PUBLIC KEY INFRASTRUCTURE (PKI) AND VIRTUAL PRIVATE NETWORK (VPN) COMPARED USING AN UTILITY FUNCTION AND THE ANALYTIC HIERARCHY PROCESS (AHP)

A THESIS PRESENTED TO THE FACULTY OF THE DEPARTMENT OF ECONOMICS VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY ON APRIL 22, 2002 AT THE NORTHERN VIRGINIA GRADUATE CENTER, FALLS CHURCH, VA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF ARTS

KEYWORDS: UTILITY FUNCTION, AHP, VPN, PKI

By
Edward D. Wagner,
CCNA, MCP

Dr. Roger Waud, Chair
Dr. Tom Lutton
Dr. Richard P. Theroux

Abstract

This paper compares two technologies, Public Key Infrastructure (PKI) and Virtual Private Network (VPN). PKI and VPN are two approaches currently in use to resolve the problem of securing data in computer networks. Making this comparison difficult is the lack of available data. Additionally, an organization will make their decision based on circumstances unique to their information security needs. Therefore, this paper will illustrate a method using a utility function and the Analytic Hierarchy Process (AHP) to determine which technology is better under a hypothetical set of circumstances. This paper will explain each technology, establish parameters for a hypothetical comparison, and discuss the capabilities and limitations of both technologies.

Dedication

No work of this level is completed alone. The professors of the department showed great patience and insightful guidance, however there are others that need to be recognized. My wife, Katrina, provided constant loving support and was key to my success. My children, Kaitlyn, Teddy, and Addison, missed bedtime stories and playtime with me, so I could complete this thesis. William and Dana Bloom reviewed drafts, made comments and cheered me along my way. But most of all, Jesus Christ through whom all things are possible and is perfect in my weakness.

T A B L E   O F   C O N T E N T S

L I S T   O F   T A B L E S

L I S T   O F   F I G U R E S

LIST OF EQUATIONS

1.0   Introduction

This paper compares two technologies, Public Key Infrastructure (PKI) and Virtual Private Network (VPN). PKI and VPN are two approaches currently in use to resolve the problem of securing data in computer networks. Making this comparison difficult is the lack of available data. Additionally, an organization will make their decision based on circumstances unique to their information security needs. Therefore, this paper will illustrate a method using a utility function and the Analytic Hierarchy Process (AHP) to determine which technology is better under a hypothetical set of circumstances. This paper will explain each technology, establish parameters for a hypothetical comparison, and discuss the capabilities and limitations of both technologies.

To understand the importance of this comparison, we must determine the scope of the problem and identify a set of possible solutions. The problem of securing information and computer networks has become more important as organizations increase their dependence on networks. Figure 1 illustrates the increase in the number of attempts to penetrate the integrity of networks. In 1997, the Computer Emergency Response Team (CERT) Coordination Center (CERT/CC) at Carnegie Mellon reported over 2,000 security incidents. The number rose to over 8,000 in 1999,[1] and to over 20,000 in 2000.[2]

Figure 1. Computer Incidents Reported to CERT/CC [3]

---
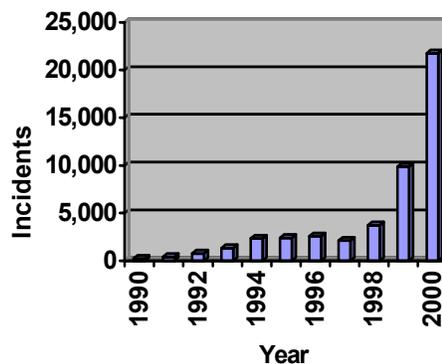
[1] *Braithwaite, Timothy, "Understanding Network Security Monitoring and Intrusion Response (NSMIR),"April 17, 2001, Tech Republic ,p2*

[2] *Carnegie Mellon Software Engineering Institute," CERT/CC Statistics 1988-2001," http://www.cert.org/stats/cert_stats.html, October15, 2001*

[3] *Ibid 2*

These incidents often have a profound impact on an organization. For a government agency, it can be the loss of secret or sensitive information as well as a tarnished image. For a commercial firm there is a need to protect information which they consider propriety in nature. Firms wish to avoid the loss of communication with customers and suppliers because this can translate into lower revenues and increased costs. In every event there is an increased labor and material cost to repair the damage. When computer networks go down, customers often delay or reconsider purchases. One survey found the average cost to respond to an incident was over $250,000.[4] Many people have touted PKI as the solution to all security problems. But the slow adoption of PKI in the market place has made people wonder about its viability. Others have adopted the use of VPN.

2.0   Evaluation of Criteria

When an organization selects a security product, they usually select the security product minimizing the chance for penetration of their computer networks. The organization wants to select the technology that will maximize their utility for information security. Organizations have constraints such as budgetary limits that they must balance with their desire to maximize utility.

This analysis of the two options uses a utility function to determine which option is preferable, given the set of criteria. A utility function is a mathematical representation of a firm's preferences. The utility function we will use is based on eight criteria. We will assign relative value to each technology for each criterion based on the logic presented in the Relative Value Logic section. The relative value represents the rank of the technology compared to the other technology. The relative value two (2) is assigned to the preferred technology. The value one and one half (1.5) indicates no preference or the two options are equal by that criterion. The value one (1) is assigned to the technology not preferred. In addition to the relative value, we will assign weights to each criterion. To determine the weights, we will use the Analytic Hierarchy Process (AHP). In this

paper we will do a comparative analysis of the criteria to determine weights for the utility function. The result is a utility function based on a weighted sum of relative values.

$$MAX\sum(W_i)\,(RV_i) = (W_1)(RV_1) + (W_2)(RV_2) + (W_3)(RV_3) + \ldots + (W_n)(RV_n)$$

s.t. Constraints

Where: RV_i = Relative Value of each technology of the

i^{th} = Evaluation Criterion

W_i = Weight of the ith Evaluation Criterion

We will evaluate the data by using a linear equation for each technology, PKI or VPN, and then compare the results:

Equation 1. Utility of PKI

$$Utility\,_{PKI} = (W_1)(RV_1) + (W_2)(RV_2) + (W_3)(RV_3) + \ldots + (W_n)(RV_n) \qquad [1]$$

Equation 2. Utility of VPN

$$Utility\,_{VPN} = (W_1)(RV_1) + (W_2)(RV_2) + (W_3)(RV_3) + \ldots + (W_n)(RV_n) \qquad [2]$$

3.0   Assumptions and Constraints

For the purpose of comparison, this paper will compare the two technologies in a hypothetical establishment of remote access for 10,000 users equipped with laptops. The users will need access on their laptops to applications contained within the Local Area Network (LAN). The applications will do functions such as time and expense reporting. Both fictitious deployments use the security device, firewall, and similar network hardware in order to make the comparison as fair as possible. Since both scenarios require a local dial up connection to the network, this cost is not included in the analysis. To ensure greater comparability, the description of costs for PKI and VPN are based on the Government Services Administration (GSA) pricing schedule. Other differences and assumptions will be apparent in the discussion of each technology.

---

[4] *Ibid 1*

4.0   Market Penetration

In Forrester Research's survey of authentication methods, the slow market penetration of PKI is illustrated as shown in Figure 2. Frank Prince found in the 1999 survey of 50 Global 2,500 companies that 2% of firms were using digital certificates. [5]   Digital certificates are a component of PKI technology.

The same survey done in 2000 found that 24% of the firms had adopted digital certificates. Given the increase hacker activity and the promise of secure networks by PKI, many computer security experts expected greater penetration. According to Prince, once companies started implementing PKI, the problems associated with it became apparent to the industry. The result was less adoption than had been expected. For organizations to implement PKI they must see a real possibility of a return on their investment. Complicated deployments run the risk of unexpected costs.

Figure 2. Certificate Usage [6]

---
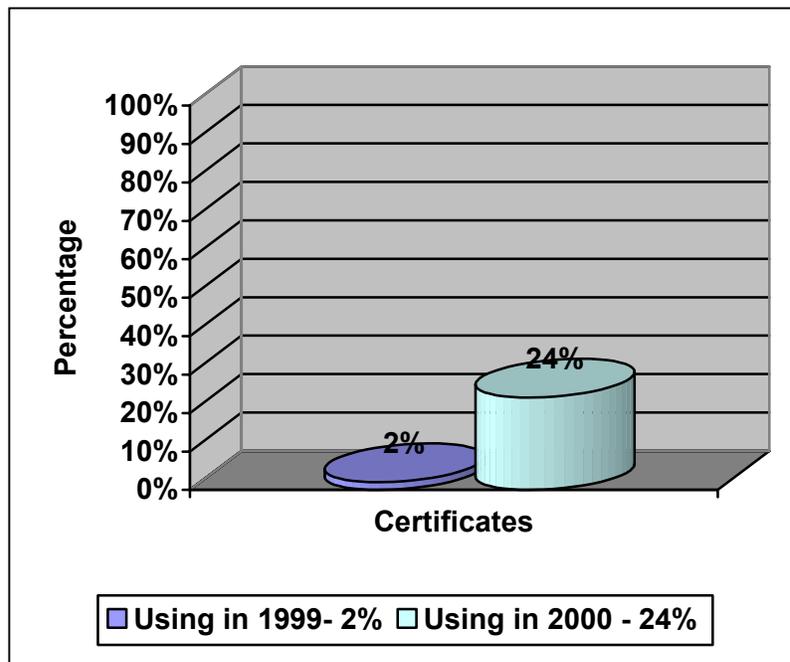
[5]*Prince, Frank, Buss, Christian, and Howe, Carl D., "Biometrics' Bubble Burst," November 28, 2000, Forrester Research, Inc*

[6] *Ibid 5*

In the Computer Security Institute's "2001 CSI/FBI Computer Crime Survey," respondents report which security measures they are using. In Figure 3 practically all the reporting organizations use one of the most popular security measures, access control, firewall, anti-virus software, and/or physical security. Other measures are used at varying levels.

Figure 3. Percentage of Security Measures [7]
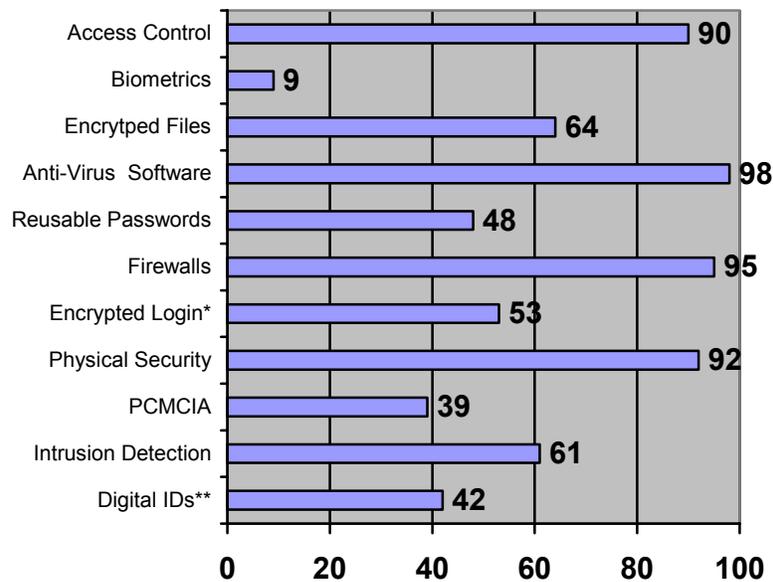
*VPN is described as Encrypted Login

** PKI is described as Digital IDs

According to the survey, PKI technology is used by 42 percent of system administrators and 53 percent use VPNs. A fact to consider is that security measures are often used in combinations. So it is possible for the security measures in Figure 3 to be compliments

---

[7] *Computer Security Institute, "2001 CSI/FBI Computer Crime Survey," spring 2001*
    http://www.gocsi.com/

or substitutes depending on the computer system environment and the information security needs of the organization. By combining security technologies, the computers systems become more secure. The percentage usage of PKI in Figure 3 (42%) differs from that noted in Figure 2 (24%). The nature of the participants in the two surveys can account for the difference. The CSI/FBI survey in Figure 3 is conducted from a boarder population of participants. Figure 2 is a more focused group of 50 Global firms. For the purpose of this analysis, we will isolate our comparison to VPN used in combination with a firewall and PKI used in combination with a firewall. So PKI and VPN are described as substitutes in our comparison.

5.0   *Components of Public Key Infrastructure*

A trustworthy networking environment can be established by using PKI. This environment is created through the use of digital certificates based on encryption using mathematical algorithms. The sophistication of the algorithm prevents "brute force attacks." A brute force attack occurs when a person uses computer systems to gain the encrypted result without the use of the algorithm. The algorithms available for use include Digital Encryption System (DES), Triple DES, and, the newest algorithm, Advanced Encryption System (AES).

The information can only be made readable when a user with a matching algorithm receives the encrypted data and de-crypts it. To match up the encryption algorithm, a system of keys is established. Each user has a pair of "keys," which are actually digital representations of very large numbers. PKI uses special digitally signed messages (called "certificates") to connect a user's identity to his or her public keys. A digital certificate is issued by a trusted "Certification Authority" (CA) and signed using that CA's private signature key. Registration Authorities (RA) can also verify certificates and reduce the burden on one CA. This scalability is important in large organizations. To validate the CA's signature on one user's certificate, the other user must first know the public key of the first user's CA. The user always knows the public key of at least one CA that is trusted.

Figure 4. Conceptual Configuration
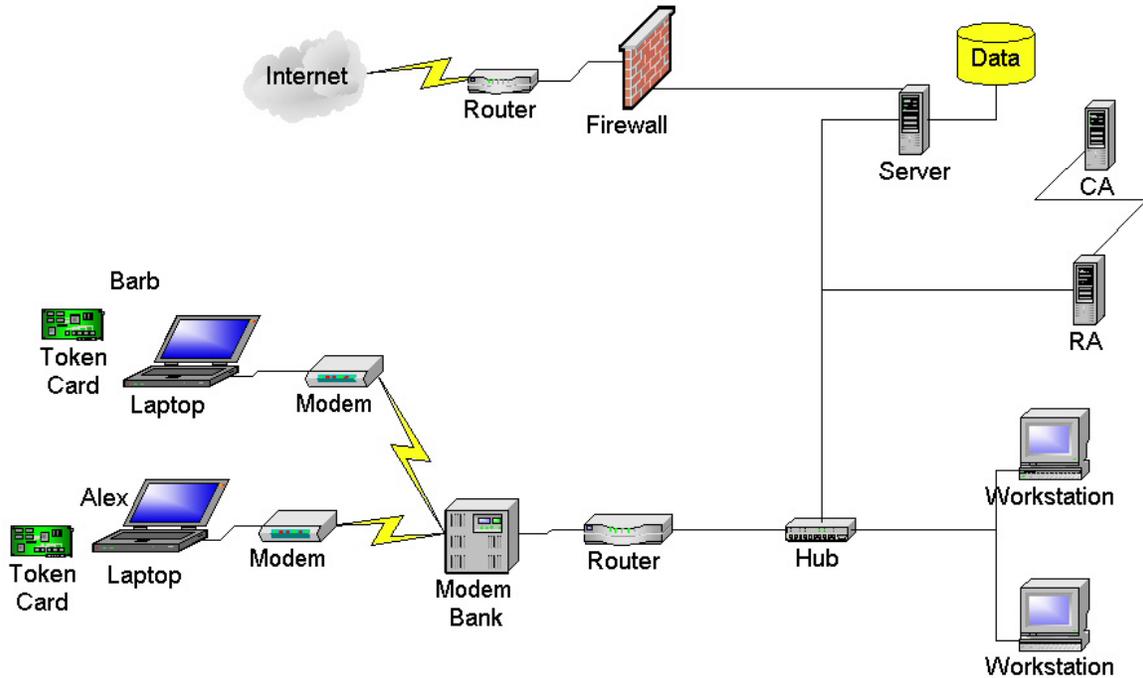
Figure 4 depicts the relationship between the different parts in a PKI access control method into a Local Area Network (LAN). It is a conceptual diagram, not a configuration, to support 10,000 users. A user must gain access in order to share information or access data within the LAN. The access control method depicted is PKI. PKI can become infinitely more complicated than this, but it will always have the requirement to share something in common. PKI uses a CA to provide digital certificates connecting the identity of an individual to his or her public keys (An individual may have more than one public key). Another component is the RA; the RA may be used to certify the individual's identity to the CA so that the CA will issue a digital certificate. A

subscriber will use the following steps to become an authorized user with remote access:[8]

- A key pair containing a public and private component is generated,

- The user gives the RA proof of identity and a copy of the public key,

- The user registers at the RA, possibly physically signing a registration form,

- After verifying the identity of the individual requesting a digital certificate, the RA tells the CA to issue the digital certificate binding the subscriber's public key to his or her identity,

- The CA places the certificate in a public database, called a repository, which may hold certificates issued by many CAs, and

- When a user, Alex, needs to communicate with another user, Barb, Alex obtains Barb's certificate containing his public key from a repository. Barb's certificate is signed using the private signature key of the CA. Alex then verifies the CA's signature on Barb's digital certificate using the CA's public key, and recovers Barb's public key.

The CA prevents intermediaries from intercepting and substituting keys passed between users because each new exchange must be validated using a public key issued by the CA and encrypted using its algorithm.

The use of this key system allows messages or transactions to be authenticated or encrypted using one of the user's keys. Then the information can only be verified or decrypted using the user's other key. Thus, when a user uses his private signature key to sign an electronic message or other transaction digitally, anyone who knows his or her corresponding public key can verify his or her signature. A similar method using public key technology can be used to encrypt messages for confidentiality as they transit an open network such as the Internet. If a key becomes compromised, then it can be revoked. Each key has a limited life after which it is then void.

---

[8]*Lyons-Burke, Kathy, "Federal Agency Use of Public Key Technology for Digital Signatures and Authentication," October 2000 National Institute of Standards & Technology (NIST) Special Publication 800-25*

Digital Signatures are used like written signatures on a document except digital signatures exist in a digital format. Their purpose is to verify a person's identity and specify the date and time of a message. Digital signatures offer the feature of non-repudiation on transactions, which has significant economic implications because it documents the date of a transaction and the parties involved.

PKI typically uses a token card or smart card with a card reader to verify identity of the user. Biometric devices use a reader to scan the fingerprints or the iris of the user to enable access. Smart Cards come in various forms; most are physical cards used with a reader to give you access to the information secured by the PKI system. Biometric devices can be used in conjunction with or instead of a smart card system. The access method for the user is a critical vulnerability point. Many computer attacks take advantage of weak access methods.

6.0   Components of Virtual Private Network

In the Virtual Private Network, a user dials remotely to gain access into a LAN. In the hypothetical configuration depicted in Figure 5, the user gains access through the VPN device instead of going through the firewall. To get authentication, the user dials up the modem bank and is prompted to login just as the user might login to any other network. The authentication method used is RADIUS, which is a VPN protocol. A protocol is simply a list of steps, which must be followed between computer systems. RADIUS is an encryption protocol, which ensures the data passing from computers within the local area network and the laptop is encrypted. This encryption of data traffic allows access through modems, as in this example, but it also can create an encrypted tunnel or access through a public network like the Internet.

Figure 5. VPN Components
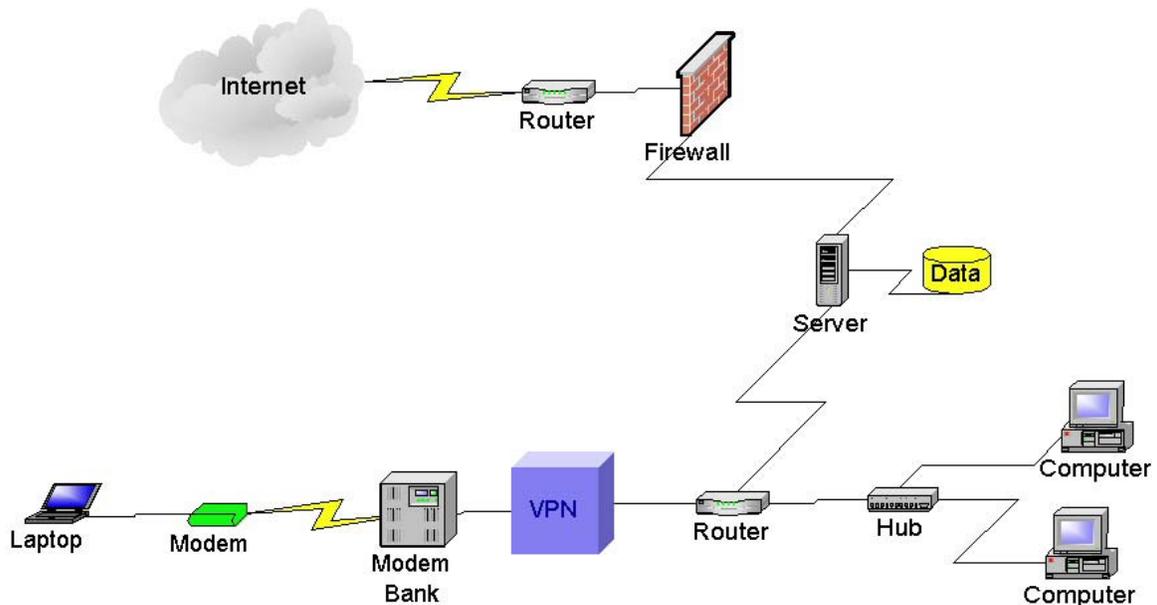
Normally, the user account is established and maintained on a database stored on a server within the LAN. One central database can be established for authentication. An example of this is a Lightweight Directory Access Protocol (LDAP) server, which stores users and their passwords for authentication to the network as well as to applications.

7.0   Public Key Infrastructure Costs

The Federal Government has adopted PKI. As a result many government agencies have implemented PKI. With the passage of the Government Paperwork Elimination Act (GPEA) (1998), and Electronic Signature in Global and National Commerce (E-SIGN) Act (2000), government agencies are strongly encouraged to implement electronic systems to replace paper based systems. The GPEA requires government agencies to find ways to replace paper-based systems with electronic-based systems in the agencies' interactions with the public. The E-SIGN act gives digital signatures the same weight as traditional paper signatures. This has resulted in many agencies scrambling to implement electronic-based programs. Often, these programs require a strong level of security, or the program itself introduces electronic transactions requiring a digital signature.

To understand the comparison of the two technologies, the reader must understand different components that make up the implementation of each technology. Using the hypothetical implementation discussed in Section 3.0 Assumptions and Constraints, this paper will outline the cost to implement PKI. In the next section we will discuss the same elements of cost for VPN.

PKI provides proper authentication of users into the local area network and any applications needed by the authorized user. PKI can even provide access control to applications within the network. So, in our scenario PKI can enable access to the network and then to the time and expense reporting applications.

Table 1. Cost Estimate of PKI Solution with Smart Cards[9]

Item	Unit Cost	Quantity	Total Cost
Cost of Tokens	$15	10,000	$150,000
Cost of Network Readers	$75	10,000	$750,000
Cost of Building Access Readers	$200	1,000	$200,000
Cost of Infrastructure	$200,000		$200,000
Cost of Issuing Certificates	$125,000		$125,000
Total			$1,425,000

Table 1 lists the costs for our hypothetical PKI deployment to 10,000 users using smart card technology. While there are multiple costs in Table 1, they can be classified into two categories: fixed and variable costs. The cost of the infrastructure and issuing certificates are fixed. Issuing certificates describe the general support required to enable distribution of certificates. These costs include planning and program management costs.

---

[9] *Booz- Allen and Hamilton "CIO PKI/Smart Card Project Approach for Business Case Analysis of Using PKI on Smart Card for Government Wide Applications," Washington, D.C. December 1, 2000*

In order to issue certificates, measures must be taken to ensure identities of the users can be verified and the system can be deemed reliable. The cost of tokens, network readers, and building access readers are variable depending on the number of users. This cost estimate does not include the additional cost of staff turnover. In any organization of 10,000 persons the number does not remain static. The higher the turnover rate, the higher the cost in tokens. Each token or smart card is estimated to cost $15. This problem also exists for the cost of issuing certificates. Certificates are unique to the individual. Therefore, the loss of an employee and the replacement of that employee will also impact the $125,000 estimate.

8.0   Virtual Private Network Costs

PKI is complex and requires integration with the network operating system. VPN is a simpler implementation. The VPN device grants access to users outside the network. The database contains the list of users and their passwords. In my comparison of PKI and VPN, both technologies require improvements to the network infrastructure. These additions are necessary to enable additional traffic from an outside source. Table 1 and Table 2, includes these costs in "Cost of Infrastructure." For the VPN implementation, these costs include the VPN devices, an LDAP server, and the networking infrastructure. Additional routers are required to direct the network traffic. The estimate in Table 2 is for an organization with 10,000 users just as in the example with PKI in Table 1.

Table 2. VPN Cost

Item	Unit Cost	Total Cost
Cost of Infrastructure	$98,000	$98,000
Cost of Software Licenses	$505,000	$505,000
Support	$5,000	$5,000
Total		$608,000

When comparing PKI and VPN, user turnover is an important consideration. Every new user has to be issued a new certificate with PKI. Therefore, if a user leaves and a new one joins the organization, a new certificate has to be issued, and the old certificate has to be revoked. With VPN, each user works under a software license. The license is not unique to the individual and can be reused. Therefore, if there is a 10% turnover of the users of PKI smart cards, it will cost an additional $15,000. VPN is not subject to such cost.

9.0   *Description of Criteria*

To determine the preferred technology in our hypothetical scenario we will consider eight areas for evaluation. Each of the options will be compared against these criteria. The eight areas of consideration are:

Non-Repudiation - The ability to document a transaction. The transaction date and parties involved are documented, so participants cannot deny their involvement in the transaction.

Interoperability - The ability of systems to provide services to and accept services from other systems and to use the services to operate effectively.

Authentication - Verification of the user's identity at logon.

Data Integrity - The reliability of data passing through the system. Concerns include data tampering or inconsistent availability.

Confidentiality - Ensures that information (e.g., customer data and intellectual property) is not disclosed to unauthorized persons, processes, or devices. Confidentiality is especially important when considering medical data or financial information.

Scalability - How well a hardware or software system can adapt to increased demands.

Portability – How the system allows for people to carry large amounts of pertinent information and equipment needed to gain access.

Efficiency – Minimizing the time and cost added by the security product. If a security product makes the information secure but adds large amounts of time, it may result in an unacceptable cost.

When comparing the two options relative to one another, it is important to measure specifically, how each option is ranked relative to the other according to each criterion. In Equations 3 and 4 we re-write our Utility Equations to incorporate each criteria defined above:

Equation 3. Utility Equation - PKI

$$\text{Utility }_{PKI} = W_1R+W_2A+W_3D+W_4C+W_5S+W_6T+W_7I+W_8E \qquad [3]$$

Equation 4. Utility Equation - VPN

$$\text{Utility }_{VPN} = W_1R+W_2A+W_3D+W_4C+W_5S+W_6T+W_7I+W_8E \qquad [4]$$

Where:

Non-repudiation = R

Authentication = A

Data integrity = D

Confidentiality = C

Scalability = S

Portability = T

Interoperability = I

Efficiency = E

10.0   Methodology using Analytical Hierarchy Process

Given Equations 3 and 4, we will use the Analytical Hierarchy Process (AHP) authored by Thomas A. Saaty, to compute weighting of the criteria and find the utility value of VPN and PKI in our comparison.[10]   The AHP provides a mathematical process to input subjective and personal preferences of an individual making a subjective decision.[11] Thomas Saaty's explanations of the use of matrix algebra and Eigenvectors in AHP are found in Appendix A. Saaty's concept of using Eigenvectors is not unique. Anthony J. Pettofrezzo in "Matrices and Transformations," says there are many applications of matrix algebra in mathematics, physics and engineering.[12]   So Saaty has taken a useful mathematical tool and applied it to decision making.

Saaty says there are three principles when conducting problem solving. They are the principles of decomposition, comparative judgments, and synthesis of priorities.[13]   We see this in the methodology used in the AHP. We have already decomposed the problem by identifying and defining our criteria in the Description of Criteria section. Later we will compare all the criteria and make subjective judgments based on logic presented in Section 11.0, Pairwise Comparison Matrix Logic, to form a pairwise comparison matrix. Then using the Eigenvector method we will be able to synthesize these pairwise comparisons into a criteria weighting.

Let us define the parameters of the elements used in the development of the pairwise comparison matrix. We say that $\mathcal{A}$ is the finite set of n elements called alternatives, or for our examination, criteria. Next, we say C is the set of attributes or properties of these

---

[10] *Saaty, Thomas A, "How to Make a Decision: The Analytical Hierarchy Process" Interfaces 24: 6, pp19-43, November-December 1994*

[11] *Saaty, Thomas A, "The Seven Pillars Of The Analytic Hierarchy Process" ISAHP Proceedings, Kobe 1999*

[12] *Pettofrezzo, Anthony J., "Matrices and Transformations" Dover Publications, Inc., New York, N.Y.,1966 p86*

[13] *Saaty, Thomas A., "Axiomatic Foundation of the Analytic Hierarchy Process," Management Science, Vol.32 No. 7, July 1986, p841*

criteria.[14]   A physical example is $\mathcal{A}$ being a set of rocks and C being the set of weights for the rocks. Each element of $\mathcal{A}$ represents a comparison. This comparison can be described as a binary comparison. Further we will say >c represents more preferred according to the property and ~c represents indifferent to according to the property of C. Moreover:

> "Every pair $(A_i, A_j) \in \mathcal{A}X\mathcal{A}$ can be assigned a positive real number $Pc(A_i, A_j) = a_{ij}$ that represents the relative intensity with which an individual perceives a property $C \in \mathbb{C}$ in an element $A_i \in \mathcal{A}$ in relation to other $A_j \in \mathcal{A}$:

> $A_i > cA_j$ if and only if $Pc(A_i,A_j) > 1$
> $A_i \sim cA_j$ if and only if $Pc(A_i,A_j) = 1$

> Reciprocal Condition. Given alternatives $(A_i, A_j) \in \mathcal{A}X\mathcal{A}$ the intensity of preference of A_i over A_j is inversely related to the intensity of preference of A_j over A_i:

> $Pc(A_i,A_j) = 1/Pc(A_j,A_i), \quad \forall A_i,A_j \in \mathcal{A} \quad C \in \mathbb{C}$"[15]

Therefore, the pairwise comparison matrix will compare each criterion to every other criterion on the 1 to 9 ratio scale in Table 3. The comparison will generate cell values in a square matrix $\mathcal{A}$.

---

[14] *Harker, Patrick T., and Vargas, Luis G., "The Theory of Ratio Scale Estimation: Saaty's Analytic Hierarchy Process," Management Science, Vol. 33, No. 11, November 1987 p1384*

[15] *Ibid 14 p1385*

Table 3. Comparison Scale [16]

Value	Preference
1	Equal
3	Slightly favored
5	Favored
7	Strongly favored
9	Extremely favored
2,4,6,8	Compromise between the above values

Given these definitions we can now let $Pc(A_j, A_i)$ denote how we compare *j* to *i*. So that when comparing criteria a to b, where a is strongly favored to b, then $Pc(a, b)=7$. $Pc(b, a)$ is simply the reciprocal of $Pc(a, b)$. This relationship is shown in Equation 5:

Equation 5. Pairwise Comparison Reciprocal Relationship

$$Pc(b,a) = \frac{1}{Pc(a,b)} \qquad [5]$$

Since each criterion is of equal importance to itself, the diagonal in the pairwise comparison matrix is filled with (1)s. For example, if $Pc(a, b)=x$, $Pc(a, c)=y$ and $Pc(b, c)=z$ then a pairwise comparison matrix would be constructed as shown below.

$$\begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{ccc} a & b & c \\ \begin{bmatrix} 1 & x & y \\ \dfrac{1}{x} & 1 & z \\ \dfrac{1}{y} & \dfrac{1}{z} & 1 \end{bmatrix} \end{array}$$

---

[16] *Saaty, Thomas A, "How to Make a Decision: The Analytical Hierarchy Process" Interfaces 24: 6, pp19-43, November-December 1994, p43*

The example of a pairwise comparison matrix above gives us a set $\mathcal{A}$ and the elements which are the comparisons come from the set C.

After we have inputted the subjective values of our pairwise comparison matrix we will apply the Eigenvector method to determine our criteria weights, W_i in equations [3] and [4]. The Eigenvector method takes the information $Pc(A_i,A_j)$ for all $A_i,A_j \in \mathcal{A}$ and creates the set of weights W_i for all $A_i \in \mathcal{A}$, further that $a_{ij} \equiv Pc(A_i,A_j)$. The mapping Pc is said to be consistent if $a_{ij}a_{jk}=a_{ik}$.[17]

It is important to use consistent logic when inputting the cell values of the pairwise comparison matrix. Some inconsistency is to be expected in developing a pairwise comparison using judgmental methods. However, inconsistency outside an acceptable boundary will result in calling into question our conclusions. Sugden, the author of "Why be Consistent? A Critical Analysis of Consistency Requirements in Choice Theory," says,

> "Consistency conditions are imposed on choice functions as a means of ruling out patterns of choice that are held to be irrational…In many theories of choice the most fundamental concept is not the choice function but the notion of preference, interpreted as a binary relation *R* on the set *X*, where *xRy* is read as '*x* is at least preferred as *y*'…Consistency conditions are then formulated which place restrictions on the form of the relation R and which require certain kinds of correspondence between the choice function and the preference relation."[18]

In constructing the pairwise comparison matrix *n* x *n* cells wide the actual number of comparisons performed in AHP is *n (n – 1) / 2*.[19] In comparisons where the *n* value is small the number of comparisons is also small. However, where the *n* value increases the number of comparisons increase. As each criterion is compared more often the

---

[17] *Saaty, Thomas A., "Axiomatic Foundation of the Analytic Hierarchy Process," Management Science, Vol.32 No. 7, July 1986, p845*

[18] *Sugden, Robert, "Why be Consistent? A Critical Analysis of Consistency Requirements in Choice Theory," Economica, New Series, Vol. 52, Issue 206, May 1985*

[19] *Shepperd, Martin and Cartwright, Michelle, "Predicting with Sparse Data," Empirical Software Engineering Research Group School of Design, Engineering & Computing, Bournemouth University, Talbot Campus, Poole, UK August 14, 2000 p4*

possibility of a single erroneous judgment impacting the final estimate decreases. For example, in our comparison of PKI and VPN we have 8 criteria so there are 28 comparisons. Also, we have a way to measure these judgments for errors, the calculation of a consistency index (CI). The CI is calculated thus:

Equation 6. Consistency Index[20]

$$CI = (\lambda_{max} - n)/(n - 1) \qquad [6]$$

Where:

λ_{max} is the largest eigenvalue of the pairwise comparison matrix.

n is the order number

As the CI approaches zero the more consistent the judgments.[21] This CI can be compared to that of a Random Index (RI), which is the average CI of randomly generated matrices of the same order. The ratio derived is termed the Consistency Ratio (CR).

Equation 7. Consistency Ratio[22].

$$CR = \frac{CI}{RI} \qquad [7]$$

Where:

CI is the consistency index from Equation 6

RI is the appropriate random index from Table 4

---

[20] *Saaty, Thomas A., "Axiomatic Foundation of the Analytic Hierarchy Process," Management Science, Vol.32 No. 7, July 1986, p850*

[21] *Saaty, Thomas A, "How to Make a Decision: The Analytical Hierarchy Process" Interfaces 24: 6, November-December 1994, p28*

[22] *Dodd, F. J., Donegan, H. A., McMaster, T. B. M., "Reassessment of Consistency Criteria in Judgment Matrices," Statistician, Vol. 44, Issue 1, 1995 p33*

Random Index Values

Table 4. Random Index [23]

N	RI
2	0.00
3	.52
4	.89
5	1.11
6	1.25
7	1.35
8	1.40

Where:

     N is the number of Criteria

     RI is the Random Index value

If this CR fails to reach a required level then answers to comparisons may be re-examined. Saaty established a CR threshold of 5% for a 3x3 matrix, 8% for a 4x4 matrix, and 10% for a matrix 5x5 or larger for consistency by examining the distributions of sample sets of matrices for each order.[24]

We will calculate the CR for two examples to provide a better context to our discussion of consistency. An example of a logic error or inconsistent logic in the series of relationships would be like saying A>B>C and then going on to say C>A. We can input a series of similar judgments into a pairwise comparison as show in Table 5. The first row of numbers in Table 5 compares the A criterion to each criterion.

---

[23] *Ibid 10*

[24] *Dodd, F. J., Donegan, H. A., McMaster, T. B. M., "Reassessment of Consistency Criteria in Judgment Matrices," Statistician, Vol. 44, Issue 1, 1995, p36*

The 1 compares A to A. The 7 compares A to B. So A is strongly favored over B. Also, this row is shows that A is equal to C. In the next row notice the 7 shows B is strongly favored to C. This series of relationships is inconsistent. If A is strongly favored to B then B cannot be strongly favored to C, because A is equal to C.

Table 5. Example of a Logic Error

	A	B	C
A	1	7	1
B	.143	1	7
C	1	.143	1

Given the pairwise comparison in Table 4, we estimate the criteria weights W_i by taking the Eigenvector of the pairwise comparison matrix. The Eigenvector of the pairwise comparison matrix are the criteria weights W_i. To calculate the Eigenvector, each cell in the matrix is divided by its column sum. For example, the sum of the first column in (1+0.143+1) is equal to 2.143. We divide each number in the column by 2.143 (1÷2.143=0.467, 0.143÷2.143=0.067, 1÷2.143=0.467). This is repeated for each column. The result is the normalized matrix. The row averages in the normalized matrix provide an approximation of the Eigenvector of the pairwise comparison matrix. Each element of this Eigenvector approximation is the criterion weight W_i for each evaluation criterion, RV_i in equation [1].

Normalized Comparison and Criterion Weights

$$
\begin{array}{ccc}
\overline{NormalizedComparision} & & \overline{CriterionWeights, W_i} \\
0.467 \quad 0.860 \quad 0.111 & & 0.479 \; forRV_A \\
0.067 \quad 0.123 \quad 0.778 & & 0.322 \; forRV_B \\
0.467 \quad 0.018 \quad 0.111 & & 0.198 \; forRV_C
\end{array}
$$

To test for consistency, a matrix product is calculated by multiplying the criterion weight column and the original pairwise comparison matrix array, Table 5. The first numbers in the matrix product is [(0.479x1)+(0.322x7)+(0.198x1)]= 2.935. The rest of the matrix is

completed in a similar fashion. Then each product is divided by the criteria weights. For A, we divide 2.935 by 0.479 to determine the eigenvalue 6.124.

Step 1.

$$\begin{bmatrix} 1 & 7 & 1 \\ 0.143 & 1 & 7 \\ 1 & 0.143 & 1 \end{bmatrix} \times \begin{bmatrix} 0.479 \\ 0.322 \\ 0.198 \end{bmatrix} = \begin{bmatrix} 2.935 \\ 1.780 \\ 0.724 \end{bmatrix}$$

Step 2.

$$2.935 \div 0.479 = 6.124$$
$$1.780 \div 0.322 = 5.521$$
$$0.724 \div 0.198 = 3.647$$

To determine the CI, we must determine the maximum eigenvalue calculated above, 6.124. This value will be called λ_{max}. Then, we will recall the number of criteria (3), and call it n. With these numbers in hand we recall Equation 6.[25]

Consistency Index

$$CI = \frac{\lambda_{max} - n}{n-1}$$

$$CI = \frac{6.124 - 3}{3 - 1} = 1.562$$

After computing the consistency index, we estimate a consistency ratio. The consistency ratio is the consistency index divided by the random index as noted in Equation 7. The random index values are listed in Table 4.

---

[25] *Saaty, Thomas A., "Axiomatic Foundation of the Analytic Hierarchy Process," Management Science, Vol.32 No. 7, July 1986, p850*

The consistency ratio of the pairwise comparison in Table 5 where we concluded we had a logic error in series of relationships between A, B, and C is 3.004. This is greater than the 0.05 threshold noted by Saaty and shows a high degree of inconsistency.

Consistency Ratio

$$CR = \frac{CI}{RI}$$

$$CR = \frac{1.562}{0.50} = 3.004$$

Given an example of an inconsistent pairwise comparison, lets look at a more consistent pairwise comparison. In this case, A is slightly favored over B, B is slightly favored over C, and A is strongly favored over C.

Table 6. Example of Consistent Logic

	A	B	C
A	1	3	7
B	.33	1	3
C	.143	.33	1

Normalized Comparison and Criterion Weights

$$
\begin{array}{ccc}
\overline{NormalizedComparision} & & \overline{CriterionWeights} \\
\end{array}
$$

$NormalizedComparision$			$CriterionWeights$
0.677	0.692	0.636	0.669
0.226	0.231	0.273	0.243
0.097	0.077	0.091	0.088

Step 1.

$$
\begin{bmatrix} 1 & 3 & 7 \\ 0.33 & 1 & 3 \\ 0.20 & 0.33 & 1 \end{bmatrix} \times \begin{bmatrix} 0.669 \\ 0.243 \\ 0.088 \end{bmatrix} = \begin{bmatrix} 2.835 \\ 1.077 \\ 0.374 \end{bmatrix}
$$

Step 2.

$$2.835 \div 0.669 = 3.014$$
$$1.077 \div 0.243 = 3.005$$
$$0.374 \div 0.088 = 3.002$$

Consistency Index

$$CI = \frac{\lambda_{max} - n}{n - 1}$$

$$CI = \frac{3.014 - 3}{3 - 1} = 0.00697$$

Consistency Ratio

$$CR = \frac{CI}{RI}$$

$$CR = \frac{0.00697}{0.58} = 0.012$$

In this second example we intuitively understand that if A is slightly favored over B, B is slightly favored over C, and A is strongly favored over C, we have a is consistent series of relationships. In this pairwise comparison the CR is 0.012. It is well below the 0.05 threshold observed by Saaty. Therefore, we can be confident it has a high degree of consistency.

Given the scenario stated in Section 3.0, Assumptions and Constraints, each criterion is compared to the other criteria. We can create a pairwise comparison matrix for our analysis of PKI and VPN in Table 7. The following is an example of how to read Table 7:

- Non-Repudiation is slightly favored over Interoperability,
- Non-Repudiation is strongly favored over Efficiency listed in the last column,
- Authentication is slightly favored over Data Integrity,
- Portability is slightly favored over Efficiency.

Table 7. Pairwise Comparison Matrix

	Non-repudiation	Interoperability	Authentication	Data Integrity	Confidentiality	Scalability	Portability	Efficiency
Non-repudiation	1	3	3	5	5	5	7	7
Interoperability	0.333	1	2	3	3	5	5	7
Authentication	0.333	0.5	1	3	3	3	5	5
Data Integrity	0.2	0.333	0.333	1	2	3	3	5
Confidentiality	0.2	0.333	0.333	0.5	1	2	3	3
Scalability	0.2	0.2	0.333	0.333	0.5	1	3	3
Portability	0.143	0.2	0.2	0.333	0.333	0.333	1	3
Efficiency	0.143	0.143	0.2	0.2	0.333	0.333	0.333	1

1 is equal

3 is slightly favored

5 is favored

7 is strongly favored

11.0   Pairwise Comparison Matrix Logic

The values inputted into Table 7 are based on the Assumptions and Constraints presented in Section 3, and the logic in the following section. A decision maker in an organization with different parameters will likely input the values in Table 7 differently. The purpose of this paper is to present a useful method given a set of parameters. Given the nature of information security products, no result is applicable to every situation. To understand the logic used in this paper, the following section describes the comparison of Non-Repudiation to each criterion.

Non-repudiation versus Interoperability - Non-Repudiation is slightly favored. Given our scenario, Non-Repudiation can facilitate electronic transactions, such as submitting time and expense reports. Interoperability relates only to the complexity of interacting with time reporting and expense applications. Non-Repudiation provides the basis for such a transaction and, therefore, is more important.

Non-Repudiation versus Authentication - Non-Repudiation is slightly favored. Non–Repudiation gives the ability to audit transactions, while authentication simply verifies a user at logon. Since Non-Repudiation is harder to achieve it is more valuable to a security product.

Non-Repudiation versus Data Integrity - Non-Repudiation is favored. Data Integrity refers to the veracity of data sent across a network. Simple encryption can create a high certainty as to the veracity of the data. Non-Repudiation certifies the time, date, and author of a transaction. The benefits of certifying each transaction are more valuable, therefore, Non-Repudiation is more significant.

Non-Repudiation versus Confidentiality - Non-repudiation is favored. Confidentiality allows users to send sensitive data like time reporting or financial information without a third party being able to intercept it. Confidentiality is not as difficult to achieve or valuable as a benefit to security measures as Non-Repudiation.

Non-Repudiation versus Scalability - Non-repudiation is favored. Scalability is the ability to expand the system to accommodate more users. Scalability has long-term implications, but is not considered important in the short term. Non-Repudiation is important in the long and short term.

Non-Repudiation versus Portability - Non-Repudiation is strongly favored. Portability is the ability to transport equipment required to function tasks in our scenario. Since the users are using remote access laptops, the security equipment needs to be transported. While this is convenient, Non-Repudiation is more central to the issue of information security.

Non-Repudiation versus Efficiency - Non-Repudiation is strongly favored. The security product should work efficiently and minimize any additional time required to conduct work. This is another convenient feature, but not nearly as significant as the importance of Non-Repudiation.

The remaining pairwise comparisons listed in the Table 7 are consistent with the ratings of Non-Repudiation to each criterion we have discussed.

Now we proceed following the same steps as in our 3x3 example above. Given the pairwise comparison in Table 7, we estimate the Eigenvector to determine criteria weighting. To calculate the Eigenvector, each cell in the matrix is divided by its column sum. For example, the sum of the first column of our pairwise comparison matrix in Table 7 (1+0.333+0.333+0.2+0.2+0.2+0.143+0.143) is equal to 2.552. We divide each number in the column by 2.552 (1÷2.552=0.392, 0.333÷2.552=0.131, 0.333÷2.552=0.131, etc.). This is repeated for each column. The result is the normalized matrix Table 8.

Table 8. Normalized Comparison and Criterion Weights

	Non-repudiation	Interoperability	Authentication	Data Integrity	Confidentiality	Scalability	Portability	Efficiency	Criterion Weight
Non-repudiation	0.392	0.525	0.405	0.374	0.330	0.254	0.256	0.206	0.343
Interoperability	0.131	0.175	0.270	0.224	0.198	0.254	0.183	0.206	0.205
Authentication	0.131	0.088	0.135	0.224	0.198	0.153	0.183	0.147	0.157
Data integrity	0.078	0.058	0.045	0.075	0.132	0.153	0.110	0.147	0.100
Confidentiality	0.078	0.058	0.045	0.037	0.066	0.102	0.110	0.088	0.073
Scalability	0.078	0.035	0.045	0.025	0.033	0.051	0.110	0.088	0.058
Portability	0.056	0.035	0.027	0.025	0.022	0.017	0.037	0.088	0.038
Efficiency	0.056	0.025	0.027	0.015	0.022	0.017	0.012	0.029	0.025

The row averages provide an approximation of the Eigenvector of the pairwise comparison matrix. This approximation gives the criterion weight W_i for each evaluation criterion. The result is shown in the last column of Table 8 with the heading criterion weight. These weights are reflective of the inputs from the pairwise comparison.

Next we will test our comparison for consistency. A matrix product is calculated by multiplying the criterion weight column from Table 8 and the original pairwise comparison matrix of Table 7.

$$
\begin{bmatrix}
1 & 3 & 3 & 5 & 5 & 5 & 7 & 7 \\
.33 & 1 & 2 & 3 & 3 & 5 & 5 & 7 \\
.33 & .5 & 1 & 3 & 3 & 3 & 5 & 5 \\
.2 & .33 & .33 & 1 & 2 & 3 & 3 & 5 \\
.2 & .33 & .33 & .5 & 1 & 2 & 3 & 3 \\
.2 & .2 & .33 & .33 & .5 & 1 & 3 & 3 \\
.143 & .2 & .2 & .33 & .33 & .33 & 1 & 3 \\
.143 & .143 & .2 & .2 & .33 & .33 & .33 & 1
\end{bmatrix}
\times
\begin{bmatrix}
0.343 \\
0.205 \\
0.157 \\
0.100 \\
0.073 \\
0.058 \\
0.038 \\
0.025
\end{bmatrix}
=
\begin{bmatrix}
3.031 \\
1.813 \\
1.386 \\
0.852 \\
0.620 \\
0.481 \\
0.313 \\
0.212
\end{bmatrix}
$$

Then each product is divided by the criteria weights to give the eigenvector.

$$
\begin{array}{rcccl}
3.031 & \div & 0.343 & = & 8.843 \\
1.813 & \div & 0.205 & = & 8.837 \\
1.386 & \div & 0.157 & = & 8.813 \\
0.852 & \div & 0.100 & = & 8.543 \\
0.620 & \div & 0.073 & = & 8.481 \\
0.481 & \div & 0.058 & = & 8.277 \\
0.313 & \div & 0.038 & = & 8.167 \\
0.212 & \div & 0.025 & = & 8.320
\end{array}
$$

In the illustration above, the numbers are rounded to 3 decimal places. The λ_{max} value

from the division of the matrix product by the criteria weights is 8.843. The consistency index, Equation 6, is:

$$CI = \frac{\lambda_{max} - n}{n - 1}$$

$$CI = \frac{8.843 - 8}{8 - 1} = 0.120$$

After computing the consistency index, we estimate the consistency ratio, the consistency index divided by the random index, Equation 7. The random index represents the consistency of a randomly generated pairwise comparison matrix. The random index values are listed in Table 4.

$$CR = \frac{CI}{RI}$$

$$CR = \frac{0.120}{1.40} = .086$$

According to Saaty a CR below 0.10 in our pairwise comparison matrix is evidence of an acceptable degree of consistency.

Table 9. Resulting Weighting From Pairwise Comparison

Criteria	Weight
Non-repudiation	0.343
Interoperability	0.205
Authentication	0.157
Data integrity	0.100
Confidentiality	0.073
Scalability	0.058
Portability	0.038
Efficiency	0.025

Consistency ratio = 0.086

Table 9 lists the weights from Table 8 for each criterion resulting from the pairwise comparison. The Eigenvector method enables determination of weighting. Substituting these weights into Equations [1] and [2] we have.

$$\text{Utility}_{PKI} = 0.343R + 0.205A + 0.157D + 0.100C + 0.073S + 0.058T + 0.038I + 0.025E$$

$$\text{Utility}_{VPN} = 0.343R + 0.205A + 0.157D + 0.100C + 0.073S + 0.058T + 0.038I + 0.025E$$

12.0   Relative Value Logic

Given the scenario stated in Section 3.0, Assumptions and Constraints, we can now determine the relative values for our evaluation of VPN and PKI. These are subjective judgments based on the following arguments.

Non-Repudiation – PKI exhibits non-repudiation on transactions through the use of Digital Signatures. A VPN system can date stamp a transaction through an application, but there is no legal standing for such a system. PKI's digital signatures provide a way to certify a transaction, which has legal standing. – **Preference PKI (relative value 2), VPN not preferred (relative value 1)**

Interoperability – PKI interacts with more components and applications within the LAN than VPN. This greater interaction complicates the implementation of PKI. VPN does not need to interact with the applications and components of the LAN. Therefore, its simplicity makes it less intrusive and more interoperable. – **Preference VPN (relative value 2), PKI not preferred (relative value 1)**

Authentication – PKI provides a more reliable method. Given the parameters set in this evaluation, VPN uses a simple username and password. PKI uses two-factor authentication. It requires possession of a physical object and knowledge of a password. These requirements make PKI more secure. – **Preference PKI (relative value 2), VPN not preferred (relative value 1)**

Data Integrity – Both options provide encryption of data. For the scope of this evaluation we will only compare the two options via the use of encryption. Both options

use encryption, therefore they compare equally. Because they both use encryption, a third party cannot modify the data without the recipient recognizing the result immediately. Therefore encryption is very useful in making data secure. – **Equal Preference Each option has a relative value of 1.5**

Confidentiality – Because both options encrypt the data, they both make the data unreadable by a third party. Thus anyone trying to intercept a data transmission would not be able to read it. Therefore, sensitive data such as customer data and intellectual property cannot be read without access to the encryption process. Both options make use of encryption so they are rated equally. – **Equal Preference Each option has a relative value of 1.5**

Scalability – VPN is less intrusive and interacts less with components and applications of the Local Area Network (LAN). This makes expansion of the system easier. To expand PKI, more certificates must be managed and additional RA servers must be added to the network. Therefore expanding from 10,000 users to 20,000 users would be a lot easier with a VPN system. – **Preference VPN (relative value 2), PKI not preferred (relative value 1)**

Portability – Because the PKI system requires additional equipment, the smart card and the card reader, it becomes less portable. If the user forgets, misplaces or has a problem with the equipment, then their access is not possible. No authentication can take place. VPN with fewer components is less likely to have a problem. – **Preference VPN (relative value 2), PKI not preferred (relative value 1)**

Efficiency – VPN's implementation is less intrusive. In our scenario, VPN uses a LDAP server to store usernames and passwords, which is highly compatible with other applications. VPN's simplicity makes it more efficient. – **Preference VPN (relative value 2), PKI not preferred (relative value 1)**

Table 10. Utility Matrix on Relative Criteria

	Non-repudiation	Interoperability	Authentication	Data integrity	Confidentiality	Scalability	Portability	Efficiency	Total
Weights	0.343	0.205	0.157	0.100	0.073	0.058	0.038	0.025	
PKI	2	1	2	1.5	1.5	1	1	1	1.586
VPN	1	2	1	1.5	1.5	2	2	2	1.413

- Note: Consistency ratio = 0.086

The relative values discussed in the Evaluation of Criteria section are listed for each criterion in Table 10. Using the utility equation and inputting the relative value and weight for each criterion, we obtain the total values listed in the last column. The results show that PKI is preferred since 1.586 is higher than VPN's 1.413. In the weighting, Non-Repudiation is the most important factor with its weight of 0.343.

Figure 6. Utility vs. Cost Diagram
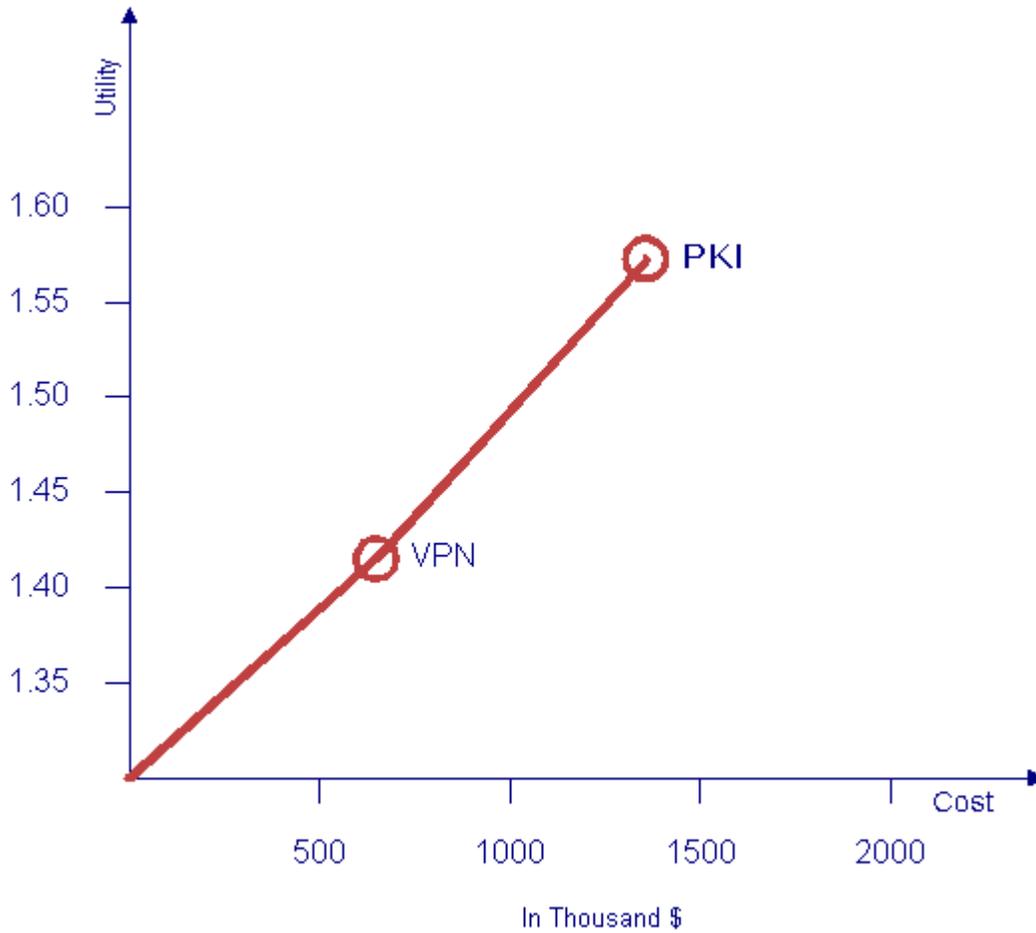
Figure 6 depicts the relationships between the utility of VPN and PKI versus their cost. The comparison of the two technologies in eight areas demonstrates that PKI exhibits a higher utility value as noted in Table 10. The cost of VPN is displayed in Table 2, while the cost of PKI is displayed in Table 1. The analysis shows that attainment of a higher level of utility requires a greater level of investment in information security technology.

13.0   The Survivability of Networks

In the previous section, we concluded greater utility of computer security was attained at a higher cost. This is only one consideration an organization must make when deciding on an information security strategy. An organization must consider the level of risk that exists for the network, which security products will provide the greatest level of information security utility, and cost constraints. The CERT Coordination Center has studied the benefits of implementing computer network security in general against the cost of such investment given different rates of incident. Their study did not look at any one security product in particular. The study examined incident data from 1988 to 1995 to determine the impact of attacks on networks sites.[26] They tried to determine if it was fruitful to invest in a network in order to better survive an attack by hackers. Could there be a way to measure the benefit of such investment? In the technical report, "The Survivability of Network Systems: An Empirical Analysis," Moitra and Konda create three models: one to characterize incidents, one for the response of the system to incidents, and one to calculate the resulting survivability rates. An incident can be characterized as an attempt to gain unauthorized access to a system, unwanted disruption, or the unauthorized use of a system. The response would be the system administrator's response to the incident in order to return to the same state that existed prior to the incident. Lastly, a model to determine rates that networks continued operations without disruption. Moitra and Konda suggest that a cost curve does exist where costs can be traded off for increased survivability of a network. Therefore, the more critical the function of a network, the greater the survivability rate that can be achieved by increased investment. Moitra and Kondas' study considers multiple security measures and not just access control like PKI or VPN. The study implies that higher the investment rate in security does result in a more secure network.

---

[26] *Moitra, Soumyo and Konda, Suresh, "The Survivability of Network Systems: An Empirical Analysis," Technical Report, CMU/SEI-2000-TR-021, Carnegie Mellon University Software Engineering Institute, December 2000*

Figure 7. Cost/Survivability Curve [27]
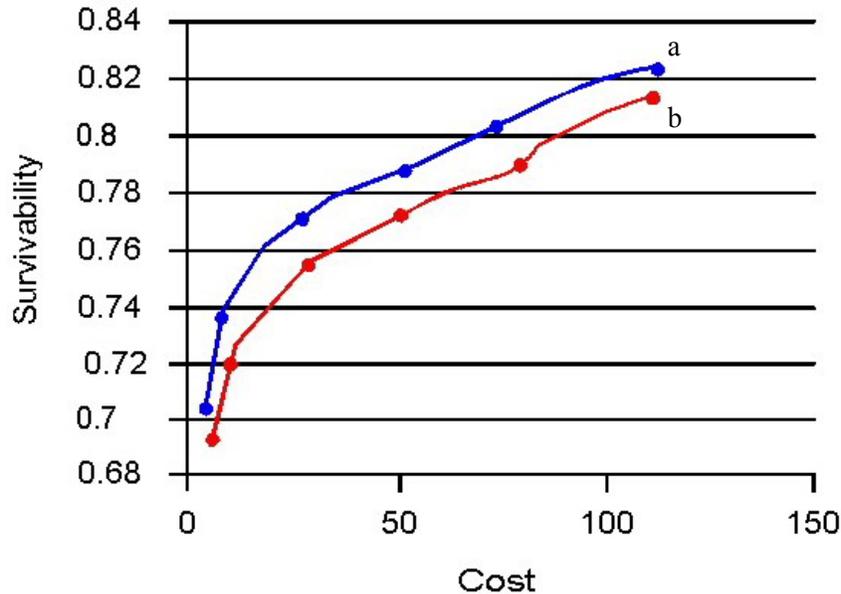
The two curves illustrated in Figure 7 show the cost/survivability at two different probabilities of attack levels. Line "a" illustrates the relationship when the probability of an incident is equal to .55. Line "b" shows the relationship between cost and survivability when probability of an incident is equal to .65. Since the functions exhibit similar characteristics, attention should be drawn to the early slope of the curves and how it flattens out moving away from the origin. Note that the two curves have a similar shape. The shape itself suggests survivability increases rapidly initially with increases in expenditures and then increases at a slower rate.

14.0   Cost of Information Security Breaches

In the Computer Security Institute's 2001 CSI/FBI survey of computer crimes, the cost and resulting impact is striking. The survey based its data on 538 responses from government and commercial organizations. According to the survey, 78% of the

---

[27] *Ibid 26*

respondents acknowledged financial losses and 37% could quantify a cost.[28] The total

loss from the 37% that could quantify losses was $377,828,700.[29] Two examples can

suggest why financial losses tend to be under reported. Many financial institutions refuse

to report publicly that a security breach occurred, for fear of a loss of consumer

confidence in the financial institution. Some losses are hard to quantify. When firms like

Yahoo or CNN shutdown because of a denial of service, it is hard to quantify that loss.

In addition to the loss of advertising revenue how does an organization account for the

loss of prestige and its service availability on the Internet? Does it discourage wider use

of the Internet when hackers bring down the largest sites?

Table 11 illustrates the 13 categories that the Computer Security Institute used in its

survey. The data include the number of respondents who claimed financial loss, the

average loss, and the total reported loss. While this data is not suitable for analysis

because its sources are varied and cannot be verified, it does provide some insight to the

problem of cost when information security is lacking in a computer network. The impact

of the financial loss is obviously significant, but what role can a PKI or VPN

implementation play in reducing or eliminating this risk? Are we examining the right

criteria? Our inclusion of Non-repudiation, Authentication, Data integrity, and

Confidentiality evaluates VPN and PKIs' ability to defend against outside attackers. The

remaining categories, Interoperability, Scalability, Portability, and Efficiency address the

way PKI and VPN interact with other systems within the overall computer network

system. Of the 13 categories listed in the survey only 5 (Theft of Proprietary

information, System Penetration by Outsiders, Financial Fraud, Spoofing, and

Unauthorized Insider Access) could possibly be deterred by a PKI system.   Respondents

reported the highest loss in the category called "Theft of Proprietary Information." This

is the category for which PKI can provide the greatest degree of protection. Because

transmission of data using PKI is encrypted and user access is controlled through smart

cards or biometrics, proprietary information enjoys a greater degree of security. While

many companies, agencies, and individuals are hesitant about digital signatures, the

---

[28] *Computer Security Institute, "2001 CSI/FBI Computer Crime Survey," Spring 2001*
[29] *Ibid 28*

Electronic Signatures in Global and National Commerce Act gives electronic signatures the same legal weight as a paper signature.[30] Similar legislation has been passed in several states. VPN can provide protection from four categories (Theft of Proprietary information, System Penetration by Outsiders, Financial Fraud, Spoofing). It does not offer any additional protection against unauthorized insider access. Because VPN uses username and passwords, it is vulnerable to misuses of valid users within the system.

---

[30] *Ibid 9*

Table 11. CSI/FBI Information Security Survey[31]

	Respondents with Quantified Losses 2001	Average Losses 2001	Total Annual Losses 2001
Theft of Proprietary Info	34	$4,447,900	$151,230,100
Sabotage of Data Networks	26	$199,350	$5,183,100
Telecom Eavesdropping	16	$55,375	$886,000
System Penetration by Outsider	42	$453,967	$19,066,600
Insider Abuse of Net Access	98	$357,160	$35,001,650
Financial Fraud	21	$4,420,738	$92,935,500
Denial of Service	35	$122,389	$4,283,600
Spoofing	N/A	N/A	N/A
Virus	186	$243,845	$45,288,150
Unauthorized Insider Access	22	$275,636	$6,064,000
Telecom Fraud	18	$502,278	$9,041,000
Active Wire Tapping	0	$0	$0
Laptop theft	143	$61,881	$8,849,000
Total			$377,828,700

15.0   Summary

In the field of information security, it has been very difficult to determine the best path to achieve an optimum solution. This report provides a tool and a method to consider information security investment. Because of the large upfront expenses required to implement PKI, the features of Non-Repudiation and Authentication must be paramount in the consideration of the network security to justify the greater expense.

---

[31] *Ibid 28*

PKI is complex. Managers making Information Technology investment decisions often struggle to understand how to implement PKI effectively. The technicians installing PKI must be properly trained and understand how it works with other parts of the organization's computer systems. With a shortage of qualified computer technicians, the problem is only compounded.

VPN is relatively simple. It has less interaction with applications of systems within the network. It simply allows access to the resources. PKI is designed to interact with applications, and as a result, can be less interoperable.

Organizations will always try to maximize their utility and minimize their cost in information security investments. But they cannot do both. So they must strike a balance. They can only invest a portion of their budget on information security. The report, "The Survivability of Network Systems: An Empirical Analysis," indicates that the money spent on information security is beneficial up to a point and may be more beneficial than other information technology spending. Given the hypothetical scenario in this report, PKI provides a higher level of security at a higher cost as noted in Figure 6: Table 10 indicates an organization will get more security per dollars spent from VPN based on the cost data in Tables 1 and 2. Other scenarios may offer different results. This paper simply provides a method to draw a conclusion given a set of criteria.

16.0   List of Sources

1. Booz – Allen and Hamilton, "CIO PKI/Smart Card Project Approach for Business Case Analysis of Using PKI on Smart Card for Government Wide Applications," General Services Administration (GSA), Washington, D.C. December 1, 2000

2. Braithwaite, Timothy, "Understanding Network Security Monitoring and Intrusion Response (NSMIR), "April 17, 2001, Tech Republic, http://www.techrepublic.com/index.jhtml

3. Carnegie Mellon Software Engineering Institute, "CERT/CC Statistics 1988-2001," http://www.cert.org/stats/cert_stats.html, October 15, 2001

4. Computer Security Institute, "2001 CSI/FBI Computer Crime Survey," Spring 2001, http://www.gocsi.com/

5. Dodd, F. J., Donegan, H. A., McMaster, T. B. M., "Reassessment of Consistency Criteria in Judgment Matrices," Statistician, Vol. 44, Issue 1, 1995

6. Harker, Patrick T., and Vargas, Luis G., "The Theory of Ratio Scale Estimation: Saaty's Analytic Hierarchy Process," Management Science, Vol. 33, No. 11, November 1987

7. Lipson, Howard F. and Fisher, David A., "Survivability – A New Technical and Business Perspective on Security," CERT Coordination Center, Software Engineering Institute Pittsburgh, PA, http://www.cert.org/research

8. Lyons-Burke, Kathy, "Federal Agency Use of Public Key Technology for Digital Signatures and Authentication," October 2000, National Institute of Standards and Technology (NIST), Special Publication 800-25, http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.pdf

9. Moitra, Soumyo and Konda, Suresh, "The Survivability of Network Systems: An Empirical Analysis" Technical Report, CMU/SEI-2000-TR-021, Carnegie Mellon University Software Engineering Institute, http://www.cert.org/research December 2000

10. Pettofrezzo, Anthony J., "Matrices and Transformations" Dover Publications, Inc., New York, N.Y., 1966

11. Prince, Frank, Buss, Christian, and Howe, Carl D., "Biometrics' Bubble Burst," November 28, 2000, Forrester Research, Inc, http://www.forrester.com

12. Ragsdale, Cliff T., "Spreadsheet Modeling and Decision Analysis," South-Western Publishing 2001, p. 766

13. Saaty, Thomas A, "How to Make a Decision: The Analytical Hierarchy Process" Interfaces 24: 6, pp19-43, November-December 1994

14. Saaty, Thomas A., "The Seven Pillars Of The Analytic Hierarchy Process," ISAHP Proceedings, Kobe 1999

15. Saaty, Thomas A., "Axiomatic Foundation of the Analytic Hierarchy Process," Management Science, Vol.32 No. 7, July 1986

16. Shepperd, Martin and Cartwright, Michelle, "Predicting with Sparse Data," Empirical Software Engineering Research Group School of Design, Engineering & Computing, Bournemouth University, Talbot Campus, Poole, UK August 14, 2000

17. Sugden, Robert, "Why be Consistent? A Critical Analysis of Consistency Requirements in Choice Theory," Economica, New Series, Vol. 52, Issue 206, May 1985

17.0   Glossary of Terms

Analytical Hierarchy Process - Analytical Hierarchy Process (AHP), represents a theoretically founded approach to computing weights representing the relative importance of criteria. Weights are not assigned directly, but represent a "best fit" set of weights derived from the Eigenvector of the square reciprocal matrix used to compare all possible pairs of criteria.

Authentication - The verification of the identity of a user who is logging into a computer system.

Confidentiality - Confidentiality ensures that information (e.g., customer data and intellectual property) is not disclosed to unauthorized persons, processes, or devices. Confidentiality is especially important when considering medical data and financial information.

Data integrity - The reliability of data passing through the system. Concerns include data tampering or inconsistent availability.

Efficiency - Minimizing the time added by the security product. If a security product makes the information secure but adds large amounts of time, it may result in an unacceptable cost.

Eigenvector - A statistical method to represent a "best fit" set of weights derived from a square reciprocal matrix used to compare all possible pairs of criteria.

Interoperability - Interoperability is the ability of systems to provide services to and accept services from other systems and to use the services to operate effectively.

Non-Repudiation – This is the ability to document a transaction. The transaction is dated and the parties involved in the transaction cannot deny their involvement in the transaction.

Portability – This is how the system allows for people to carry large amounts of pertinent information and equipment need to gain access.

Scalability – This is how well a hardware or software system can adapt to increased demands.

Yahoo – An Internet firm which depends on internet traffic across its site for the bulk of its revenues from advertising.

18.0   Acronyms

AES	Advanced Encryption System
AHP	Analytical Hierarchy Process
CA	Certification Authority
CCNA	Cisco Certified Network Associate
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordination Center (CERT/CC)
CI	Consistency Index
CNN	Cable News Network
CR	Consistency Ratio
CSI	Computer Security Institute
DES	Digital Encryption System
FBI	Federal Bureau of Investigations
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MCP	Microsoft Certified Professional
PKI	Public Key Infrastructure
RA	Registration Authorities
VPN	Virtual Private Network

19.0   Appendix A

THE ANALYTIC HIERARCHY PROCESS by Dr. Thomas L Saaty

"The AHP has four axioms: (1) judgments, (2) homogeneous elements, (3) hierarchic or feedback dependent structure, and (4) rank order expectations [Saaty 1986]

Assume that one is given n stones, $A_1,\dots, A_n$, with known weights $W_1,\dots,W_n$, respectively, and suppose that a matrix of pairwise ratios is formed whose rows give the ratios of the weights of each stone with respect to all others. Thus one has the equation:

$$Aw = \begin{array}{c} \\ A_1 \\ \cdot \\ \cdot \\ \cdot \\ A_n \end{array} \begin{bmatrix} \overset{A_1}{\dfrac{w_1}{w_1}} & \cdot\;\;\cdot\;\;\cdot & \overset{A_n}{\dfrac{w_1}{w_n}} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \dfrac{w_n}{w_1} & \cdot\;\;\cdot\;\;\cdot & \dfrac{w_n}{w_n} \end{bmatrix} \begin{bmatrix} w_1 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{bmatrix} = n \begin{bmatrix} w_1 \\ \cdot \\ \cdot \\ \cdot \\ w_n \end{bmatrix} = nw$$

where A has been multiplied on the right by the vector of weights w. The result of this multiplication is nw. Thus, to recover the scale from the matrix of ratios, one must solve the problem $Aw = nw$ or $(A - n\mathrm{I})w = 0$. This is a system of homogeneous linear equations. It has a nontrivial solution if and only if the determinant of $A - n\mathrm{I}$ vanishes, that is, n is an eigenvalue of A. Now A has unit rank since every row is a constant multiple of the first row. Thus all its eigenvalues except one are zero. The sum of the eigenvalues of a matrix is equal to its trace, the sum of its diagonal elements, and in this case the trace of A is equal to n. Thus n is an eigenvalue of A, and one has a nontrivial solution. The solution consists of positive entries and is unique to within a multiplicative constant.

To make w unique, one can normalize its entries by dividing by their sum. Thus, given the comparison matrix, one can recover the scale. In this case, the solution is any column of A normalized. Notice that in A the reciprocal property $a_{ji} = 1/a_{ij}$ holds; thus, also $a_{ii} = 1$. Another property of A is that it is consistent: its entries satisfy the condition $a_{jk} = a_{ik}/a_{ij},$. Thus the entire matrix can be constructed from a set of n elements which form a chain across the rows and columns.

In the general case, the precise value of w_i/w_j cannot be given, but instead only an estimate of it as a judgment. For the moment, consider an estimate of these values by an expert who is assumed to make small perturbations of the coefficients. This implies small perturbations of the eigenvalues. The problem now becomes $A'w' = \lambda_{max} w'$ Where is the largest eigenvalue of A'. To simplify the notation, we shall continue to write $Aw = \lambda_{max}w$, Where A is the matrix of pairwise comparisons. The problem now is how good is the estimate of w. Notice that if w is obtained by solving this problem, the matrix whose entries are w_i/w_j, is a consistent matrix. It is a consistent estimate of the matrix A. A itself need not be consistent. In fact, the entries of A need not even be transitive; that is, A_1 may be preferred to A_2 and A_2 to A_3 but A_3 may be preferred to A_1. What we would like is a measure of the error due to inconsistency. It turns out that A is consistent if and only if $\lambda_{max} = n$ and that we always have $\lambda_{max} \geq n$.

Since small changes in a_{ij} imply a small change in λ_{max}, the deviation of the latter from n is a deviation from consistency and can be represented by $(\lambda_{max} - n)/(n - 1)$, which is called the *consistency index* (C.I.). When the consistency has been calculated, the result is compared with those of same index of a randomly generated reciprocal matrix from the scale 1 to 9, with reciprocals forced. This index is called the *random index* (R.I.). Table 11 gives the order of the matrix (first row) and the average R.I. (second row).

n	1	2	3	4	5	6	7	8	9	10
Random Consistency Index (R.I)	0	0	0.52	0.89	1.11	1.25	1.35	1.40	1.45	1.45

Table 11: The order of the matrix (first row) and the average R. I. (second row).

The ratio of C.I. to the average R.I. for the same order matrix is called the consistency ratio (C.R.). A consistency ratio of 0.10 or less is positive evidence for informed judgment.

The relations $a_{ji} = 1/a_{ij}$ and $a_{ii} = 1$ are preserved in these matrices to improve consistency. The reason for this is that if stone #1 is estimated to be k times heavier than stone #2, one should require that stone #2 be estimated to be 1/k times the weight of the first. If the consistency ratio is significantly small, the estimates are accepted; otherwise, an attempt is made to improve consistency by obtaining additional information. What contributes to the consistency of a judgment are (1) the homogeneity, of the elements in a group, that is, not comparing a grain of sand

with a mountain; (2) the sparseness of elements in the group, because an individual cannot
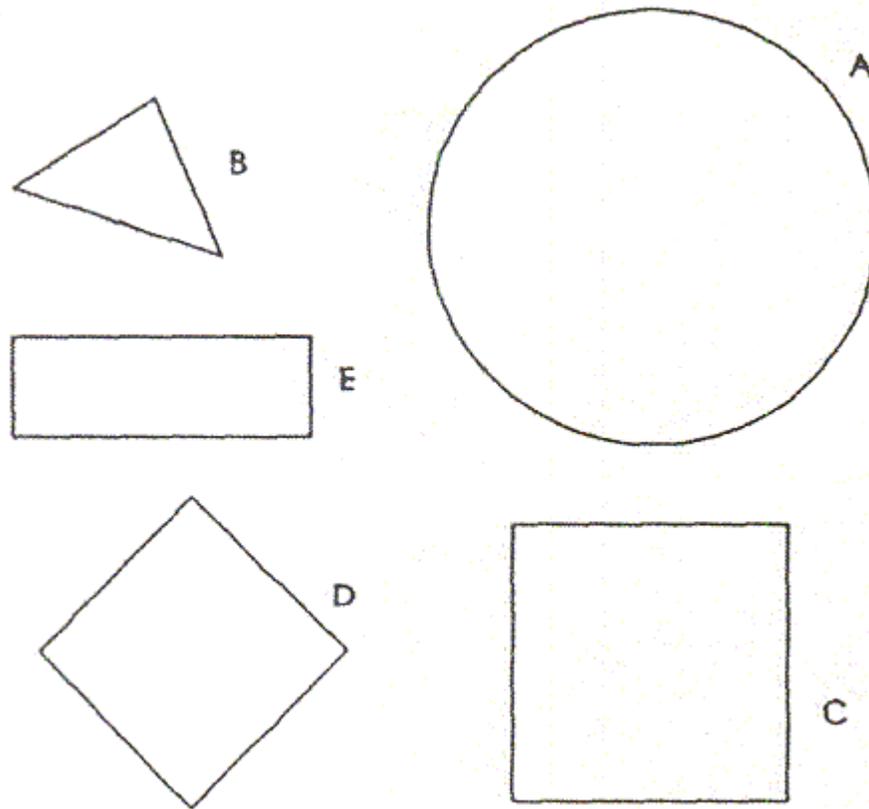

Figure 4: Five figures drawn with appropriate size of area. The object is to compare them in pairs to reproduce their relative weights.

hold in mind simultaneously the relations of many more than a few objects; and (3) the knowledge and care of the decision maker about the problem under study.

Figure 4 shows five areas to which we can apply the paired comparison process in a matrix and use the 1-9 scale to test the validity of the procedure. We can approximate the priorities in the matrix by assuming that it is consistent. We normalize each column and then take the average of the corresponding entries in the columns.

The actual relative values of these areas are A=0.47, B = 0.05, C = O.24, D = 0.14, and E = 0.09 with which the answer may be compared. By comparing more than two alternatives in a decision problem, one is able to obtain better values for the derived scale because of redundancy

```
in the comparisons, which helps improve the overall
accuracy of the judgments."32
```

Reprinted by permission, Saaty, Thomas L, "How To Make A Decision: The Analytical

Hierarchy Process," *Interfaces*, volume **24**, number 6, November-December 1994. Copyright

1994, The Institute of Management Sciences (currently INFORMS), 901 Elkridge Landing Road,

Suite 400, Linthicum, Maryland 21090-2909 USA.

---

[32] *Ibid 10*

20.0   VITA

Edward D. Wagner
Associate
Booz | Allen | Hamilton

The author was raised in New Canaan, CT where he graduated from high school in 1984. He earned the degree of Bachelor of Arts from the Virginia Military Institute in 1988. He earned the degree of Master of Arts in Economics from the Virginia Polytechnic Institute and State University in 2002.

Mr. Wagner served on active duty in the U.S. Army as an officer and was assigned to the 101st Airborne Division. He participated in Operation Desert Shield/Storm and was awarded the Bronze Star Medal. Mr. Wagner continues to serve in the Army Reserves as a Major with the National Capitol Region Information Operations Center. He has held many positions in the Information Technology field from system administration and web development to network design and information assurance planning. He is currently employed with Booz | Allen | Hamilton as an Associate. He has supported many clients within the Department of Defense including members of the Office of the Secretary of Defense, the Joint Staff and the Joint Task Force-Computer Network Operations. Mr. Wagner currently resides in Northern Virginia with his wife Katrina and their three children.