanie Miller. IASEP protocol October 1999 meeting notes. URL `http://www.cerias.purdue.edu`, October 1999.

[19] James L. Schaub and Ken D. Biery, Jr. *The Ultimate Computer Security Survey.* Butterworth-Heinemann, 1995.

[20] Charles Cresson Wood. *Information Security Policies Made Easy: A Comprehensive Set of Information Security Policies.* Baseline Software, Inc., 1997.

[21] Ernst & Young LLP. 5th Annual Information Security Survey. http://www.ey.com/publicate/aabs/isaapdf/FF0148.pdf, 1997.

[22] Gregory Dalton. Acceptable risks. *Information Week*, pages 36–48, August 1998.

[23] *Family Educational Rights and Privacy Act (FERPA).* 34 C.F.R. Part 99.

[24] B. Fraser. *RFC 2196: Site Security Handbook.* Internet Activities Board, September 1997.

[25] Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278 – 1308, September 1975.

[26] B. Guptill, C. Price, J. Block, G. Lynch, and W. Nicklin. *Creating an Enterprisewide Internet and Intranet Policy.* Gartner Group, September 1996. Strategic Analysis Report.

[27] Richard Power. *Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare.* Computer Security Institute, 1998.

[28] Indiana Department of Education, Division of Special Education. *Informational Packet*, 1999. IASEP training booklet.

[29] Helen H. Arvidson, John N. Cunningham, Melanie A. Davis, and Deborah Bennett. *Program Manual.* Indiana Department of Education, Division of Special Education, 1999. IASEP training booklet.

[30] Indiana Department of Education, Division of Special Education. *Training Tutorial*, 1999. IASEP training booklet.

[31] Authur E. Hutt, Seymour Bosworth, and Douglas B. Hoyt, editors. *Computer Security Handbook.* John Wiley and Sons, third edition, 1995.

[32] Computer Security Institute. *1997 Computer Security Products Buyers Guide*, 1997.

[33] William Hugh Murray, CISSP. Introduction to Security Architecture. In *CSI NetSec '99.* Deloitte and Touche LLP, 1999. Slide presenation.

[34] William Stallings. *Cryptography and Network Security: Principles and Practice.* Prentice Hall, second edition, 1999.

[35] Philip R. Zimmermann. *The Official PGP User's Guide.* MIT Press, 1995.

[36] Terry Bernstein, Anish B. Bhimani, Eugene Schultz, and Carol A. Siegel. *Internet Security for Business.* John Wiley and Sons, 1996.

[37] Frederick C. Mish (editor-in chief). *Merriam Webster's Collegiate Dictionary.* Merriam-Webster, Inc., 1994.

[38] TopSpeed Corporation. Clarion development tool. URL `http://www.topspeed.com`.

[39] Indiana Assessment System of Educational Proficiencies. Building Brighter Futures for Indiana Students: Safeguarding your Students Data, 1999.

[40] Office of Learning Resources Indiana Department of Education. Acceptable Use Policy. http://www.doe.state.in.us/olr/aup/welcome.html.

[41] Dennis Longley and Michael Shain. *Data and Computer Security: Dictionary of standards concepts and terms.* M Stockton Press, 1987.

[42] Mel Davis, Deborah Bennett. Email communications, 1999.

VITA

VITA

Stephanie Miller is a masters student in the Department of Computer Sciences at Purdue University. During her time as a graduate student, she worked as a research assistant in the COAST lab (now CERIAS) on a variety of projects. The topic of this thesis has been a primary focus area for her during that time. Additionally, she has been heavily involved with the creation of a firewall evaluation environment. This project has been the collaborative work of many students and advisors along the way and is concerned with analyzing characteristics of various firewalls in the market today. She has also contributed to the lab's vulnerability database. Over the summer months she was part of a joint effort with Andersen Consulting to develop a framework to address the challenges for policy deployment in today's organizations. The result of that project was a whitepaper that is being used by Andersen consultants, and it will be presented at the SANS2000 conference in Orlando.

During the two years prior to her academic pursuits at Purdue, Ms. Miller was a full-time technical consultant with Hewlett-Packard's professional service organization. While with HP, she was actively engaged on-site at many financial services customers in an assortment of security related projects.

Ms. Miller received High Distinction from Indiana University with a Bachelors of Science degree in Computer Science and a minor in Mathematics. She graduated as the salutatorian from Bloomington North High School in Indiana.