SAIS 2009 Proceedings

Southern (SAIS)

3-1-2009

Productivity and Usability Effects of Using a Two-Factor Security System

Dennis Strouble
dennis.strouble@afit.edu

Gregory M. Shechtman

Alan S. Alsop

PRODUCTIVITY AND USABILITY EFFECTS OF USING A TWO-FACTOR SECURITY SYSTEM

Dennis D. Strouble
Air Force Institute of Technology
Dennis.strouble@afit.edu

LtCol Gregory M. Schechtman
Air Force Institute of Technology
Gregery.schechtnan@afit.edu

Maj Alan S. Alsop
Defense Logistics Agency
Alan.alsop@dla.mil

ABSTRACT

The Department of Defense has mandated the use of a two-factor security system for access and authentication. The increased security of such a system has been extensively researched by the military. This research uses a survey to examine the effects on productivity and usability of implementing such a system.

Keywords

Two-Factor Security, Usability, Productivity, CAC,

INTRODUCTION

The security of information on a computer based system has always been a balancing act between the usability and productivity increase that a system provides and the actual security of the system. It has often been said that the safest system is one that is not connected to a network but then one gives up all of the advantages than using a network including access to the internet that it provides. Recently the Department of Defense (DoD) has issued a ban on the use of memory sticks, thumb drives, and camera flash memory cards to protect against adversary attacks and the result has been that a lot of organizations have had to change their ways of doing business with a resulting, at least temporary, loss of productivity. The military is currently in the process of moving to a two-factor identification system to increase security. This study looks at what is being given up to achieve that security and the cost of this improvement.

DoD has a long history of using a password authentication system for protection. As vulnerabilities to attacks have been exposed including social engineering exploits, new and stronger password requirements and procedures have evolved. The Air Force currently requires a password with 15 characters including a combination of upper and lower case, numbers, and symbols and a number of other rules to attempt to minimize the chance that it will be compromised. However, with numerous passwords to remember, users sometimes use shortcuts which make them vulnerable to attacks. One study found: 96% of users recycling or using similar password for multiple applications, 71% wrote their password down, 39% shared their password with others, 29 % used familiar names, places, or dates, and 68% changed a password to one that is easy to remember.

Since 1993, the DoD has been conducting evaluations of “smart card” technology. A smart card uses a complex embedded system that takes advantage of current technologies and microprocessors to insure that a user must use both the smart card and a PIN number in order to access a system. This is referred to a “two-factor authentication.” The user must have something, in this case a smart card known as a common access card (CAC) and know something, the PIN. The CAC is being evaluated or used for network authentication as well as a number of other applications. In November, 1999, the Deputy Secretary of Defense and the Defense Management Council decided to adopt the CAC card for identification, physical access, and as an authentication token. Guidance for the use of the card was incorporated into DoD directive 8190.3 dated 31 August 2002 and in August of 2004, Homeland Security Presidential Directive; HSPD-12 adopted the use of the CAC card for all federal employees and the contractors that work for the federal government.

This paper does not examine the security increases that have resulted from the use of the CAC card. This has been extensively studied by the DoD and the use of the CAC has been mandated. Rather this study looks at the effects on usability and productivity that have resulted from the implementation of the CAC. We examine two propositions:

P1 Usability will decrease with the need to have a physical object especially when away from the primary work place.

P2 Productivity will decrease with the use of the two-factor authentication.

METHODOLOGY

Data to examine these propositions was collected via a 40-item survey instrument using Likert items developed to question individuals using a new information system authentication technique. These questions were addressed aspects of network security behavior related to the two-factor authentication method, the user's physical control of smart cards, and remote access capabilities. Before administration, the new instrument was pilot tested on a sample of 20 subjects. The results of the piloting supported the instrument's reliability and content validity. The final instrument was sent via email to a representative sample of 4,530 military and civilian members of the United States Air Force. Of the 749 respondents, 313 provided usable responses for a final response rate of approximately 15%.

The data was first analyzed by statistically examining responses from both Likert style and binary (yes/no) questions. Once this was accomplished, we then conducted a qualitative review of the respondents' comments to opened items and the linkages that appeared between them. The results of this approached were deemed appropriate for an exploratory study intended to gauge real world reactions to a change in organizational information system processes. At each step, results were analyzed by two researchers and the results compared for reliability.

RESULTS

Research Question One: Usability

To answer the first research question, "Will usability of the networks decline as individuals find it more difficult to perform job tasks away from the primary workplace due to the requirement of having a smart card to authenticate?" In Table 1 we see that users that are required to use a CAC reader to access their email accounts from remote locations find the ease of remote access more difficult than those who are not required to use a CAC reader. It is apparent that users that can only access the email remotely via the use of a CAC reader find this new authentication technique to be significantly more difficult than those who do not have to use the CAC reader.

Question Asked	Question	Response						
	Number	*n*	Yes	No	DK	*		
To access your work email account remotely (e.g. Home, TDY, In Transit), do you have to use a CAC reader?	Q21	*725*	42.9	28.6	27.9	0.7		
			VD	SD	NC	LE	ME	*
Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely (All responses)	Q22	*725*	40.3	17.1	23.2	7.2	7	5.2
Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely (CAC required for remote access)	Q22	*311*	58.2	19.3	12.5	5.5	3.5	1
Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely (CAC not required for remote access)	Q22	*207*	33.8	16.4	29.5	8.7	9.2	2.4
			Yes	No	Some	*		
Do you feel that using the CAC and PIN authentication method is burdensome? (All Responses)	Q26	*725*	37.1	42.8	19.7	0.4		
Do you feel that using the CAC and PIN authentication method is burdensome? (CAC required for remote access)	Q26	*311*	44.1	33.4	22.2	0.3		
Do you feel that using the CAC and PIN authentication method is burdensome? (CAC not required for remote access)	Q26	*207*	34.3	46.9	18.4	0.5		
VD = Very Difficult; SD = Slightly More Difficult; NC = No Change; LE = Little Easier; ME = Much Easier								

Table 1: Results of CAC/PIN items

We also looked responses to whether a user considers the two-factor authentication method a burden versus their requirement to use the smart card reader remotely. Once again, based on the data in figure 1, there is a trend in which users that require a

CAC to access their email account remotely, consider the new CAC and PIN authentication method more burdensome than users not require a CAC

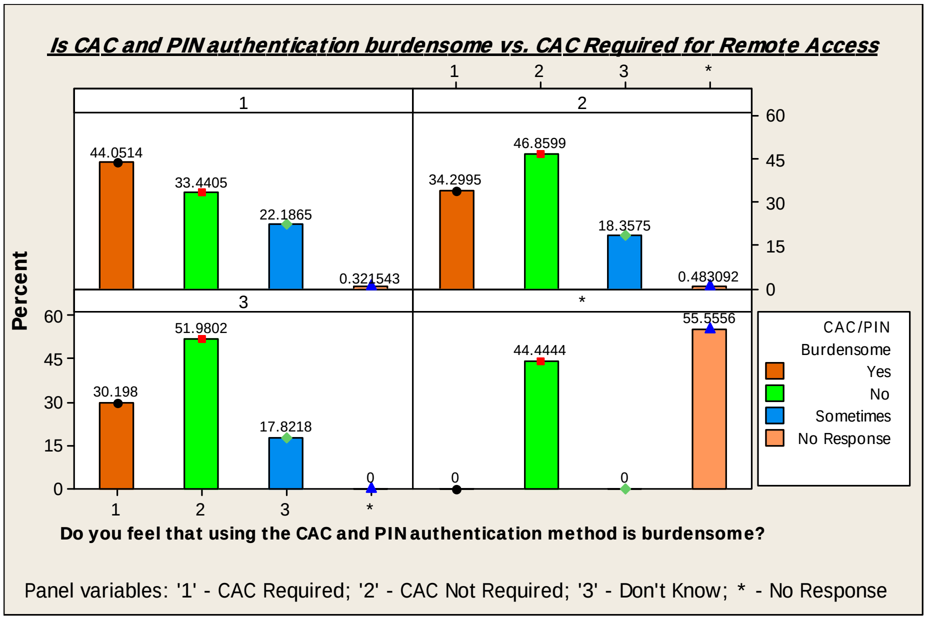

Figure 1 - CAC / PIN burden due to remote access ability

Finally, we also found that 35.5 percent of survey respondents stated that accessing email remotely is more difficult. Based on this analysis, we conclude that the network accessibility while away from their primary workplace has declined significantly due to the increased level of difficulty of getting access. This was one of the most heavily commented on concerns of the survey. Most users find that the inability to access their email from locations other than their primary workplace significantly hampers their ability to do their job and be responsive. For example, one response from the officer in charge (OIC) of a reserve unit stated, "The introduction of the CAC card for home use has decimated the communications channels that our reserve unit has spent years developing. We are now looking at going back to paper bulletins with stamps." This was their primary method of disseminating information and maintaining recall information for all the reservists in the unit. Due to the loss of ubiquitous remote email access capability because of the requirement for a CAC, normal communication capabilities were severely hampered. Collectively this evidence lends support to proposition 1's assertion that network usability would decrease with the need to use a two factor authentication system

Research Question Two: Productivity

To answer the second research question, we looked to see if the new authentication technique contributed to a loss in worker productivity. To do this, we analyzed this question by evaluating the respondent's answers to two questions. One that pertained specifically to the issue of users leaving their CAC behind in a card reader and another that determined CAC loss or theft attributed to the new authentication technique. Data from all CAC-loss items are shown in table 2

Questions	**Q#**	***n***	**Yes**	**No**	**Some**	*****		
With the new CAC/PIN authentication, do you have to leave your CAC in the card reader while accessing the network?	**Q12**	*725*	86.1	6.9	6.8	0.3		
In the last 6 month, have you inadvertently left your CAC behind in the computer?	**Q13**	*725*	66.8	33.2	n/a	0		
			1	**2**	**3**	**4**	**5+**	*****
In the last 6 months, how many times have you left your CAC at work, in the computer?	**Q14**	*484*	21.9	30.8	20	7.6	19	0.6
			G	**M**	**S**	**None**	*****	

How much did the new CAC/PIN authentication technique contribute to this?	**Q15**	*484*	69.4	10.1	9.1	11.2	0.2	
			Yes	**No**	*****			
Since implementation of the CAC and PIN to authenticate on the network, has your CAC been lost, stolen, or misplaced?	**Q17**	*725*	6.1	93.9	0			
			1	**2**	**3**	**4**	**5+**	*****
How many times has your CAC been lost, stolen, or misplaced?	**Q18**	*44*	77.3	13.6	4.5	0	2.3	2.3
			G	**M**	**S**	**None**	*****	
How much did the new CAC/PIN authentication technique contribute to loss, theft, or misplacement?	**Q19**	*44*	27.3	11.4	2.3	56.8	2.3	

Table 2—CAC loss survey items

To predict the number of CACs left behind based on a population of 491,786 military and civilian members, we used regression analysis to determine a 95 percent prediction interval and a fitted value. This regression model gave us 841,539 +/- 43,149 CACs left behind during a six month period. Using the fitted value of 841,539 instances in which users left their CAC behind, unsecured at a computer workstation during a six-month period, we extrapolated the value for a one-year period to be 1,683,078. Building on that number, we incorporated the results of the question, "When you left your CAC at work, did it cause you problems in accessing the base or base services?" Additionally, we assumed that the lost productive time per incident would be about 30 minute's total. That is 15 minutes for the person attempting to access the base and 15 minutes for the co-worker that has to go to the base entrance to either return their CAC or sign them onto the base. The results show that the USAF loses the equivalent of 261 work years, per year, just to grant individuals access to the base due to the new CAC and PIN authentication technique. If the average salary for personnel were 40,000 dollars a year, this would equate to 10.44 million payroll dollars a year spent on individuals to wait at the gate and signing people onto the base.

In addition to smart cards being left behind at work, the new authentication method also contributed to the loss and theft of smart cards. According to our data, 40.91 percent of the CACs that were lost or stolen in the last 6 months were the result of the new CAC and PIN authentication technique. Using the number of CACs that were lost or stolen and were not attributed to the new authentication technique (58 percent) as the baseline, we show an increase of lost or stolen smart cards by 72 percent. To predict the number of CACs lost or stolen based on a population of 491,786 military and civilian members, we used regression analysis to determine a 95 percent prediction interval and a fitted value. The regression model (figure 6) gives us 14,111 +/- 2,132 CACs that were lost or stolen in the last 6 months due specifically to the new CAC and PIN authentication technique.

This also incurs a cost in regards to time lost from accomplishing the mission. Using the fitted value of 14,111 instances in which users had their CAC lost or stolen during a six-month period, and an hour's time to replace the card, the USAF loses the equivalent of 14.11 work years, per year, to replace lost or stolen CACs due to the new CAC and PIN authentication technique. If the average salary for personnel were 40,000 dollars a year, this would equate to 564,400 payroll dollars a year spent on individuals just to replace their CAC card because theirs was lost or stolen due to the new authentication technique. Based on these results, we concluded that proposition two is supported and the use of a CAC and PIN authentication technique as implemented by the DoD has contributed to a loss in worker productivity and an increase in the loss or theft of CACs due to the increased insecure handling of the CAC.

DISCUSSION

This research took a systemic view of an organization seeking to secure its information systems via moving to a two factor authentication system. To the end, it looked at two related research questions. First, when an organization moves to such a system, does the enhanced security decrease system usability? Second, apart from usability concerns, does the move to two factor authentication system decrease employee productivity? To answer these questions, members of the U.S. Air Force were surveyed and asked their views on their experiences during that branch's migration to just such a system.

The results suggest that when the USAF moved to its two factor system it negatively impacted its members from both a network usability and overall productivity perspective. During the initial move to this system 2/3 of users left their CAC behind in the reader productivity losses upwards of 260+ person-years and $10.4 million. While these results are exploratory, it does identify the otherwise uncaptured losses that actually occurred to one organization making such a change.

When one gets past the productivity aspect, the network's usability was similarly degraded in the eyes of our survey respondents. Across almost every survey item, users who were required to use the CAC in order to access their email remotely found the system to be significantly more difficult and burdensome than those who are not required to use the CAC

Ultimately, this research produced interesting findings that have implications for any organization seeking to implement a two factor password system for their networks. The notion that such approaches provide enhance security is well documented. However, this research provides new insights into the unintended implications of implementing such a system in a real world organization. When the United States Air Force implement this type of security, while computer security goes up, the user's perception of the overall network's usability and the their own productivity are negatively impacted. Steps can be taken early on to possibly mitigate such perceptions and put into place processes that overcome the person-hour losses that this research has shown to affect real employees trying to accomplish their mission in a real world environment.

LIMITATIONS

No research is without limitations. This research was done on a military sample and its results may not generalize to the civilian sector. Additionally, some of the analysis was done on Boolean survey items. This may have caused us to lose some of the granularity other types of items may have provided. Finally, while this was intended to be an exploratory examination of actual workers using an operational information system, it should be noted that the survey did not capture all aspects of positive and negative implications of the move to a two factor authentication system. This may have potentially biased our results by inadvertently over emphasizing the negative aspects of this change on employees.

FUTURE RESEARCH

For the DoD, the CAC was supposed to replace all other tools that performed standard identification, physical access, and logical access to DoD installations and networks. The implementation of the CAC and PIN authentication method for network access has increased security, but at the cost of availability of the network and productivity of the user. There are plans to incorporate using the CAC for finance, medical and dental readiness, deployment readiness, and training. Before this is undertaken, it would be in the best interest of the USAF to analyze exactly 'how' the CAC is going to be used in order to reduce further vulnerabilities to loss, theft, damage, or misplacement. While having a single tool such as a CAC to access all these systems and services can make our lives easier, all considerations should be given to ensuring that users have it secured at all times. Any item with this much power represents a potential single point of failure and losing or misplacing it can seriously disrupt the capability and productivity of the owner.

DISCLAIMER

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

REFERENCE

1. Adams, Anne, *Users Are Not The Enemy*. Association for Computing Machinery, Communications of the ACM, 1999. 42(12): p. 40-46.

2. Braz, Christina, *Security and Usability: The Case of the User Authentication Methods*, in *IHM*. 2006, Association of Computing Machinery: Montreal, Quebec, Canada.

3. CSD, *Personal Identity Verification (PIV) for Federal Employees and Contractors: Federal Information Processing Standards (FIPS) Publication 201*, C.S.D.C.I.T. Laboratory, Editor. 2005, National Institute of Standards and Technology.

4. DoD/ACO, *Security of the Common Access Card*, D.o.D.A.C. Office, Editor. 2000, Department of Defense.

5. DoD/ACO, *DoD Smart Card Information Briefing*, D.o.D.A.C. Office, Editor. 2000, Department of Defense.

6. DoD, *Department of Defense Common Access Card Fact Sheet*, D.o. Defense, Editor. 2003, Department of Defense.

7. DoD, *Department of Defense Common Access Card White Paper*, D.o. Defense, Editor. 2001, Department of Defense.

8. Neumann, P.G., *Risks of Passwords.* Association for Computing Machinery, Communications of the ACM, 1994. **37**(4): p. 126.

9. Philippe Proust, J.-P.T., Laurent Sourgen, Fabien Germain, *High Security Smart Cards*, in *Design, Automation and Test in Europe Conference and Exhibition*. 2004, IEEE: Europe.

10. Scheuermann, D., *The smartcard as a mobile security device.* Electronics & Communication Engineering Journal, 2002: p. 205-210.

11. Shelfer, Katherine J.D.P., *Smart Card Evolution.* Comminications of the ACM, 2002. 45(7): p. 83-88.

12. White-House, *Homeland Security Presidential Directive/HSPD-12*. 2004.