Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2001 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2001

A Study of Public Key Infrastructure Software

Bhavikkumar Shah
Southern University at New Orleans

Kai Koong
Southern University at New Orleans

Lai Liu
Southern University at New Orleans

A STUDY OF PUBLIC KEY INFRASTRUCTURE SOFTWARE

Bhavikkumar U. Shah
Southern University at
New Orleans

Kai S. Koong
Southern University at
New Orleans
kkoong@suno.edu

Lai C. Liu
Southern University at
New Orleans
lliu@suno.edu

Abstract

Most companies use different combinations of technologies such as encryption, firewalls, and passwords to help secure their systems. One new technology in the realm of encryption is known as public-key cryptography. This new tool, commonly called Public Key Infrastructure (PKI), enables computer establishments to authenticate transactions from one system to the other with the use of cryptography. Such an arrangement helps to minimize fraud and accidental access to protected resources of a company. It also helps companies to control which piece of information can be accessed and by whom. However, there are many manufacturers of PKI system, each with common as well as unique task abilities. This study examines selected public key infrastructure software. Specifically this research attempts to identify the different features and essential components contained in PKI software. The result of this study will be useful to the companies involved in e-commerce, security-key providers, encryption writers/regulators and hardware engineers, bankers, insurance agents, health insurance agents and even credit card companies/banks involved in electronic payments.

Introduction

According to the ***Computer Security Institute Annual Report*** covering the period 1996 through 2000, there was an increase in the number of crimes in all categories. These security problems included intentional as well as unintentional access to computer systems by employees and outside perpetrators. Tangible losses incurred by companies and agencies include data, equipment, and money (Kou 1997).

The proliferation of computer crimes and other security problems have resulted in the growth of a major software segment specializing in the detection and prevention of such problems. For home users, most of their problems are central around the occurrences of menaces such as computer viruses, worms, and Trojan horses. Both the Norton Antivirus and McAfee Antivirus are currently common remedies to the home computer security problem. In addition to these two popular software packages, corporate America and governmental agencies are also using other tools such as firewalls and filters as their first line of defense against computer crime problems. Certain business segments are also using industry specific software because certain features in the custom-tailored software may be more effective in securing their computer systems (Levine 2000; Lewis 2000)

A popular encryption application among financial institutions such as banks and investment firms is called Public Key Infrastructure (PKI) software (Marlin 1999). It can take up to twenty-two hours for a relatively skilled hacker to decipher and penetrate a PKI system (Levitt 2000; MacVittie 2000; McKinley 2000). From a Web-based perspective, PKI can be viewed as a collection of Internet technologies that require the management of computer security using public and private keys and digital certificates.

Statement of the Problem

Since the early1990s, many corporations worldwide have devoted a good amount of their investments in electronic commerce technologies and formulated major strategies to compete in the world of online business. In 1999, online commerce attained record interest because companies actually began making profits from Web-based operations (Hussey 1999). Parallel to the growth in the online industry is the increase in the number of computer crimes and problems. According to data collected and analyzed by the Federal Bureau of Investigation, all categories of computer crimes are on the rise. Web-based business systems are venerable targets because viruses, worms and Trojan horses can hinder operations, hackers can cripple networks, and thieves can steal invaluable computer assets and intelligence.

There are many tools available in the market that can be used to protect online systems. PKI is one of the fastest growing security infrastructures available. According to Datamonitor Technology's Global PKI Markets study, PKI will continue to grow over the next four years. By 2003, revenues from PKI sales will reach $1.4 billion worldwide (Armstrong 2000).

A major user problem in the area of PKI deployment is that there are about forty major PKI software vendors worldwide. The first time buyer or novice user of PKI software will most probably encounter hardships with the many choices available. Compounding the problem is the fact that there are different views about essential PKI components (Stender 1998; Robinson 2000)

This lack of standardization and the wide variety of features available in PKI systems can be any decision-maker's nightmare. For a first time buyer, an understanding about essential features can help him or her to better select a basic software package that meets his or her needs. An understanding of essential features can help the more advanced and sophisticated users to better choose among the different alternatives by merely comparing specific limitations or unique added features.

Statement of the Objective

The objective of this research is to identify the major features or components of PKI software. Specifically, this study examines all the features contained in the PKI software of all the major vendors. The types of components contained in the majority of all the PKI software will be classified as primary features. Other common components contained in PKI software will be classified as secondary features. Any component that is contained in a minority of the PKI software will be classified as unique features.

The results of this study should be useful to developers of PKI software, first-time buyers of PKI software, sophisticated users of PKI packages, security-key providers, encryption writers and regulators, cryptography experts, information security analyst, and hardware engineers. Business consultants involved with e-commerce design, law enforcement officers, especially agents working at the Federal Bureau of Investigation and the Central Intelligence Agency, and Internet Service Providers will find the outcomes of this report important. Computer scientists, scholars, educators, and students in the areas of cryptography, authentication, security, and access control will find this study interesting.

Data Gathering

To obtain a list of PKI software packages, an Internet search for developers was conducted using the keywords "PKI," "PKI software," "PKI Solution Providers," "PKI Features," and "PKI Vendors." Forty companies were identified from this initial search. Each of the companies was then examined to determine if they have a PKI software package. Consulting firms, installation providers, and other PKI service providers were removed from the list of companies identified. The number of companies identified to have PKI software packages was found to be 25. To ensure that all the PKI software developers were included in the study, the vendor listing provided in ***SC Magazine*** was also used to verify the identified PKI vendors (Robinson 2000).

The Web sites of the companies identified were visited and information about the PKI software was downloaded from the Web sites. In cases where the information about the PKI software was incomplete or was not available, the vendors were contacted by telephone to obtain the information. Based on the above procedure, information about the PKI products examined in this research was collected from the following sources: product brochures, published information on a specific vendor's Web site, vendor white pages and data sheets about the products, electronic documents provided via email by the company's representative, and verbal information obtained via telephone calls to vendors. The final list of nineteen PKI vendors included in this research is presented in Table 1.

The different PKI software packages available in the market provide a wide range of features. Some of the features are contained in all packages. Others may be contained in a majority of the packages. Some features may exist in selected packages only. A total of 13 features were identified and examined in this research.

Method of Analysis and Presentation

The total number of PKI software having each of the features was first examined and tallied. The percentage of PKI software having each of the features was then computed by taking the total number of observations and dividing it by 19 and multiplying the outcome by 100.

Table 1. List of PKI Vendors and Products

Vendor	Product Name
Baltimore Technologies	Unicert
BCE Emergis	Emergis Security
Celo Communications Inc.	Celocom Pki Manager
Cybersafe	TrustBroker Security Client/Server
Cylink Corporation	Cylink Netauthority™ PKI
E-Lock	Assured PKI
Entegrity Solutions	Entegrity Assureweb
Entrust Technologies Inc.	Entrust/PKI
IBM	Tivoli Secureway
IRE	Safenet/Soft-PK
Microsoft	PKI Software is included in Windows 2000
Network Associates	Net Tools PKI Server (PGP)
Penta Security Systems Inc.	Issac-PKI
RSA Security	RSA Keon
Shiva (Intel)	Shiva Certificate Authority
Smarttrust	Sonera
Spyrus	Spyrus PKI
Verisign	On Site
Xcert International, Inc.	Sentry Ca

The total number of features in each of the software was also examined and tallied. The percentage of features in each PKI software package was calculated by taking the total number of observations and dividing it by 13 and multiplying the outcome by 100. This computation and method was used to examine if all the software have about the same number of features.

Three major tables were used to organize the data collected and analyzed in this research. Two tables were used to show the percentages of features contained in the respective PKI software. The last table was used to show the number of features provided by each software vendor. Features contained in at least 75 percent of all the PKI software packages were classified as primary features. Features contained in less than 50 percent of all the packages were categorized as unique features. The rest of the features were classified as secondary features.

Findings

The initial list of PKI software providers obtained from the Internet search and the ***SC Magazine's*** PKI survey 2000 contained 25 software companies (Robinson 2000). Complete data was obtained from 19 companies and these companies were included in this research study. Despite repeated attempts during a period of three months, six of the companies did not provide the needed information. The six companies were Ashley Laurent, Inc., Computer Associates, Gradkell Systems, Inc., Okiok Data, Rainbow Technologies, and Shym Technology, Inc. With the 19 companies, the percentage of companies represented in the targeted population comes to 76 percent. With the exception of two companies, the rest of the developers are based in seven major states in the United States of America. The majority of the companies are based in California or Massachusetts. The two foreign firms are based in Australia and in Korea.

The respective PKI features were then assigned a corresponding number. These numbers were used because their full text would make the Table too large and may not fit on one page. The numbers were: (1) Certificate Authority, (2) Registration Authority, (3) Certificate Management, (4) Key Backup and Recovery, (5) Revocation System, (6) Non-Repudiation, (7) User Mobility/Authentication, (8) Policy Management, (9) Interoperability, (10) Cross Certification, (11) Auditing, (12) Web Based Administration, and (13) Automatic Certificate Update/Renew.

The features contained in the 19 PKI software examined in this research is presented in Table 2. A summary of the major observations is presented below:

1. Three of the PKI features were found in all the 19 PKI software. The three features were Certificate Authority, Certificate Management, and Non-repudiation.
2. Only one company, Verisign, has all the 13 features examined.
3. Both the foreign companies, Penta Security Systems, Inc. (Korea) and Spyrus (Australia), have10 features.

Table 2. Distribution of Features among Vendors

Vendor	1	2	3	4	5	6	7	8	9	10	11	12	13	Total Features
Baltimore Technologies	X	X	X	X	X	X	X	X	X	X	X	X		12
BCE Emergis	X	X	X	X	X	X	X	X	X	X		X		11
Celo Communications Inc.	X	X	X	X	X	X	X	X	X	X	X	X		12
Cybersafe	X		X	X	X	X	X	X	X	X		X		10
Cylink Corporation	X	X	X		X	X	X	X	X	X	X	X	X	12
E-lock	X	X	X	X	X	X	X			X	X	X	X	11
Entegrity Solutions	X	X	X	X	X	X	X	X	X	X	X	X		12
Entrust Technologies Inc.	X	X	X	X	X	X	X	X	X	X		X	X	12
IBM Corporation	X	X	X		X	X	X	X	X	X	X	X		11
IRE	X		X			X	X	X	X	X		X		8
Microsoft Corporation	X		X	X	X	X	X	X	X	X		X		10
Network associates	X		X	X	X	X	X	X	X	X		X	X	11
Penta Security Systems Inc.	X	X	X		X	X	X	X		X		X	X	10
RSA Security	X	X	X	X	X	X	X	X	X	X		X	X	12
Shiva (Intel)	X		X		X	X	X	X					X	7
Smarttrust	X		X		X	X	X	X	X	X	X	X	X	11
Spyrus	X	X	X	X	X	X		X	X		X	X		10
Verisign	X	X	X	X	X	X	X	X	X	X	X	X	X	13
Xcert International, Inc.	X	X	X		X	X	X	X		X		X	X	10
Total Vendors	19	13	19	12	18	19	18	18	15	17	9	18	10	

The percentage of PKI vendors having a specific feature is presented in Table 3. Nine features can be classified as primary or critical features. Some major observations are presented below:

1. All 100 percent of the vendors provided the three features Certification Authority, Certificate Management, and Non-Repudiation.
2. About 94.7 percent of the vendors provided the four features Policy management/support, Revocation System, User Mobility/Authentication, and Web-based administration.
3. Some 89.4 percent of the vendors provided the feature Cross Certification.
4. About 78.95 percent of the vendors provided the feature Interoperability.

Three features can be classified as secondary features. The three features and their corresponding percentages in descending order are Registration Authority (68.42%), Key backup and Recovery (63.16%) and Automatic Certificate Update/Renew (52.63%). Finally, only one feature, auditing, can be classified as a unique feature. About 47 percent of the PKI software have this feature.

Table 3. Percentage Distribution of Vendors

Number	Feature	Number of Vendors Providing this Feature (out of 19)	Percentage (%)
1	Certification Authority	19	100.00
2	Registration Authority	13	68.42
3	Certificate Management	19	100.00
4	Key Backup And Recovery	12	63.16
5	Revocation System	18	94.74
6	Non-Repudiation	19	100.00
7	User Mobility/Authentication	18	94.74
8	Policy Management/Support	18	94.74
9	Interoperability	15	78.95
10	Cross Certification	17	89.47
11	Auditing Feature	9	47.37
12	Web-Based Administration	18	94.74
13	Automatic Certificate Update/Renew	10	52.63

Information about the number of features contained in each of the PKI software was presented in Table 4. Of the 19 PKI software examined in this research, only one company has 100 percent of all the features. Using the 80 percent criterion established in this study, seven of the companies failed to make the cut. A summary of the percentages and the names of companies that made the 80 percent criteria set forth in this research are presented below:

1. Verisign was the only company that provided 100 percent of the features.

2. Six companies provided about 92.31 percent of the features. They are Baltimore Technologies, Celo Communications, Inc., Cylink Corporation, Entegrity Solutions, Entrust Technologies, Inc., and RSA Security.

3. Five companies provided about 84.62 percent of the features. They are BCE Emergis, E-Lock, IBM, Network Associates, and Smarttrust.

The companies that have less than 80 percent of the 13 features are Cybersafe, IRE, Microsoft, Penta Security Systems, Inc., Shiva (Intel), Spyrus, and Xcert International, Inc. Both the foreign vendors (Penta Security Systems, Inc. and Spyrus) fallinto this category. Intel is the company that made the PKI software with the least number of protection features.

Summary and Conclusions

In conclusion, this study found that the features of PKI software could be classified into three broad categories. There are nine primary features, three secondary features, and one unique feature. Even though there are 19 PKI software examined, the number of features contained in the software can vary widely. Some can have 100 percent of all the features. On the other hand, some vendors can offer only about half of the features identified.

From a managerial perspective, security managers and corporate consultants can use the results of this study as a reference tool to enhance their purchase decisions as well as training programs. For example, first time buyers of PKI software now can use this study to guide their purchase decisions. Sophisticated users can use the results here to better understand the features offered by the many vendors. For security trainers, the three broad categories can be used as a framework for developing cost-effective and user-friendly training curriculum. Novice users, for instance, may start with the primary functions and advance to secondary features and niche components as they mature in their abilities to use the application.

Table 4. Numbers of Features Provided by Vendor

Vendor	Number of Features Provided (Out of 13)	Percentage of Listed Features (%)
Baltimore Technologies	12	92.31
BCE Emergis	11	84.62
Celo Communications Inc.	12	92.31
Cybersafe	10	76.92
Cylink Corporation	12	92.31
E-Lock	11	84.62
Entegrity Solutions	12	92.31
Entrust Technologies Inc.	12	92.31
IBM	11	84.62
IRE	8	61.54
Microsoft	10	76.92
Network Associates	11	84.62
Penta Security Systems Inc.	10	76.92
RSA Security	12	92.31
Shiva (Intel)	7	53.85
Smarttrust	11	84.62
Spyrus	10	76.92
Verisign	13	100.00
Xcert International, Inc.	10	76.92

Software engineers and systems developers of PKI solutions can evaluate their existing products against the checklist provided in this study. The results can help them to determine their competitive position and what features, if any, should be added to their products.

References

Armstrong, I. "PKI: Has it Truly Arrived yet?" SC Magazine(11), August 2000, p. 24.

Hussey, P. "PKI Security in the New Extranet Marketplace," Computer Technology Review(19), October 1999, pp. 14-16.

Kou, W. *Networking Security and Standard,* Norwell, Massachusetts: Kluwer Academic Publishers, 1997.

Levine, D. E. "Public Key Infrastructure Adds Security to E-Business," Information Week(747), May 22,2000, pp. 94-100.

Levitt, J. "What is Public Key Infrastructure?" Information Week(771), January 31,2000, p. 82.

Lewis, J. "Maturing PKI Products will Take Center Stage in E-Business Strategy," Internet Week(799), February 7, 2000, p. 29.

MacVittie, L. "Buyer's Guide: Desktop Encryption," Network Computing(11), September 4, 2000, pp. 106-108.

McKinley, B. "The ABCs of PKI," Network World(17), January 17, 2000, pp. 55-56.

Robinson, P. "Market Survey PKI," SC Magazine(21), February 2000, pp. 32-38.

Stender, T. J. "Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective," Case Western Reserve Journal of International Law(30), 1998, pp. 287-337.