Computer Security Economics Based On Risk Analysis Of Multilevel Authentication Design For Access Control

FORD LUMBAN GAOL
Faculty of Computer Science
Bina Nusantara University
Jl. Kebon Jeruk No27, Jakarta.
INDONESIA
fgaol@binus.edu

Abstract: - Several password techniques for multilevel authentication mechanism in the development of secondary password are presented. These include user-selected passwords, system-generated passwords, passphrases, cognitive passwords, and associative passwords. A comparative evaluation on the users ' memorability and users' subjective preferences for those various password mechanisms was conducted. The Return on Investment (ROI) of the access control was calculated based on the result of the users ' memorability and risk analysis. From the comparative evaluation and the study on the ROI of the access control, it can be concluded that cognitive passwords and associative passwords appear to be the most appropriate techniques for secondary passwords.

Key-Words: - user preferred password, ease of recall, secondary password, return on investment, Cost Based Analysis, Value of Information

1 Introduction

The feasibility study for access control to determine the alternative multilevel passwords have to be determined from the side of cost effective before the implementation of the access control. Economical justification for control access is the most difficult stage before the implementation since the economical value of control access are classified as the intangible value.

Generally, there are two areas that have become focus of the project feasibility study from the economical perfective (Siponen & Kukkonen, 2007; Anderson and Moore 2006; Moran and Moore, 2010; Moore, et al., 2009; Bohme and Moore, 2009):

1. How effective in terms of economics the implementation of that project?
2. How can we decide which one for those methods that has the lowest price

We identify six variables that specially analyze for access control project:

1. Present cost capital.
2. The cost for the access control itself.
3. The failure probabilities of the system
4. The tax interest.
5. The yearly benefit, and
6. System lifetime.

The access control project has to determine the risk of the project (Pfleeger and Pfleeger, 2006 ; Aceituno, 2005; Kumar, et al., 2010)). The mathematical modeling for this problem has to use the Risk Analysis and Cost Based Analysis (CBA). We call Computer Security Economics based on Risk Analysis (CSEbRA) as the combination of Cost Based Analysis (CBA) and Risk Analysis (RA) Approach.

CSEbRA is the combination of CBA and RA as the input to calculate Return of Investment (RoI)

2 Computer Security Economics Based on Risk Analysis

Computer Security Economics Based on Risk Analysis consists of Risk Analysis and Cost Analysis. At this section, we will discuss in depth about those parts.

2.1. The Multilevel Authentication

To implement the multilevel authentication we will adopt 7 (seven) principles from (Furnell & Katsikas, 2008; Moore, et al., 2009; Moore and Clayton., 2009).

In this paper we will examine for 5 (five) type of passwords:

1. User-Generated Password

User-generated password is the most traditional password. Access control with user-generated password is the most general that implement in

Operating System. The user will get the user-id and create password that only known by the user him/her self. Ideally the password has to be long enough that consists of characters and easy to remember by the user (Myers, 2009). This method introduces in the first time by L.S. Hoffman in IBM Data Security Centre in 1979 [Fisher, 2006].

2. System-Generated Password.
In system generated password, access control was generated by the operating system and grant it to the used. Basically, this method use pseudo-random number that generated the random number. In (Payne & Edwards, 2008), Payne & Edwads discuss in detail about system generated password.

3. Pasphrarase
Pasphrarase is the other form of user-generated password. Pasphrarase is the list of the words that has meaning. Example: "to_be_or_not_to_be". This method was introduced in the first time in 1982 and discuss in depth in (Harrisa & Lib, 2010). This access control was designed to overcome the user problem due to difficulties to memorize the password.

4. Cognitive Password
Cognitive password is the password that introduced in the first time by Zviran and Haga in 1998 and discusses in depth in (Bertino & Sandhu, 2005; Dhillon, 2006). This method base on "Question and Answer." The user will ask to answer certain questions that related with his/her profile.

5. Associative Password.
Associative password introduce on the first time in 1987 and discussed in depth in (Zviran & Erlich, 2006). In this access control with associative-password, the user will ask to construct the list of "Statement and response" for certain theme.

2.2. Cost Based Analysis

On Cost Base Analysis, the major consideration is the effective use of the cost that allocated to the project. The Cost Base Analysis reflected with the interest rate that given from the sponsor that reflected with the rate of return with the certain investment (Birchler & Bütler, 2007). The rate that we use is known as T-Bill Rate or hurdle. The T-Bill rate is known as the minimum rate that have to be exceed if we want the project financially sound. If the expected rate of return below than the hurdle rate then the project is not feasible in terms of the cost.

To evaluate the benefit of the project, we used the method NPV (*Net Present Value*) and IRR (*Internal Rate of Return*). Prior to calculate NPV and IRR, we have to calculate *PV* (*Present Value*).

Present Value (*PV*)
Present Value or PV is *Discounted Cash Flow* from investment as the amount that have to be invested using *k*% interest per year or known as discount rate at the end of *n* years will accumulate *FVn* (*Future Value*).
The relationship between FV and FVn can be written as follow:

$$PV = \frac{FVn}{(1+k)^n} \quad \text{.....1}$$

NPV (*Net Present value*)
NPV (Net Present Value) was defined as the accumulation from PV for each of investment period or cash stream minus the initial cost for certain project. One investment will be feasible if NPV is positive value

$$NPV = \sum_{t=0}^{n} \frac{PV_t}{(1+k)^t} \quad \text{.....2}$$

where:
n = number of period;
t = period of ;
PV_t = *Cash Flow*);
k = *discount rate* (%);
NPV = *Net Present Value*.

IRR (*Internal Rate of return*)
IRR was defined as the future discount rate that equivalent with the value of investment. If IRR bigger than discount rate then the investment is feasible. IRR is equal with the amount of interest r from PV for the cash out flow.

$$\sum_{t=0}^{n} \frac{PV_t}{(1+r)^t} = 0 \quad \text{.....3}$$

Where : n = number of period;
t = Period of ;
r = *discount rate* in %; and
CF_t = Cash Flow.
The equation number (3) will be solved for the value of r using Newton iteration method.

2.3. Binomial Distribution

We have to know the type of distribution before evaluate the possibility of failure. For this case, there are two possibility, Fail or Success. This case was known as Binomial Distribution.

$$b(x, n, p) = \binom{n}{x} p^{x} q^{n-x} \text{ ..... .4}$$

Where :
p = the possibility of password failure
q = 1-p;
n = number of respondents; and
x = Number of password failure from n tests

3 Financial consideration for alternative Access Control

Financial considerations are needed to determine the feasibility of the project in terms of economically. The discussion will be focused on cost saving from implementation of access control and the calculation of the breakeven that basically taken from Net present Value (NPV) (Shawn, 2002; Anderson and Moore, 2006).

3.1. Assumptions

We will analyze the alternative access control from some assumptions. All of the assumptions will be used in US$ as the currency and US tax federal as the regulations [Downes & Goodman**,** 2010).

1. *Corporate tax Rate*
   United Stated companies will get tax 34% or more if their revenue more than US$ 335,000/year.

2. *Cost of Capital*
   Cost of Capital will be influenced by the capital market globally from organization itself. Cost of capital will be adhere with US Government Bonds with maturity 5 years with the amount of 5.59%.

3. Cost of Control Access Project
   Cost of this project will be determined as US$ 200 for each user. The amount of the cost will be constant for ROI project calculation.

4. The number of control access use/year.
   Assumed that the use of control access is five times/day. This reference number was taken from the average of all users that use the control access /day. In one year, the effective day work is 212 days, so there are 1060 times the users will use the control access in one year.

5. *Time to Verify Password*
   Time to verify to control access used these standards:

Table 1. Time to verify for each password alternative Password

Password	Verification (second)
Self-Generated	2
Associative	6
Cognitive	6
Passpharase	4
System-Generated	3

6. Salary employee/hour
   Assume that the net salary/year is US$ 30,000 added with 20% bonus. Bonus is dividend that delivers to the employee. The total of salary and bonus is US$ 36,000. The effective working hours in one day is 8 hours or 1696 hours/years. So for each hour the employee will get US$ 21.2.

7. *Annual Maintenance*
   Yearly maintenance for this alternative password will use as the standard to update each password that required US $ 5 that included with the password form.

Table 2. yearly maintenance

Password	Cost (US $)
Self-Generated (Estimated will be used 51.68 times/year)	51.68 X 5 = 258.4
Associative (Estimated will be used 20 times/year)	20 X 5 = 100
Cognitive (Estimated will be used 20 times/year)	20 X 5 = 100
Passpharase (Estimated will be used 51.68 times/year)	51.68 X 5 = 258.4
System-Generated (Estimated will be used 51.68 times/year)	51.68 X 5 = 258.4

8. *Cost of Information*
   Cost of information is the value of accessibility of information to the user (in US$). Cost of information predicts in the range of US$ 10,000 to US $ 1,000,000,- with median range from US$ 100,000 to US$ 1,000,000,- with median US$ 100,000,-. The cost of information become the variable of ROI.

9. *Cost for System Failure*
   We will divide the cost for system failure become *system reconstruction* and *cost of information*. The reconstruction cost defined as the cost for the recovery time (in hours) times with the salary of the employee/hour. The cost for loosing of information is the value of the information itself. The cost for the failure of information is the cost for the lost or the leak of information and the cost to fix the system

10. *Probability of System Failure*
    The threat that cause the failure of access control from the user side due the relationship of the system to the outer world. The probability of the system failure will use the standard how easy to recall the password in % (Gaol and Johnson. 2000).

Table 3. Probability the success and failure to recall the password for 120 users in 3 months

Password	*ease of recall*	*Failed of recall*
self-Generated	27.5%	100%-27.5%=72.5%
Associative	69%	100%-69%=31%
Cognitive	74%	100%-74%=26%
Passphrase	25%	100%-25%=75%
System-Generate	19.2%	100%-19.2%=80.8%

Table 4. Probability the failure to recall the password in one year

Password	*Failed of recall*
self-Generated	2.13%
Associative	0.91%
Cognitive	0.77%
Passphrase	2.21%
System-Generate	2.38%

Example: the probability for self-generated password for 120 respondent in 60 days. So, for one person in 212 days = (72.5%/120) X (212/60) = 2.13%

3.1. Return on Investment (ROI) Calculation

1. *Discount Rate* will use the assumption on Number 2.
2. *Corporate Tax rate* (%) will use the assumption on Number (1)
3. *Number of Verification/ Year* will use the assumption on Number (4)
4. *Amount of Time/Verification* (*second*) will use the assumption on Number (5).
5. *Hourly Salary*(*US $*) will use the assumption on number (6)
6. *Effective Working Time/Day* (*hour*) will use the assumption on number (6)
7. *Number of Users* is the total of user that will be tested.
8. C*ost of Control Access/User* (US$) will use the assumption on number (3)
9. *Annual Maintenance /user (US $)* will use the assumption on number (7).
10. *Value of Information (US $)* will use the assumption on number (8).
11. (*Cost of One Malfunction System (US $)) = Value of Information + (Hourly Salary * Effective working/day)*. This formula will use the assumption on number (9).
12. *Probability of Malfunction System* will assume from the Table 3.
13. *Probability of at Least One Password Being Failed* used with binomial distribution equation:
$$b(x,n,p)=\binom{n}{x}p^{x}q^{n-x}$$
14. *Probability of No Password Being Failed* = 1-*Probability of at Least One Password Being Failed.*
15. *Probability of at Least One Password Being Failed = ((Cost of One Malfunction * Probability of At Least One Password Being Failed*) – *Cost of Control Access) * Number of Users.*
16. The amount of cost (US $)) for probability of *Probability of No Password Being Failed =* (*Cost of Control Access * Probability of No Password Being Failed.* * *Number of Users*) * *Number of Users.*
17. The initial cost is (*Total Initial Purchase (US $)*) = (*Cost of Control Access/Users*) * (*Number of Users)*.
18. *Total Savings/cost (US $*).

19. *Total Annual Maintenance(US $)*) = *Annual Maintenance * Number of users.*
20. *(Total Cost of Verification* (*US $*)) = (*Hourly Salary*/3600)*(*Amount of time/ verification) * (number of verification/year*) * *Number of users*.
21. *Yearly total (US $)*) = *Total Saving/Cost + Total annual maintenance + Total cost of Verification.*
22. *Tax Expense (US $)*) = *Yearly total * Corporate tax Rate*.
23. *Total Cash for Period (US $)) = Yearly total – Tax expense*.
24. NPV (*Net Present Value*).
25. IRR (*Internal Rate of Return*).

4 Return On Investment

1. The calculation of ROI (*Return on Investment*) for each all of the *password* (*Self Generated, Passphrase, Cognitive, Associative,* & *System Generated*) used these mathematical standards:

Table 5. Constant and Variable that used in ROI Calculation**.**

Name	TYPE	
	Constant	Variable
Discount Rate	*Probability and Number of User*	*Value of Information*
Corporate Tax Rate		
Number of Verification/Year		
Amount of Time/Verification		
Hourly Salary		
Effective working days		
Number of Users		
Cost of Control Access		
Annual Maintenance		

2. For each of alternative password will give with the value of different information. ROI calculation indicates that for each used of alternative passwords Self Generated, Passphrase, Cognitive, Associative, & System Generated, will be represented on the appendixes on Chart 1, 3, 5, 7, 9.

3. For each of alternative password will give with the value of different information. ROI calculation indicates that for each used of alternative passwords *Self Generated, Passphrase, Cognitive, Associative,* & *System Generated,* are feasible to implement. For each of alternative password will be represented on the appendixes on Chart 3, 5, 7, .9.

Table 6. Value of Information for one user

password	Value of Information (US $)
Self Generated	34,390
Associative	66,305
Cognitive	79,125
Passphrase	33,797
System generated	31,082

We can conclude that using the cognitive password will have the value of information higher than other alternative password.

4. Base on the calculation, we can conclude that the effectiveness of a control depends on the information value that resides on the system itself. This was proven by the calculation result for each alternative passwords base on the appendices on Chart 2, 4, 6, 8, 10. Each of the alternative password produce NPV with positive value that shown that the project is feasible if the value of information equal with 0.

5. Each addition for one user will reduce the value of information. This is happen due to the disparity of the failure of the password in Binomoal distribution become smaller such as deduction of the saving value will imply to the value of information become smaller than before.

6. In the certain case, the addition of the users will be in the equilibrium state where the value of information will not change. This point known as breakeven point for each of alternative password. The details as follow:

Tabel 7. *Breakeven* points for each of the alternative passwords

password	*Breakeven* points (user)	Value of Information (US $)
Self Generated	475	376
Associative	1075	251
Cognitive	1275	251

Passphrase	475	387
System generated	475	380

The possibility of the system failure will increase if the number of users increase. If the probabilities of the system failure increase that will add the cost saving and reduce the breakeven point. This situation will cause cognitive password has the highest breakeven point, i.e. 1275 with the smallest value of information, i.e. 251
For the further result, look at on Chart 1, 2, 3, 4, 5 .

7. The value of information that reside have relationship with the probability of system failure such that the feasibility to the cost that occur have to count user as one of the variables.

5 Conclusion

In this paper we already discussed:

- *Use- Generated Password*
- *System-Generate password*
- *Passphares Password*
- *Cognitive Password.*
- *Associative password.*

Base on the testing for *user* and *ease-of-recall* we can have this result:

- ***SELF-GENERATED PASSWORD***
  - ✓ There is no relationship for the choice of *Self-Generated Password* and *recall of success*.
  - ✓ There is relationship between format of *Self-Generated Password* and *recall of success*. In this case, 94% respondent able to recall the password correctly using alphabet format.
  - ✓ Number of characters on the password do not influence to the recall of success.
- ***SYSTEM-GENERATED PASSWORD***
  - ✓ In S*ystem-Generated Password*, the ability to recall the password will be determined by the type of password, in this case *pronounceable*.
  - ✓ The difficulties to remember the password push the user to wrote down the password in piece of paper.
- ***COGNITIVE PASSWORD***
  - ✓ We find some differences between *recall of success* between *fact-based* and *opinion-based*.
  - ✓ The probability of password recall for *fact-based* is higher than *opinion based*.
- ***ASSOCIATIVE PASSWORD***
  - ✓ More than 90% of users give corrects answer from all of the users. The theme of the password is crucial.
- ***PASSPHRASE***
  - ✓ Level of *recall of success passphrase* is around 25%. This is reflecting that only small number of users that able to retrieve password correctly.
    - ✓ There are only 10% of users that able to memorize the *passphrase* password..

Base on Spearman Test on Table 8, we can conclude that there is no relationship between *ease of recall* and *user preferred password.*
Using r*ecall success score* as risk indicator, we have compute ROI and the result as follow.

- *Cognitive password* produces the highest value of information for one user.
- For each additional user, it will decrease the value of information. This will give impact that the distribution of password failure will be smaller
- *Cognitive password* wil produce the highest point for *breakeven* that is 1275 users with the smallest value of information that is US $ 251.

Table 8. The comparison between ease of recall and user preferred password

password	*Ease of recall rank*	*Recall success score (%)*	*Actual recall success rank*
Self-Generated	1	27.5	3
Associative	2	68	2
Cognitive	3	74	1
Passpharse	4	25	4
System-Generated	5	19.2	5

5 Further Study

We can expand the method in assessing of control access into another security fields such as feasibility study for firewall and feasibility study for e-commerce authentication.

References:

[1] Kumar, V., Srivastava, J., Lazarevic, A., "Managing Cyber Threats: Issues, Approaches, and Challenges (Massive Computing)." Springer; 2010.

[2] Payne, B.D and Edwards, "W.K. A Brief Introduction to Usable Security." Internet Computing 12(3), pp. 13-21., May-June 2008. doi: 10.1109/MIC.2008.50

[3] Downes. J. and J.E. Goodman, "Dictionary of Finance and Investment Terms " Barron, 8th ed, (2010).

[4] Siponen, M & Kukkonen, H., " A review of information security issues and respective research contributions." ACM SIGMIS *Database*, **38(1)**, pp. 16-25., October 2007. doi: 10.1145/1216218.1216224

[5] Fisher, P., "Information System Security." wiley, USA., 2006.

[6] Bertino, E & Sandhu, R., "Database security - concepts, approaches, and challenges.' IEEE Transactions on Dependable and Secure Computing, **2(1)**, pp. 2 - 12., April 2005. doi: . 10.1109/TDSC.2005.9

[7] Gaol, F.L. and T. Johnson, "Alternative password for multilevel authentication mechanism". Technical Report, Faculty of Computer Science, University of Indonesia., April 2000.

[8] Myers, D., "Exploring Psychology." 3rd Ed., Worth Publisher, pp: 223-253., 2009

[9] Shawn, BF., " Security Attribute Evaluation Method: A Cost Benefit Approach." Proceedings International Conference on Software Engineering 2002

[10] Birchler, U & Bütler, M., "Information Economics (Routledge Advanced Texts in Economics and Finance)." Routledge, USA., 2007.

[11] Pfleeger, C.F. & S.L. Pfleeger, "Security in Computing." Prentice-Hall, NJ., 2006.

[121] Harrisa, D & Lib, W. C., "An extension of the Human Factors Analysis and Classification System for use in open systems ." Theoretical Issues in Ergonomics Science, **1**, pp. 54-56., Jan 2010. doi: 10.1080/14639220903536559

[13] Zviran, M & Erlich, Z., "Identification and Authentication: Technology and Implementation Issues." Communications of the Association for Information Systems: Vol. 17 (4)., Feb 2006 doi: 10.1016/0167-4048(87)90027-7

[14] Furnell, SM, & Katsikas, S., "Securing Information and Communications Systems;, Principles, Technologies, and Applications Artech House Publishers; 2008.

[15] Aceituno, V., "On Information Security Paradigms", ISSA Journal, September, 2005.

[16] Dhillon, G., "Principles of Information Systems Security: Texts and Cases" wiley, USA., 2006

[17] Anderson, R., and T. Moore, "The economics of information security." Science 314 (5799), pp.610–613., Oct, 2006. doi: 10.1126/science.1130992).

[18] Moran, T. and T. Moore, "The phish market protocol: Securely sharing attack data between competitors". Financial Cryptography Data Security., 2010:. doi; 10.1145/1655925.1655932

[19] Moore, T., R. Clayton and R. Anderson, "The economics of online crime." J. Econ. Perspectives 23(3), pp. 3-20., Sept 2009. doi: 10.1257/jep.23.3.3

[20] Bohme, R. and T. Moore, "The iterated weakest link–A model of adaptive security investment." Proceedings of 8th Workshop on the Economics of Information Security (WEIS)., London, UK., June, 24 2009. doi; 10.1109/MSP.2010.51

[21] Moore,T., R. Clayton and H. Stern,2009 "Temporal correlations between spam and phishing websites." Proceedings of 2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '09)., Boston, MA., April 2009. doi: 10.1145/1299015.1299018

[22] Moore, T. and R. Clayton, 2009 "Evil searching: Compromise and recompromise of internet hosts for phishing." Proceedings of 13th International Conference on Financial Cryptography and Data Security., Barbados., Feb 2009. doi; 10.1007/978-3-642-03549-4.16

Appendixes

Calculation of Return On Investment (ROI)

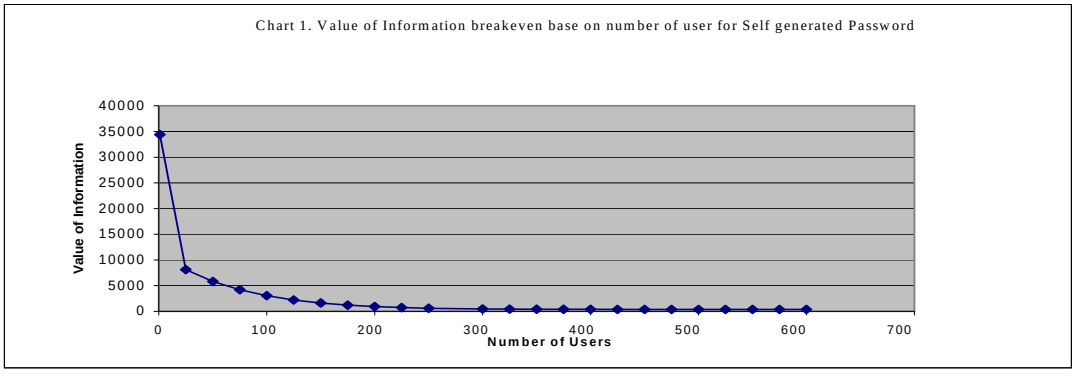
1. Calculation of ROI for Self-Generated Password

Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	2	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200	
Annual Maintenance/Users (US $)	$ 258.4	
Value of Information (US $)	$ 34,390	
Cost of One Malfunction System (US $)	$ 34,560	
Probability		
p(1)= Control access being failed	0.021	
p(1)= Control access being succeeded	0.979	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.021	$537.75
No password being failed	0.979	$ (195.73)
Total Savings/cost		$342.02
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ 342.02
Total Annual Maintenance (US $)		$ (258)
Cost of Verification (US $)		$ (12.48)
Yearly Totals (US $)		$ 71.14
Tax Expense/credit (US $)		$ (24.19)
Total cash for period (US $)	$ (200)	$ 46.95
NPV of Project	$ 0.0	
IRR of Project	5.59%	

Figure 1 Value of Information for One User

Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	2	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200	
Annual Maintenance/Users (US $)	$ 258.4	
Value of Information (US $)	$ 0	
Cost of One Malfunction System (US $)	$ 170	
Probability		
p(1)= Control access being failed	0.021	
p(1)= Control access being succeeded	0.979	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.021	$ (196.38)
No password being failed	0.979	$ (195.73)
Total Savings/cost		$ (392.11)
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ (392.11)
Total Annual Maintenance (US $)		$ (258)
Cost of Verification (US $)		$ (12.48)
Yearly Totals (US $)		$ (662.99)
Tax Expense/credit (US $)		$ 225.42
Total cash for period (US $)	$ (200)	$ (437.58)
NPV of Project	$ (2,064.0)	
IRR of Project	#NUM!	

Figure 2. NPV for the project for the value of information = 0



2. Calculation of ROI for Associative Password

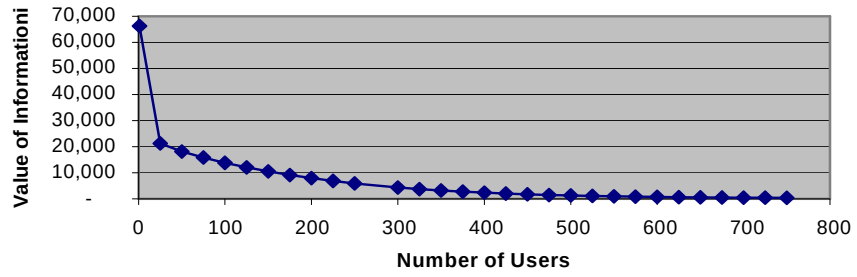
Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	6	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200	
Annual Maintenance/Users (US $)	$ 100	
Value of Information (US $)	$ 66,305	
Cost of One Malfunction System (US $)	$ 66,475	
Probability		
p(1)= Control access being failed	0.009	
p(1)= Control access being succeeded	0.991	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.009	$ 406.77
No password being failed	0.991	$ (198.17)
Total Savings/cost		**$ 208.59**
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ 208.59
Total Annual Maintenance (US $)		$ (100.00)
Cost of Verification (US $)		$ (37.45)
Yearly Totals (US $)		$ 71.14
Tax Expense/credit (US $)		$ (24.19)
Total cash for period (US $)	$ (200)	$ 46.95
NPV of Project	$ 0.0	
IRR of Project	5.59 %	

Figure 3. Value Of Information for One User

Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	6	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200	
Annual Maintenance/Users (US $)	$ 100	
Value of Information (US $)	$ 0	
Cost of One Malfunction System (US $)	$ 170	
Probability		
p(1)= Control access being failed	0.009	
p(1)= Control access being succeeded	0.991	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.009	$ (198.45)
No password being failed	0.991	$ (198.17)
Total Savings/cost		**$ (396.63)**
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ (396.63)
Total Annual Maintenance (US $)		$ (100.00)
Cost of Verification (US $)		$ (37.45)
Yearly Totals (US $)		$ (534.08)
Tax Expense/credit (US $)		$181.59
Total cash for period (US $)	$ (200)	$ (352.49)
NPV of Project	$ (1,701.54)	
IRR of Project	#NUM!	

Figure 4. NPV for the project for the value of information = 0

Chart 2. Value of Information breakeven base on number of user for *Associative Password*



3. Calculation of ROI for Cognitive Password

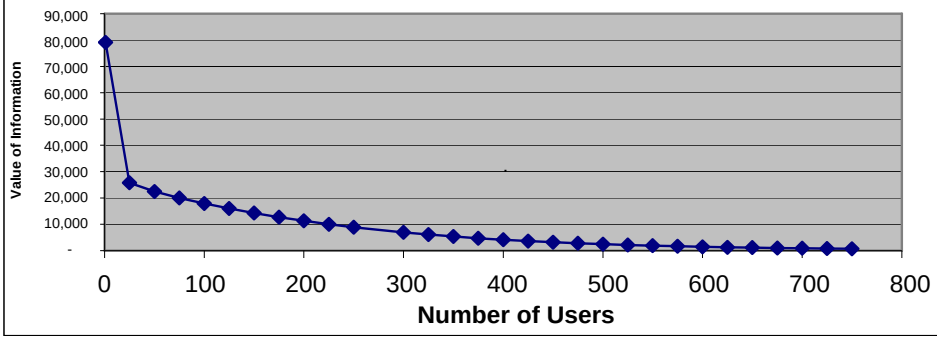
Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	6	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200.00	
Annual Maintenance/Users (US $)	$ 100.0	
Value of Information (US $)	$ 79,125	
Cost of One Malfunction System (US $)	$ 79,295	
Probability		
p(1)= Control access being failed	0.008	
p(1)= Control access being succeeded	0.992	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.008	$ 407.0 4
No password being failed	0.992	$ (198.47)
Total Savings/cost		$ 208.58
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ 208.58
Total Annual Maintenance (US $)		$ (100)
Cost of Verification (US $)		$ (37.45)
Yearly Totals (US $)		$ 71.12
Tax Expense/credit (US $)		$ (24.18)
Total cash for period (US $)	$ (200)	$ 46.94
NPV of Project	$ 0.0	
IRR of Project	5.59%	

Figure 5 Value of Information For One User

Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	6	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200.00	
Annual Maintenance/Users (US $)	$ 100.0	
Value of Information (US $)	$ 0	
Cost of One Malfunction System (US $)	$ 170	
Probability		
p(1)= Control access being failed	0.008	
p(1)= Control access being succeeded	0.992	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.008	$ (98.70)
No password being failed	0.992	$ (198.47)
Total Savings/cost		$ (397.17)
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ (397.17)
Total Annual Maintenance (US $)		$ (100)
Cost of Verification (US $)		$ (37.45)
Yearly Totals (US $)		$ (534.62)
Tax Expense/credit (US $)		$ 81.77
Total cash for period (US $)	$ (200)	$ (352.85)
NPV of Project	$ (1,703.1)	
IRR of Project	#NUM!	

Figure 6. NPV for the project for the value of information = 0

Chart 3. Value of Information breakeven base on number of user for *Cognitive Password*



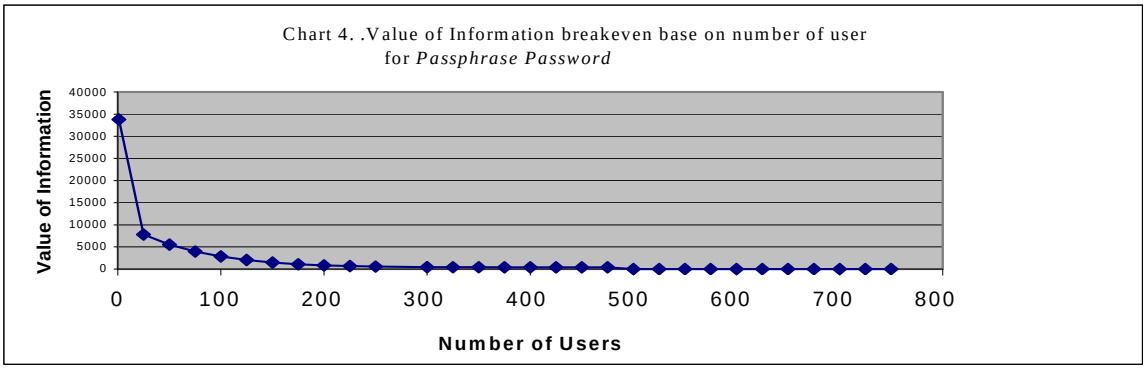
4. Calculation of ROI for Passphrase Password

Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	4	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200	
Annual Maintenance/Users (US $)	$ 258.4	
Value of Information (US $)	$ 33,797	
Cost of One Malfunction System (US $)	$ 33,967	
Probability		
p(1)= Control access being failed	0.022	
p(1)= Control access being succeeded	0.978	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.022	$ 550.10
No password being failed	0.978	$ (195.58)
Total Savings/cost		$ 354.51
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ 354.51
Total Annual Maintenance (US $)		$ (258)
Cost of Verification (US $)		$ (24.97)
Yearly Totals (US $)		$ 71.14
Tax Expense/credit (US $)		$ (24.19)
Total cash for period (US $)	$ (200)	$ 46.95
NPV of Project	$0.0	
IRR of Project	5.59%	

Figure 7. Value Of Information For One User

Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	4	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200	
Annual Maintenance/Users (US $)	$ 258.4	
Value of Information (US $)	$ 0	
Cost of One Malfunction System (US $)	$ 170	
Probability		
p(1)= Control access being failed	0.022	
p(1)= Control access being succeeded	0.978	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.022	$ (196.25)
No password being failed	0.978	$ (195.58)
Total Savings/cost		$ (391.84)
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ (391.84)
Total Annual Maintenance (US $)		$ (258)
Cost of Verification (US $)		$ (24.97)
Yearly Totals (US $)		$ (675.21)
Tax Expense/credit (US $)		$ 229.57
Total cash for period (US $)	$ (200)	$ (445.64)
NPV of Project	$ (2,098.3)	
IRR of Project	#NUM!	

Figure 8. NPV for the project for the value of information = 0



5. Calculation of ROI for System Generated Password

Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	3	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200.00	
Annual Maintenance/Users (US $)	$ 258.4	
Value of Information (US $)	$ 31,082	
Cost of One Malfunction System (US $)	$ 31,252	
Probability		
p(1)= Control access being failed	0.024	
p(1)= Control access being succeeded	0.976	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.024	$ 543.51
No password being failed	0.976	$ (195.24)
Total Savings/cost		$ 348.27
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ 348.27
Total Annual Maintenance (US $)		$ (258)
Cost of Verification (US $)		$ (18.73)
Yearly Totals (US $)		$ 71.14
Tax Expense/credit (US $)		$ (24.19)
Total cash for period (US $)	$ (200)	$ 46.95
NPV of Project	$0.0	
IRR of Project	5.59%	

Figure .9 Value Of Information For One User

Discount Rate (%)	5.59%	
Corporate Tax Rate (%)	34%	
Number of Verification/Year	1060	
Amount of time/verification (second)	3	
Hourly Salary (US $)	$ 21.2	
Effective Working/Day (Hour)	8	
Number of Users	1	
Cost of Control Access/Users (US $)	$ 200	
Annual Maintenance/Users (US $)	$ 258.4	
Value of Information (US $)	$ 0	
Cost of One Malfunction System (US $)	$ 170	
Probability		
p(1)= Control access being failed	0.022	
p(1)= Control access being succeeded	0.978	
Probability of Malfunction System		**Cost / savings**
At least one password being failed	0.022	$ (196.25)
No password being failed	0.978	$ (195.58)
Total Savings/cost		$ (391.84)
Cash Flow Analysis		
Year	**0**	**Years 1-5**
Initial Purchase (US $)	$ (200)	
Total Savings/Cost (US $)		$ (391.84)
Total Annual Maintenance (US $)		$ (258)
Cost of Verification (US $)		$ (24.97)
Yearly Totals (US $)		$ (675.21)
Tax Expense/credit (US $)		$ 229.57
Total cash for period (US $)	$ (200)	$ (445.64)
NPV of Project	$ (2,098.3)	
IRR of Project	#NUM!	

Figure 10. NPV for the project for the value of information = 0