Journal of International Technology and Information Management

Volume 19 | Issue 4 Article 2

2010

Enterprise Systems Network: SecurID Solutions, the Authentication to Global Security Systems

Emmanuel U. Opara
Prairie View A&M University

Vance Etnyre
University of Houston, Clear Lake

Recommended Citation

Opara, Emmanuel U. and Etnyre, Vance (2010) "Enterprise Systems Network: SecurID Solutions, the Authentication to Global Security Systems," *Journal of International Technology and Information Management*: Vol. 19: Iss. 4, Article 2.
Available at: http://scholarworks.lib.csusb.edu/jitim/vol19/iss4/2

Enterprise Systems Network: SecurID Solutions, the Authentication to Global Security Systems

Emmanuel U. Opara
Prairie View A&M University
USA

Vance Etnyre
University of Houston, Clear Lake
USA

ABSTRACT

Enterprise systems need reliable, flexible and secure means for making public and confidential information available to users in a secured and trusted manner. Although enterprise systems have variety of choice to authenticate these users, organizations face significant issues when granting access and providing a manageable structure for valuable access control. Logon functionalities such as user name and password algorithm have been used to grant authentication and authorization into enterprise systems network resources. Since most systems clients prefer the ease of using passwords, and since passwords are easily compromised, the urgency for a stronger authentication process becomes paramount. This study performed an internal evaluation of enterprise systems such as rating the effectiveness of a security platform as well as an external evaluation; i.e., analyzing how a security system is been rated by external entities. The study will examine correlations between system security best practices and reported or observed outcomes. The study concluded by evaluating the use of added protective layers to the two or multi-factor authentication security system.

INTRODUCTION

Enhancement in information access has necessitated new challenges to users for the fortification of susceptible data and systems resources against emergent number of security risks and theft related issues. Enterprise systems have witnessed breaches and malicious intrusions into network systems. This has raised the standard for security compliance by system engineers as they struggle to protect network vulnerabilities and meet regulatory compliance. With the rising number of data security breaches and the increasing sophistication of cybercrime, protecting access to organization critical data and systems becomes a major necessity.

System gurus comprehend the potential threats posed to their networks and are devising means to cope with those threats and implement sustainable solutions. As businesses strive for transparency, interoperability and mobility, respective corporate networks become susceptible to threats from a third party whose security apparatus is not subject to audits and control mechanism by the system (Altman, 2006). Systems employees are given administrative privileges to enable such individuals perform their administrative duties. Such rights could be compromised by disgruntled employees, contractors, vendors, or temporary workers, thereby allowing critical security services to be inoperable.

Several enterprise systems use Internet filtering tools such as intrusion detection software and firewalls to protect valuable data on their systems, but additional security measures are needed to safeguard the loss of intellectual properties and other valuable data on a system. Most of these companies do not have enforcement apparatus to enforce compliance or to report on suspicious activities (Resencrance, 2004). Phishers are constantly circumventing the two-multi factor authentication scheme by implementing man-in-the middle attacks. Due to this loophole in the enterprise policy security infrastructure, corrective measures to detect and prevent threats from malware, hackers, malicious users, become paramount.

According to Andress (2006), the Federal Trade Commission (FTC) reported that identity theft affected nearly 90 million Americans and cost approximately $173 billion in 2005. Also, Skoudis (2005) found evidence that worldwide identity theft and related crimes could cost businesses about $532 billion in losses by the end of 2010.

Since most end-users and various enterprise clients perform a fraction of their business transactions at their respective local offices, the need for a reliable and secured authentication mechanism cannot be overstated. End-users, who engage extensively on electronic services, complain that passwords have become difficult to remember (Andress, 2006). Most of the systems require password changes every 90 days and this makes it cumbersome to remember which password was used within a given period.

Logon functionalities of user name and password algorithm have been used to grant authentication and authorization into enterprise systems network resources. Although authentication provides system administrators with valuable information about who is accessing the application, users get frustrated remembering user name and logon IDs. Since passwords can be compromised, the urgency for a stronger authentication process becomes paramount.

Solutions to these problems could include the fortification of the Enterprise Network Security platform and the addition of more security layers for a stronger multifactor authentication process. A strong authentication process should include, but not limited to, a device or information that the user possesses. These could include a hardware token or a barometric characteristic or some information or code that the user knows. An example would be a Personal Identification Number (PIN). Other examples might include smart cards or badges.

REVIEW OF THE LITERATURE

Ofir (2005), Lu, Liu, Yu, and Yao (2005), Ryker and Bhutta (2005), Opara (2004), Pescatore, Nicolett, and Orans (2004), and Krim (2003) among others have noted that in the past few years, systems security administrators have seen a decline in recreational hacking, and an increase in commercial hacking. Skoudis (2005) reiterated by stressing the importance of data protection in this digital environment.

Potential proliferation and the persistency of professional hackers have lead to the desire of enterprise security administrators to protect crucial systems from unauthorized access (Vijayan, 2006). If data and information are not protected, enterprise systems could lose the confidence of customers as well as shareholders.

Vijayan (2006) stressed that by end of calendar year 2009, the annual amount of money spent on security software support services in the United States could surpass $920 million dollars. Skoudis (2005) argued that by year-end 2008, 95 percent of enterprise systems will have implemented network access control policies and procedures to guide the network system.

Vijayan (2006) and Jain (2005) in a recent study, identified some key market drivers as the reason for a stronger security platform and authentication. These are increasing open networks capabilities, the extended mobile users that connect to enterprise networks, the continuous weakness of passwords as a security mechanism, the increased number of online users, the increased emphasis on policy and regulatory compliance issues across the industries.

Ofir (2005), Scholtz (2004), Opara and Rob (2003), among others argued that speaker verification and speech recognition technologies provide viable secure caller authentication techniques with no constraint for physical tokens.

When considering a good solution for office to office connectivity, especially when a small number of trusted users access the LAN from managed corporate PCs, the network layer IPSec VPNs will be an ideal connectivity component (Altman, 2006).

Ewing (2006), Jepson (2006), Gage (2007), Price (2007) among others, conclude that the authentication market for enterprise systems would continue to grow at an exponential rate during the next few years as businesses seek to protect access to enterprise network resources.

METHODOLOGY

Determining the buoyancy level and adequacy of a stronger authentication methodology as a barrier to network systems intrusions, a survey was conducted to access users' perception and understanding of the importance of a strong authentication system. User profiling in terms of setup time will also used. The survey instrument was distributed randomly to Business Intelligence (BI) professional at the 2008 International Microwave IT symposium in Atlanta Georgia. Some of the target participants included professionals from Informatica, SAP Business Objects, Netezza, MicroStrategy Inc., IBM, Dataupia, Baseline Consulting, and DataFlux. Of the 644 surveys originally distributed, 201 were fully completed and 17 were rejected for lack of completion. The two hundred and one fully completed surveys represent a response rate of 32.2 percent (201/(644-17)). The responses were assigned weights that were summed to indicate the trends for more fortified security authentication technology. The authors noted that beyond an appeal to help the researchers, respondents were not offered any other incentives to complete the surveys.

RESULTS FROM DATA ANALYSIS DIALOG

The authors identified two of the variables from the survey as “outcome” variables. The designated outcome variables were #5 (How strongly do you agree to the effectiveness of the security systems of your organization?) and #9 (How do your customers, vendors, partners, suppliers, clients, and others agencies rate your security systems?).

One variable, #6 (Have there been security system breaches in your organization?) was viewed as a possible outcome variable as well as a contributing variable. All other variables dealt with technical aspects of security and were viewed as contributing to the outcome variables.

The authors realized that some transformations of the data would be required before meaningful statistical analysis could be performed. Most of the contributing variables had a few responses of “don’t know” or “not sure”. These variables were transformed into binary variables where 1 = “yes” and 0 = “not yes” (“no” or “not sure” or “don’t know”). This transformation allowed the use of these contributing variables as binary “dummy variables” in linear regression analyses.

Before the authors tried to analyze the outcome variables in terms of their relationships to contributing variables, the authors tried to use factor analysis to reduce the number of contributing variables. High correlations between contributing variables indicated that such a reduction might be possible. The results of the factor analysis procedure did not yield significant, useful reductions. Four composite factors emerged which could explain 71% of the variation in the set of six contributing variables. The 29% of remaining unexplained variation was deemed too large to justify reduction from six to four variables.

The authors tried to use the contributing variables to predict the values of variable #6 (Have there been security system breaches in your organization?). Using stepwise linear regression, the authors found that no contributing variable met the entry criterion of p = .05. This was not particularly surprising when you consider that variable #6 was not a true measure, but only an estimate made by respondents. There may have been many system breaches that respondents did not know about.

The authors were successful in using stepwise linear regression to find a predictive relationship between internal confidence in the system (outcome variable, #5) and two contributing variables. The two significant contributing variables were variable #6 (Breaches in the system), and variable #8 (frequency of password changes).

The overall percentage of all respondents who had confidence in their own security system was 53.7%. Table (1) below shows that the first variable to enter into the predictive model for internal confidence is variable 6 (Breaches in the system). Variable #6 entered the model with a negative coefficient. This means the more that users observed or recognized breaches in the security system, the lower the predicted confidence in the system. With this variable in the predictive model, the constant is 67.5%, 13.8 percentage points higher than the base case (with no predictive variables). That means that for respondents who reported no breaches, the predicted percentage indicating confidence was 67.5%. For respondents who reported no breaches, the ACTUAL percentage indicating confidence was 64.0%.

The coefficient for variable #6 in the predictive model was -.259. This factor is used within the predictive model for respondents who reported breaches. For those who reported breaches, the predicted percentage indicating confidence in the system would be 67.5% – 25.9% = 41.6%. For respondents who reported breaches, the ACTUAL percentage indicating confidence in the system was 42.0%.

Table 1: Predictive Models for Internal Confidence[a.]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	T	Sig.
1	(Constant)	.675	.058		13.304	.000
	V#6 eaches	-.259	.052	-.333	-4.980	.000
2	(Constant)	.564	.100		5.639	.000
	V#6 breaches	-.212	.054	-.273	-3.906	.000
	V#8 pw_freq	.124	.048	.180	2.581	.011

a. Dependent Variable: Internal

After variable #6 was included into the predictive model, variable #8 (How often are you required to change your password?) entered the predictive model. Unlike variable #6, which had a negative coefficient in the predictive model, variable #8 had a positive coefficient. This means the more often users are required to change their passwords, the higher the predicted confidence in the system.

With variable #6 and variable #8 in the predictive model, the constant is 56.4%, 2.7 percentage points higher than the base case (with no predictive variables). That means that for respondents who reported no breaches, and very low frequency for required password changes, the predicted percentage indicating Internal Confidence was 56.4%. For respondents who reported no breaches and very low frequency for required password changes, the ACTUAL percentage indicating confidence was 60.0%.

The coefficient for variable #6 in the predictive model was .124. This factor is used within the predictive model for respondents who reported a high frequency for required password changes. For those who reported no breaches and a high frequency for required password changes, the predicted percentage indicating confidence in the system would be 56.4% + 12.4% = 68.8%. For respondents who reported no breaches and a high frequency for required password changes, the ACTUAL percentage indicating confidence in the system was 64.4%.

For those who reported breaches and a high frequency for required password changes, the predicted percentage indicating confidence in the system would be 56.4% - 21.2% + 12.4% = 47.6%. For such respondents, the ACTUAL percentage indicating confidence in the system was 44.4%. These results are summarized in Table 2 below.

Table 2: Predicted and Reported Percentages of Internal Confidence.

Reported Breaches	Reported Frequent Password Change	Predicted Internal Confidence(%)	Reported Internal Confidence(%)
No	No	67.5%	64.0%
Yes	No	41.6%	42.0%
No	Yes	68.8%	64.4%
Yes	Yes	47.6%	44.4%

After analyzing internal confidence in the security system, the authors were successful in finding a predictive relationship between External Confidence in the system (How do your customers, vendors, partners, suppliers, clients, & others agencies rate your security systems) and the same two contributing variables (#6 & #8) which were significant predictors of Internal confidence. The percentage of all respondents who reported External Confidence (outcome variable, #9) was 47.3%. Table (3) below shows that the first variable to enter into the predictive model is variable 6 (Breaches in the system). Variable #6 entered the model with a negative coefficient. This means that the more users observed or recognized breaches in the security system, the lower the predicted confidence in the system. With this variable in the predictive model, the constant is 87.8%, 40.5 percentage points higher than the base case (with no predictive variables). For respondents who reported no breaches, the predicted percentage indicating confidence was 87.8%. For such respondents, the ACTUAL percentage indicating confidence was 92.0%.

Table 3: Predictive Models for External Confidence[a.]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.878	.051		17.208	.000
	V#6 breaches	-.440	.045	-.566	-9.685	.000
2	(Constant)	1.081	.087		12.387	.000
	V#6 breaches	-.485	.047	-.623	-10.240	.000
	V#8 pw_freq	.119	.042	.173	2.841	.005

a. Dependent Variable: External

The coefficient for variable #6 in the predictive model was -.440. This factor is used within the predictive model for respondents who reported breaches. For those who reported breaches, the predicted percentage indicating confidence in the system would be 87.8% – 44.0% = 43.8%. For such respondents, the ACTUAL percentage indicating confidence in the system was 40.2%. After variable #6 was included into the predictive model, variable #8 (How often are you required to change your password?) entered the predictive model. Unlike variable #6, which had a negative coefficient in the predictive model, variable #8 had a positive coefficient. This means the more often users are required to change their passwords, the higher the predicted confidence in the system.

With variable #6 and variable #8 in the predictive model, the constant is 108.1%, 20.3 percentage points higher than the base case. For respondents who reported no breaches, and very low frequency for required password changes, the predicted percentage indicating confidence was more than 100%. For such respondents (reported no breaches and very low frequency for required password changes), the ACTUAL percentage indicating confidence was 94.1%.

The coefficient for variable #6 in the predictive model was .119. For those who reported breaches and a high frequency for required password changes, the predicted percentage indicating confidence in the system would be 108.1% - 48.5% + 11.9% = 72.5%. For such respondents, the ACTUAL percentage reporting confidence in the system was 66.7%. This data is summarized in Table 4, below.

Table 4: Predicted and Reported Percentages of External Confidence.

Reported Breaches	Reported Frequent Password Change	Predicted External Confidence(%)	Reported External Confidence(%)
No	No	87.8%	92.0%
Yes	No	43.8%	42.0%
Yes	Yes	72.5%	66.7%

As a final step in the analysis of data, the authors decided to add the variable #5, Internal confidence, to the set of contributing variables in the model to predict variable #8, External Confidence, and to add External Confidence to the set of contributing variables in the model to predict Internal Confidence. Adding variable #5 (Internal Confidence) to the set of contributing variables did not change the model for predicting variable #8, External Confidence. This makes sense since people outside of an organization will not usually be influenced by (or even know) the opinions of insiders about system security.

As a contributing variable, however, variable #8 (External Confidence) was significant for predicting variable #5, Internal confidence. This can be seen in the third step of the stepwise regression analysis shown below.

Table 5: Predictive models for internal confidence[a.]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	T	Sig.
1	(Constant)	.675	.058		13.304	.000
	Breaches	-.259	.052	-.333	-4.980	.000
2	(Constant)	.564	.100		5.639	.000
	Breaches	-.212	.054	-.273	-3.906	.000
	pw_freq	.124	.048	.180	2.581	.011
3	(Constant)	.402	.132		3.032	.003
	Breaches	-.139	.067	-.179	-2.085	.038
	pw_freq	.141	.049	.206	2.913	.004
	External	.150	.078	.150	1.985	.046

a. Dependent Variable: internal

This chart shows that a high level of confidence in system security by people outside of an organization can increase the predicted confidence of people inside the organization. The last line of the table shows that this increase can be as large as 15 percentage points.

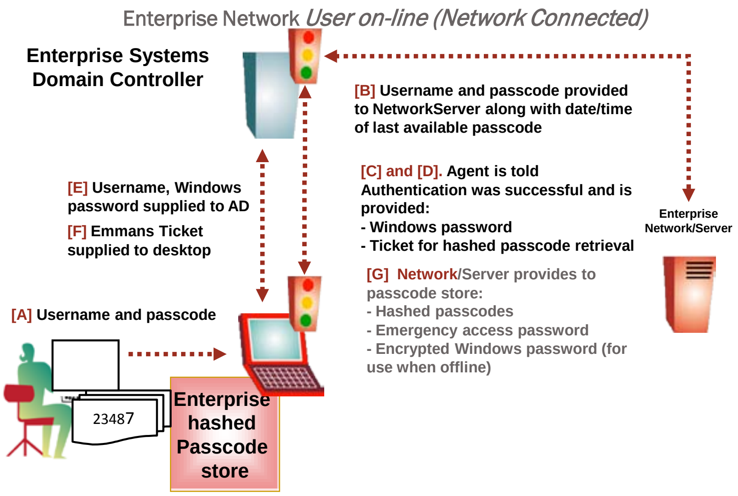
ENTERPRISE SECURID – STANDARD FOR STRONG TWO OR MULTI FACTOR AUTHENTICATION SYSTEMS

Since a single factor approach such as a password alone provides a low proof of authentication, the addition of a subsequent substantial proof assures that the authenticity will be elevated.

Wells Fargo Bank and Bank of America among other banks are examples of a widely used form of two/multi factor authentication technology. A multifactor authentication uses two or three different ways to authenticate users' profile. These include the use of a password or a knowledge based authentication such as response to a challenge question.

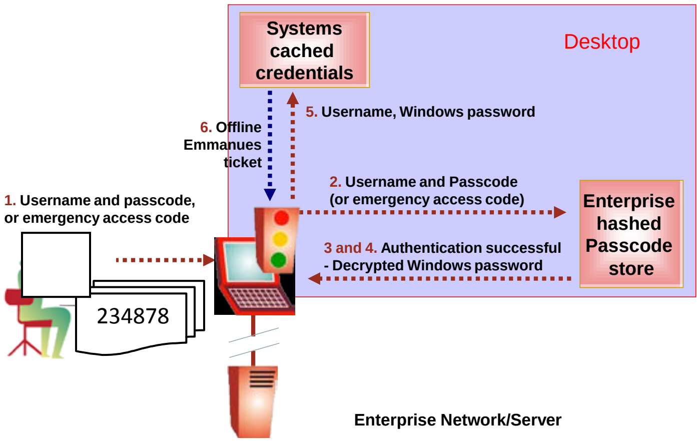
Another way is a physical apparatus, such as a smart card with a chip embedded into the cell, or hardware token that generates a one time passwords. A third component for identifying a user might be biometric technology. A fingerprint or an iris scan serves this purpose. Collectively, a multifactor approach uses a password and a second or third factor as stipulated in the figures below to authenticate the user in Figures 1, 2 and 3 (Gage, 2006).

Figure 1: How the System works.


Enterprise Network *User on-line (Network Connected)*
Enterprise Systems Domain Controller
[B] Username and passcode provided to NetworkServer along with date/time of last available passcode
[C] and [D]. Agent is told Authentication was successful and is provided:
- Windows password
- Ticket for hashed passcode retrieval
Enterprise Network/Server
[E] Username, Windows password supplied to AD
[F] Emmans Ticket supplied to desktop
[G] Network/Server provides to passcode store:
- Hashed passcodes
- Emergency access password
- Encrypted Windows password (for use when offline)
[A] Username and passcode
23487
Enterprise hashed Passcode store

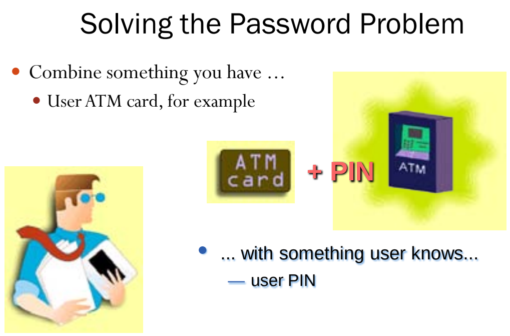
Source: Gage, 2006.

Figure 2: User off-line (Network disconnected).


Systems cached credentials
Desktop
5. Username, Windows password
6. Offline Emmanues ticket
2. Username and Passcode (or emergency access code)
1. Username and passcode, or emergency access code
Enterprise hashed Passcode store
3 and 4. Authentication successful
- Decrypted Windows password
234878
Enterprise Network/Server

Source: Gage, 2006.

Figure 3: Solutions at a banking ATM.



Solving the Password Problem

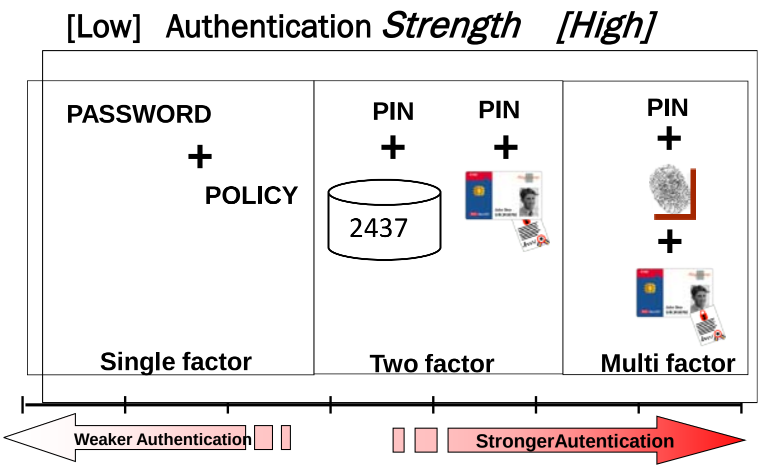
- Combine something you have …
  - User ATM card, for example

- ... with something user knows...
  - — user PIN

Source: Ewing, 2006.

Authentication choices fall into three categories, see Figure 4. The single factor which is the password and policy alone is very weak. The two-factor approach, which includes a combination of two pins, is not bullet proof. The multi-factor approach combines the two factor authentication and an additional factor such as a biometrics (Grey et al., 2005).

Figure 4: Authentication Choices.



Source: Grey et al., 2005.

Table 6: Authentication solutions.

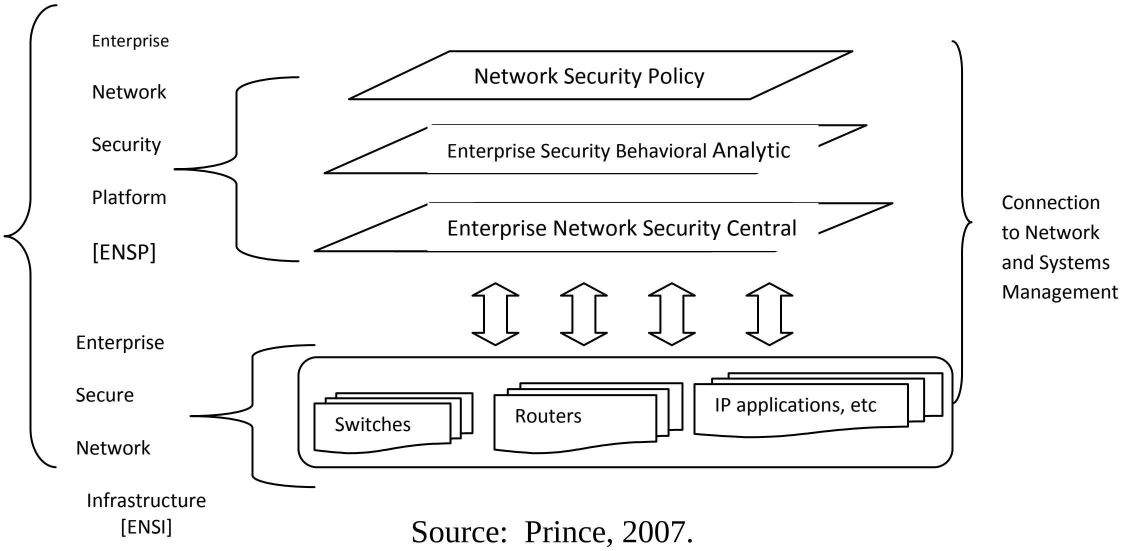
Security Levels
Authorization – RACF ETC Level This level identifies if the user is allowed to do what they're trying to accomplish on the system
Authentication Level This is level where multifactor or secured two-factors determine if the user is actually who he or she says they are.
Privacy Level This level uses the security technology of Secured Socket Layer [SSL] to protect un-authorized user from accessing user's data
Non Repudiation Level This level prevents the user from claiming that they did not authorize the transaction etc.

Source: Ofir, 2005.

As Table 6 indicates, an example of an authorization gadget is a password. This device makes it possible for the system to approve the requestor access into the system, as the true holder of the password. However, for additional level of security, it becomes paramount for the system to authenticate the user (Ofir, 2005). This process supposedly will guarantee that the user or the holder of the password is actually who they claim they are as they attempt to logon to the network. There are now breakthroughs in latest security apparatus that can be used in combination with passwords to identify authorized users, see Figure 5.

Figure 5: Complete analysis of an Enterprise Network Security Architecture

Enterprise Network Security Platform/Architecture



Source: Prince, 2007.

The enterprise network security architecture is comprised of the ENSP and the ENSI. Together, both elements are built into an enterprise architectural landscape that is able to capture, analyze and remediate security problems in real time.

As shown in the diagram above, enterprise network security platform (ENSP) is the central command facility that acts on the security information intercepted in the processing chain. The ENSP functionalities include the control, analytics and policy functions.

In order to enable enterprise centralized network security management and administration perform properly, the *control phase* ensures that all dubious information and other surveillance information collected from the ESNI are aggregated for analysis.

At the Analytics phase, data that have been stored and analyzed for behavioral anomalies are re-evaluated. These analyses could be a result of historic events on systems vulnerabilities and abnormalities on traffic patterns.

At the Policy phase, systems protective policy implementation is configured through the ENSP policy engine. This mechanism accelerates enforcement procedures based on established benchmarks. These include but not limited to gateways, access rights, ports, protocols and traffic anomalies.

The other component of the network security architecture is the Enterprise Network Secured Infrastructure (ENSI). These components are comprised of several routers, switched, IP applications, scanners, security and observatory apparatus that are in the processing chain. The ENSI perform the Enterprise Network Observatory and Enforcement duties.

In the Network Observatory phase, each periphery monitors enterprise network traffic flow for abnormities as data passes their respective locations.

In the Enforcement phase, imbedded filtering features permit each periphery to perform the duties of an Intrusion Prevention Systems (IPS) when prompted by a systems command.

The end result is that the ENSA is able to centralize security automaton enforcement thereby enhancing operational efficiency and productivity.

IMPLICATIONS TO BUSINESS AND SYSTEMS SECURITY GURUS

Systems security and network professional are constantly faced with new challenges. One of these challenges is that the networks gurus will continuously scrutinize the network for unscrupulous, dubious and unauthorized peripheries that could cause a breach in security. Another challenge that these gurus face is unending scrutiny on suspected problematic areas as they are detected. Since 911 incidents, systems security is now an on-going venture, and as such, these experts will be expected to develop breakthroughs to safeguard the enterprise.

CONCLUSION

As this study has shown, without a strong authentication mechanism, no functionality in SSL would avert a trespasser from getting biometric or keystroke recordings and impersonating an authorized user. The notion of Network Security Architecture is exclusive because it assumes an architectural approach. Combinations of this approach with a two-factor or a multi-factor approach will increase the security infrastructure of a system. Enterprise systems gurus whose organizational goals are to maximize their return on investment and exceed their customers' expectations, should implement vendor-neutral solutions that work with their existing infrastructure thereby enabling the system to quarantine and destroy threats from malware and unknown or non-compliant users.

Breakthroughs and innovative ventures are now in place that defines policies, controls and analytic measures that are now implemented to system-wide platforms. Enterprise system clients and end-users whose businesses necessitate thorough security measures are implementing Security SecurID multifactor authentication as the flag bearer for protecting network systems. The study shows that there is no definite solution at this moment to fully eliminate every threat. However, system security gurus should continue to upgrade policies, assess threats and implement control mechanism that will consistently manage and protect network security apparatus.

REFERENCES

Altman, H. (2006, February 20). Jihad web snares online shops, buyers. *Tampa Tribune.*

Andress, M. (2006). AppShield repels hack attacks-speeds e-business applications to market while keeping web servers safe. *Info World*, 22(20), May 1, 45.

Berinato, S. (2000). A UL-type seal for security? don’t bet on it. *eWeek*, October 15. Available. Online at: http://www.zdnet.com/filters/printer-friendly/ 0, 6061, 2640597-2, 00.html.

Ewing, J., Kral, G., & Young, K. (2006, January). Protecting reputational risk through data privacy compliance. *The Metropolitan Corporate Counsel.*

Gage, D. (2006, May 15). Bank of America seeks anti-fraud anodyne. *Baseline*, baselinemag.com/article2/0,1540,1962470,00.asp (accessed January 2007).

Hurwitz Report. (2000). Web application security: protecting e-business from attack. Sanctum, Inc. Available online at http://www.sanctuminc.com/Security/more/index.html

Jain, R. (2005). Contextual analysis of enterprise mobile services requirement. *Journal of International Technology and Information Systems,* 14(2).

Jepson, K. (2006, July 1). Bewear. Bware. Beware. The typosquatters. *Credit Union Journal*, 10(27).

Leclaire, J. (2007, January 3). Social networking sites in the crosshairs? *TechNewsWorld.* technewsworld.com/story/54932.html

Lu, J., Liu, C., Yu, C-S., & Yao, J. E. (2005), Acceptance of wireless internet via mobile technology in China. *Journal of International Technology & Information Management,* (14)2, 117-130.

Markoff, J. (2002, May 13). Vulnerability is discovered in security for smart cards. *The New York Times.* (http://www.nytimes.com/200205/13/technology/13SMAR.html)

Nahnybida, S. (2003, October). Expectations unfulfilled on e-billing, e-payments. *Bank Technology News*, 16(10), 62-63.

Olson, S. (2000, February 21). Protection from hackers available for e-tailers. *Indianapolis Business Journal*, 20(50).

Opara, E. (2004). Gateway for data mobility & universal connectivity. *Journal of International Technology & Information Management*, 13(3), 169-180.

Pince, B. (2007, January 22). Storm' worm continues surge around globe. *eWeek.* eweek.com/article2/0,1895,2086374,00.asp?kc=EWWHNEMNL012507EOAD (ACCESSED January 2007)

Savage, M., (2000, September 25). Locking the doors-denial of service attacks & viruses prime the market for security solutions and services. *Computer Reseller News*, 72.

Sundaram, A. (2000). An introduction to intrusion detection. *Association for Computing Machinery*. Available Online at: http://www.acm.org/crossroads/xrdds2-4/intrus.html

Krim, J. (2003, July 27). WiFi is open, free and vulnerable to hackers: safeguarding wireless networks too much trouble for many users. *The Washington Post*, A1.

Ofir, A. (2005, June). Deficiencies with active network discovery systems. Available from: http://www.insightix.com/resources-currentwhitepaper.asp

Pescatore, J. Nicolett, M., & Orans, L. (2004). *Protect your network with network access control*, Gartner, Inc. Available online at: http://www.gartner.com/DisplayDocument?doc_cd=124992

Piazza, P. (2003, December). Phishing for trouble. *Security Management*, 47(12), 32-33.

Pitney Bowes Group 1. (2007). Software Report: Customer Xhurn Report 2007.

Powell, T. (2004, May 17). Quick tips for web application security. *Network World*, 21(20), 50-51.

Rob, M., & Opara, E. (2003). Online credit card processing models: critical issues to consider by small merchants. *Human Systems Management*, 22(3), 133-142.

Rosencrance, L. (2004, September 6). Federal audit raises doubts about IRS security system. *Computerworld*, 38(36), 9.

Rubenking, N. (2002). Securing Web Services. *PC Magazines*, 21(17), Oc1, lP01-04.

Ryker, R., & Bhutta, K. (2005). Online privacy policies: an assessment of the Fortune Global 100. *Journal of International Technology and Information Management,* 14(1), 15-24.

Skoudis, E. (2005). Five malicious code myths and how to protect yourself in 2005. SearchSecurity.com, January 4 (http://searchsecurity.techtarget.com/tip/1,289483,sid14_gcu041736,00.html)

Scholtz, T. (2004). *The Benefits of an Information Security Architecture,* Meta Group, Dec 2004.

Vijayan, J. (2006). Possible S & P security holes reveal risks of e-Commerce. *Computerworld*, 34(22), May, 29 6.

Yeh, W-H., & Hwang, J-H. (2001). Hiding digital information using a novel system scheme. *Computers & Security*, 20(6), 533-538.

Young, G., & Pescatore, J., (2005, March 23). *Securing the Network Perimeter Is More Important Than Ever*, Gartner ID Number: G00126635