LAPPEENRANTA UNIVERSITY OF TECHNOLOGY
Department of information technology

Mikko Ylén

CENTRALIZED PASSWORD MANAGEMENT IN A GLOBAL ENTERPRISE

The topic of the master's thesis has been confirmed by the Department Council of the Department of Information Technology on 15th of September 2004.

Examiners for this thesis were Professor Jari Porras and MSc Jan-Erik Grön.
Supervisor was Jari Ilmonen.

Lappeenranta, 2 November 2004

_____

Mikko Ylén
Keskikatu 2 as 23
FIN-45100 Kouvola

ABSTRACT

Lappeenranta University of technology
Department of information technology

Mikko Ylén

Centralized password management in a global enterprise

Master's thesis
2004
84 pages, 23 figures, 6 tables and 2 appendices

Examiners: Professor Jari Porras, MSc Jan-Erik Grön
Supervisor: Jari Ilmonen
Keywords: password, information security, synchronization

User authentication in computer systems has been a cornerstone of computer security for decades. The concept of a user id and passwords is the most cost effective and widely used method of maintaining a shared secret between a user and a computer system. In the early days of corporate computing with only few computer systems and a small selected group of users, this model was proven effective. Over the years the number of system grew and so did the number and diversity of passwords users had to remember. No one could foresee how much password related problems employees would face every day, how much passwords would overload corporate helpdesks and how significant security risks they would cause to enterprises.

This thesis takes a look at the problems caused by passwords in a large, global enterprise. The problem is approached from four different perspectives; human, technology, security and business. The problems will be demonstrated by introducing results from an employee survey conducted as part of this thesis. A solution to these problems is introduced in a form of a centralized password management system. Features of this concept will be evaluated and a proof-of-concept type of implementation will be made to demonstrate the functionality and usability of this concept.

TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto
Tietotekniikan osasto

Mikko Ylén

Keskitetty salasanojen hallinta globaalissa yrityksessä

Diplomityö
2004
84 sivua, 23 kuvaa, 6 taulukkoa ja 2 liitettä

Tarkastajat: Professori Jari Porras, diplomi-insinööri Jan-Erik Grön
Ohjaaja: Jari Ilmonen
Avainsanat: salasana, tietoturva, synkronointi

Käyttäjien tunnistaminen tietojärjestelmissä on ollut yksi tietoturvan kulmakivistä vuosikymmenten ajan. Ajatus käyttäjätunnuksesta ja salasanasta on kaikkein kustannustehokkain ja käytetyin tapa säilyttää luottamus tietojärjestelmän ja käyttäjien välillä. Tietojärjestelmien käyttöönoton alkuaikoina, jolloin yrityksissä oli vain muutamia tietojärjestelmiä ja niitä käyttivät vain pieni ryhmä käyttäjiä, tämä toimintamalli osoittautui toimivaksi. Vuosien mittaan järjestelmien määrä kasvoi ja sen mukana kasvoi salasanojen määrä ja monimuotoisuus. Kukaan ei osannut ennustaa, kuinka paljon salasanoihin liittyviä ongelmia käyttäjät kohtaisivat ja kuinka paljon ne tulisivat ruuhkauttamaan yritysten käyttäjätukea ja minkälaisia tietoturvariskejä salasanat tulisivat aiheuttamaan suurissa yrityksissä.

Tässä diplomityössä tarkastelemme salasanojen aiheuttamia ongelmia suuressa, globaalissa yrityksessä. Ongelmia tarkastellaan neljästä eri näkökulmasta; ihmiset, teknologia, tietoturva ja liiketoiminta. Ongelmat osoitetaan esittelemällä tulokset yrityksen työntekijöille tehdystä kyselystä, joka toteutettiin osana tätä diplomityötä. Ratkaisu näihin ongelmiin esitellään keskitetyn salasanojenhallintajärjestelmän muodossa. Järjestelmän eri ominaisuuksia arvioidaan ja kokeilu -tyyppinen toteutus rakennetaan osoittamaan tällaisen järjestelmän toiminnallisuus.

PREFACE

This Master's thesis has been written for Lappeenranta University of Technology between May 2004 and November 2004.

I would like to thank the supervisor of this thesis, Professor Jari Porras for giving me good instructions on making this thesis and being one of the best teachers I have had during my studies in Lappeenranta. I would also like to thank all company employees who helped me to write a better thesis by participating in the surveys and seminars that were a big part of my work. Especially I would like to thank my instructor Jari Ilmonen, examiner Jan-Erik Grön and all my colleagues in the user management project. Keep up the good work.

Finally, the biggest thanks go to my parents. You have both, in you own way, encouraged and supported me through all these years. I hope I have made your efforts worthwhile.

Mikko Ylén

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVATIONS

AD	Active Directory
AM	Access Management
API	Application Programming Interface
DB	Database
PBE	Password Based Encryption
SHA	Secure Hash Algorithm
EDI	Electronic Data Interchange
ERP	Enterprise Resource Planning
ESSO	Enterprise Single Sign-On
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
IAM	Identity and Access Management
IBM	International Business Machines
IM	Identity Management
IT	Information Technology
ITIM	IBM Tivoli Identity Manager
J2EE	Java 2 Enterprise Edition
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
MQ	Message Queuing
OS	Operating System
ROI	Return of Investments
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
SSO	Single Sign-On
UI	User Interface
WAS	WebSphere Application Server

1 Introduction

The overall security level of an enterprise is the sum of many security elements: Security policies, network security, system security, application security, employee awareness and so on. The fist line of defense in information security is always access control. We have to have restricted and controlled access to enterprise information resources so that only legit users are allowed to access and use those resources. Protecting enterprise application and data resources requires identifying and authenticating the users before they are allowed access. This is where passwords play a big part in today's enterprise security.

There are basically three different methods you can use to authenticate users to computer systems. These three methods are usually known as *something you know*, *something you have* and *something you are*. These roughly translate to passwords, access tokens and biometrics respectively (Anderson 2000, 36). Table 1 summarizes the characteristics of these authentication methods from an enterprise point of view.

Table 1: Comparison between authentication methods (M-Tech 2003, 5).

Characteristics	Passwords	Tokens	Biometrics
Reliable authentication	Good	Very good	Excellent
Client side hardware	No	Sometimes	Yes
Client side software	No	Sometimes	Yes
Deployment Cost / user	0	50€	100€
Legacy support	Yes	No	No

Although passwords have been marked as the worst security thread in the information security community (Anderson 2000, 36), Table 1 shows why passwords are still the most common way to authenticate users to computer systems. According to (Witty & Allan 2003, 1) password will be the major authentication method in enterprises for the next two to three years. Other authentication methods have high deployment costs because of the additional hardware and software requirements and most legacy application can't support other authentication methods besides passwords.

So passwords are still an important part of today's enterprise security arsenal, but they have proliferated so quickly that managing them has become a serious real-life problem. Employees are overwhelmed by the number of passwords they have to remember and the number of security policies they have to obey on a daily basis. This has led many organizations on the path of finding solutions for this surprisingly difficult problem. (Bohan 2002, 1)

The need for centralized password management in our case arose during a user management project which purpose was to centralize and automate the management of user access rights in almost all IT systems and services. Taking into account the heterogeneous nature of this company's global and local IT systems (see chapter 1.2) as well as the versatility of policies and processes used throughout the company, this proved to be a very difficult task.

One part of the user management project was to develop a password management system for employees through which they could change their passwords to multiple IT systems simultaneously. The plan was that when a new system was taken under the centralized user management system, it would also be included in the password management system. But as the user management project was progressing very slowly, it was noticed that the password management system did not provide any real value to employees because there was only a single password that could be changed using this system. So problems in the user management project were stalling the password management system development. At this point the project needed results and it was noticed that there is a great deal of problems employees are facing with passwords on a daily basis. It was decided that password management was to be separated totally from the user management project and developed independently. It was considered that the password management solution would probably provide relatively quick results and possibly a great value for employees. This thesis is a part of that project.

To understand the scope of this thesis, the concept of "password management" must be defined. When talking about password management, the emphasis is on the word

management. The focus is on the management of password from the administrative perspective. The actual authentication techniques and methods used when users actually use the passwords are not considered. The emphasis is on what happens behind the scenes, in the password files and storages and how these passwords are managed on enterprise level. Figure 1 tries to clarify the scope of this thesis. A fully featured identity management (IM) and access management (AM) solution can be divided into two parts; administration and real time enforcement. Password management only exists in the administrative side as seen in Figure 1.

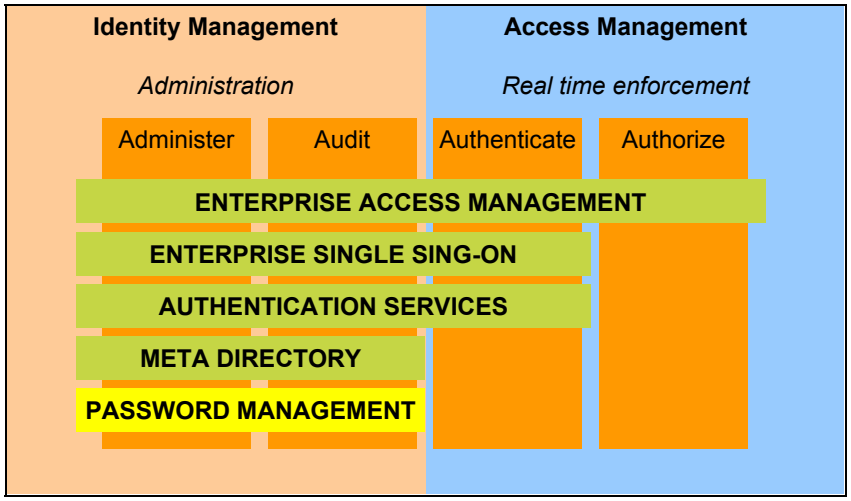

Figure 1: Aspects of identity and access management (Allan et al. 2003, 2).

This thesis has a couple of important goals. The first goal is to find out and verify the problems and risks that passwords cause on a large and global enterprise. The second one is to introduce and implement a solution for these problems in a form of a centralized password management system. A proof-of-concept type of implementation of a centralized password management system will also be made to demonstrate the features and usability of this concept in practice. As the outcome of this thesis the reader should have a clear view of password related problems and risks at large, global enterprises. The reader should also have a good understanding on how a centralized password management system can solve or reduce these problems.

1.1 Research methods

There are two main research methods used in this Master's thesis; Questionnaire to company personnel and literature research. Most of the theory in this thesis comes from literature research. Most of the references used in this thesis are gathered from the Internet. They include independent research material, articles and documentation made by password management system vendors. The information about the company in our case has been gathered from company's internal documentation and is not available in public.

The theory is challenged and confirmed by using the results from two internal surveys that were conducted as part of this master's thesis. The first survey was targeted to all company employees and contained questions about employees' password usage habits, problems with passwords and development suggestions. 850 employees participated in this survey (see Appendix 1). The other survey was targeted to Company's IT security personnel (see Appendix 2). It contained questions about security risks involved with passwords and password management as well as evaluation of different solutions from the security point of view. 32 security persons participated in this survey.

1.2 Research environment

This chapter gives a general overview of the company in question. It describes the overall nature of the company and its IT environment.

The company has production facilities in 16 countries and an extensive sales network comprising over 170 sales and distribution companies all over the world. Company's turnover in 2003 was close to 10 billion euros and the group employs approximately 35,000 people. 56% of employees work in Finland. (Internal 2004, 5-6).

Main targets of company's IT Services organization include development of new and existing global services and to deliver and support these services according to the business needs in co-operation with other IT and e-business functions and company's

contract vendors and hosting partners. Company IT offers about 40 global services that can be used company wide. These include e-mail, remote access, application integration, collaboration, security and other services. In addition different mills and business units have a vast amount of local systems. These include process automation and other production related systems. (Internal 2003, 4-41)

The company has over 400 sites connected to the company's internal network. Over 250 of these sites reside in Finland and over 150 reside outside of Finland. As a comparison, the number of sites outside Finland in 1998 was 30, so the growth has been quite rapid. The company has over 20 internet sites and 27 intranet sites and the interoperability between different sites and industries are being managed using multiple technologies, including EDI and MQ. There are 6 main IT infrastructure management centers that manage most of the 20 000 devices connected to the internal network. Of these devices about 1500 are servers and 15 000 are workstations. The total amount of traffic between these devices on a monthly basis is about 1.4 million business documents, 4 million internal e-mails and 0.5 million external e-mails. (Grön 2004a, 10-14)

1.3 Structure of the thesis

Chapter 2: Four views on password management contains the theory part for this thesis. It takes a look at passwords and password management from four different perspectives; human, technology, security and business. It will expose the problems and risks that passwords cause to large enterprises from these four perspectives and also explain the root causes for these problems. The problems are gathered from literature and are compared to the results of the survey conducted to all company employees as part of this thesis (User survey 2004). These four views form the basis for this thesis and they are used on the other chapters as well.

Chapter 3: Centralized password management provides an overview of centralized password management systems; the features they provide, what kind of architectural choices exist and what are the problems and risks that can be solved or reduced by using the features provided by a centralized password management system. These

features are evaluated from three different perspectives; human, technology and security.

Chapter 4: A Password management system contains the description of the practical part of this thesis. It explains the specifications of the company's password management system at a relatively high level. The requirements and architectural choices made while designing this system is described along with the technical environment and products used in the implementation. Analysis of this system is again conducted using the four different perspectives.

2 Four views on password management

Password related problems faced by large global enterprises were briefly discussed in chapter 1. This chapter digs deeper into these problems and find out whether these problems are real or just a marketing attempt from password management solution vendors to sell more of their products. This chapter takes a look at enterprise wide password management from four different perspectives; human, security, technology and business. The risks and problems caused by passwords are considered and also the real reasons behind these issues that actually cause these problems are investigated. By using this kind of "root-cause" approach it is possible to provide solutions that do not only treat the symptoms of password related problems but may also fix the real issues behind these problems.

All the chapters start by defining the general problems enterprises face with passwords. These problems are then confirmed or discarded based on the finding of (User survey 2004) and (Security survey 2004). The four views introduced in this chapter will form the basis for this thesis. These views will be used in the following chapters to evaluate centralized password management features and best practices. They are also used in the final analyze to describe the benefits an enterprise can achieve by implementing a centralized password management solution.

2.1 Human

The human factor is often described as the weakest part of a security system and users are often described as the weakest link in the security chain (Schneier 2004). Passwords are a good example of this, since almost all security risks related to passwords are caused by humans like discussed in chapter 2.3. While this is true, there are many sources saying that users are not the ones to blame about their bad security habits. The human-technology relationship is considered more closely in chapter 2.2, but for now the focus is on the human-password relationship. The problems faced by users are investigated and the problems they cause with their own behavior are discussed.

2.1.1 Password usage habits

There have been a few publications and surveys made about password usage habits in the last few years. All these studies claim that users use passwords poorly (M-Tech 2003) (Patrick 2002) (Protocom 2003a) (Rainbow 2003). The most common bad password usage habits are:

- Users write passwords down on a piece of paper
- Users use very simple passwords
- Users reuse passwords as often as possible
- Users share passwords with co-workers, friends etc.

In (User survey 2004) 850 company employees were asked about their password usage habits. Figure 2 show the results. Writing down passwords seems to be very common. Reading the employee comments in (User survey 2004) it was clear that writing down passwords in production factories is very common. Everybody does it, and they all have their passwords lined up on the side of the computer screens. This is quite concerning.

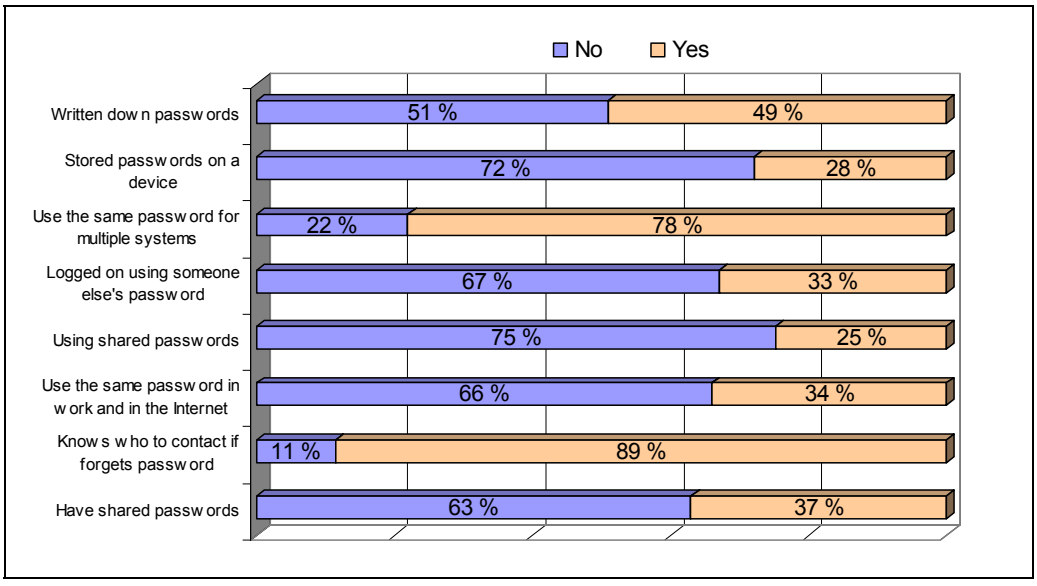

Figure 2: Password usage habits of the company's employees.

Looking at Figure 2 it can be noticed that 37% of company employees have shared their personal password with someone. Figure 3 shows with who the passwords have been shared with. Co-workers are the biggest group, and there is a good reason for this. Most of the employees participating in this survey are production level employees at company factories. They have a common habit of sharing their personal passwords with other shift workers or substitutes because it is much more convenient than going through the whole process of requesting access rights for the actual person accessing the system.

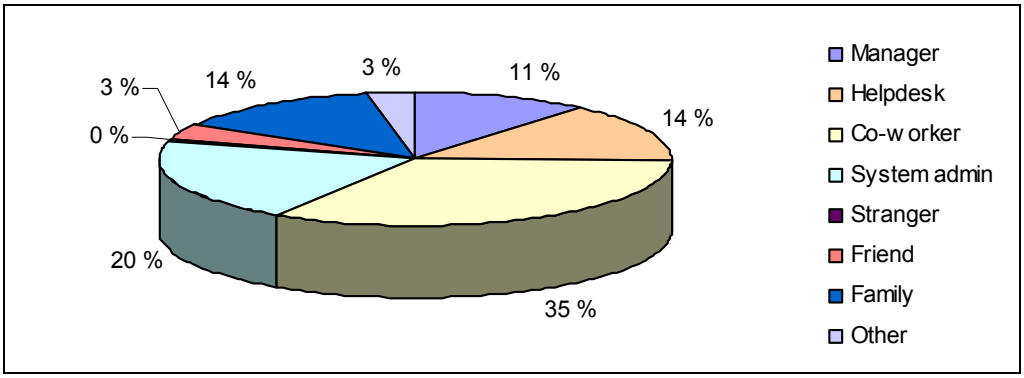

Figure 3: Employee password sharing habits.

Figure 4 shows a rather interesting and expected result. Most of the employees change their passwords only when they are instructed to do so by the system. Another observation is that the second largest group is "once per 3 months". This may come from the fact that company workstation password expiration time is 3 months and so some answers from that group can be moved in the "Whenever the system tells me to" group, making it even larger.

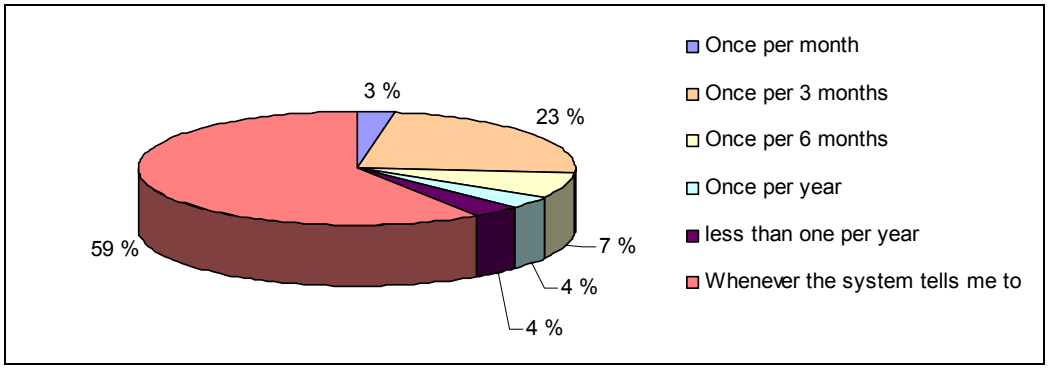

Figure 4: Company employees' password change frequency.

It does not establish a great feeling of security when going through those results. On average, over 30% of company employees neglect company's security policies in some way. This means that over 10 000 employees create security risks on password based systems company wide. That is, in nearly every system used in the company.

2.1.2 Password overload

The surveys made about the number of passwords employees must deal with (Protocom 2003a) (Rainbow 2003) suggest that in large enterprises employees have on average 5-6 passwords to remember and some employees have over 10 passwords they have to use more or less every day. This would imply that average employees have too much passwords to remember as part of their daily work. To confirm these figures with employees, they were asked how many passwords they have to use at work and on their free time.

Figure 5 shows the results from (User survey 2004). 77% of employees have 3 or more work related passwords and 40% have 7 or more work related passwords. Looking at the overall number of passwords employees have to remember, the figures go up to 93% and 69% respectively. On estimate, this means that most of the employees have to remember 6 or more passwords on a daily basis. According to (Protocom 2003a) most people have a hard time remembering 3 or more passwords. This would imply that remembering passwords would be a rather serious problem to employees.

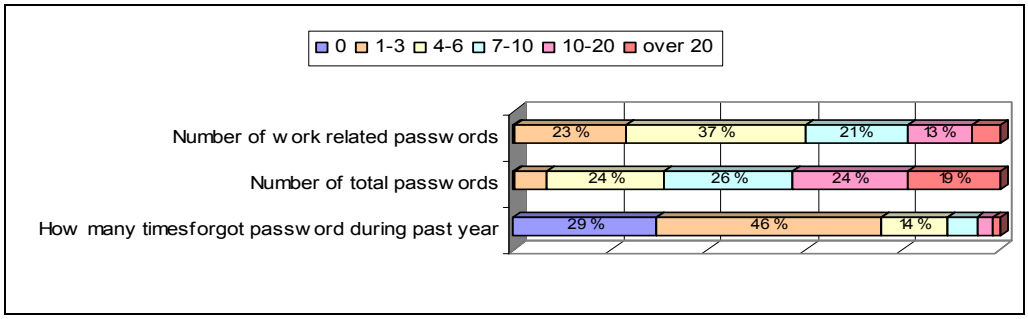

Figure 5: Number of passwords employees have to remember.

A lot of employees also forget their passwords. 71% of employees have forgotten their password more than once during last year. This is not surprising when looking at the number of passwords employees have.

2.1.3 Password related problems

Figure 6 shows the result of (User survey 2004) when the employees were asked to evaluate password related problems. At first glance it seems that most of the employees do not have problems with passwords. Surprisingly 54% don't have any problems to remember their passwords. Is this true, or are the employees just writing down passwords so that they don't have to remember them?

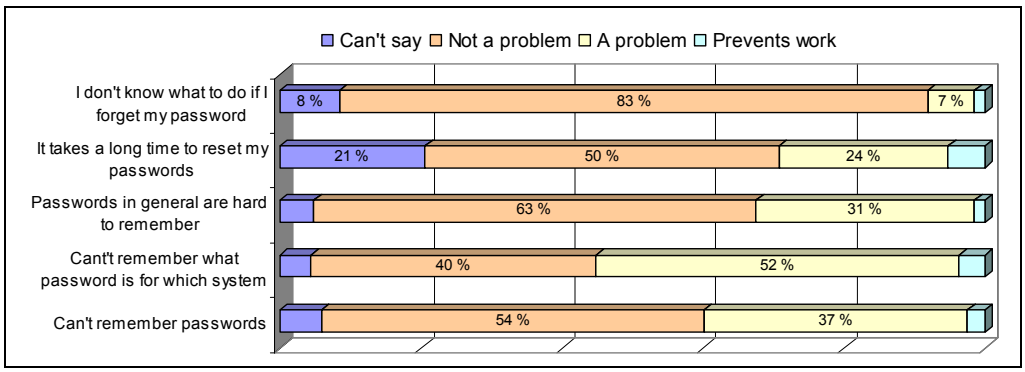

Figure 6: Password related problems.

The survey also showed that 49% of employees have written down their passwords. 52% have a hard time remembering which password was for which system.

Compared to the number of employees, this would mean that over 15000 employees have problems remembering which password is used in which system.

It is good to notice that most of the employees know what to do if they have forgotten their password; call helpdesk. The main problems introduces earlier are probably not so clearly displayed in these results, but the employee comments gathered in the survey clearly show that employees do have these problems and they cause loss of productivity and employee dissatisfaction. In chapters 2.1.4 and 2.1.5 below the two most important reasons causing these problems are introduced; human memory and social attitudes.

2.1.4 Human memory

Passwords are based on an oxymoron; passwords should be a long and random string that is easy to remember (Schneier 2004). Human memory was not designed to handle meaningless data like long and random passwords. This is why so many of the deficiencies of password authentication systems arise from the limitations of human memory (Yan et al. 2000, 3).

Some passwords are very easy to remember, like your daughters name or the name of your favorite football team. These kinds of passwords are also easy guess or break with *dictionary attacks*. On the other hand some passwords are very hard or impossible to guess and equally as difficult to break with technical means, but they are also very hard to remember. Considering a normal password rule that requires the system password to be at least 8 characters long and contain mixed lower and upper case letters, numbers and at least one special character. It is not easy to construct a meaningful, easy to remember password using the above rules. Security engineers are satisfied, because now employees can't use bad passwords anymore and the system is more secure, right?

Wrong. Employees will simply write the password down to a piece of paper and put it under their keyboard. The reason employees do this is because they would otherwise have to remember 5 or more passwords like the one described above, and

also remember the user ids that go together with these passwords and the system they are used in. Especially the systems that are accessed rarely cause problems because the password is easily forgotten if not used on a daily basis (User survey 2004).

To make things worse, security engineers increase the system security even more by forcing employees to change their passwords every 60 days, so that crackers have less time to crack passwords and compromised passwords are only valid for a short period of time. But this approach has the same effect. Now it's even harder for employees to memorize new passwords every 60 days. Even more, different systems have different password rules and password expiration times, so you have to change all your passwords at different times and they all must be very different. Also the effect of forcing the employee to change his password "now" usually makes the employee to choose a password very quickly and also forgets the new password as quickly (Patrick 2002, 2).

The above scenario pretty much describes the reasons to why employees write passwords down. There is no way employees can remember all of their passwords, especially when working with computers is not their primary job. IT personnel can somewhat manage the problem, because they are using the passwords all the time and are used to passwords. They may also be a little bit more security conscious and take the time to memorize their passwords. When employees have trouble remembering their passwords, they do one or more of the following things:

- Write down passwords
- Forget their passwords
- Use very simple passwords
- Don't change their password unless forced to
- Reuse old passwords as often as possible

In addition to having problems remembering passwords, employees also compromise security through their own behavior. This problem is discussed in the following chapter.

2.1.5 Social attitudes

Security is usually a secondary goal for employees that need to use computer systems as in addition or as part of their normal job routines. Normally employees see information security as an obstacle on the path of getting their job done (Schneier 2004). Even if this is an attitude issue, it is true that sometimes security is deployed in places where employees aren't use to have security and nowadays when almost everything is done with computers, security is everywhere. In the old days an employee would write down his weekly report on a piece of paper and hand it over to his boss. The identification and authentication was confirmed by the employee's signature and the fact that he was personally handing out the report for his boss. No user ids or passwords were required.

Today, when the same employee wants to write his weekly report he must first log on to his workstation using a user id and password. After that he must open up the reporting application and provide another user id and password. Now he can write the report and send it electronically to his boss. To read the report, the boss has to make the exact authentication steps. It can be questioned from the employee point of view which approach was more productive and user friendly, and also from the security point of view, which method had fewer security risks. But we life in a networked world and employees must cope with information security whether they like it or not; most of the time they don't (Schneier 2004).

Now that employees have to be security aware and obey all security policies the IT department throws at them, there exists a rebellion attitude against these policies. A normal attitude towards security policies is that the employee does not feel that information security is part of their job and so he doesn't have to obey the rules. Let the IT department handle the security (Weirich & Sasse 2001, 6). This attitude was also present in (User survey 2004). Some employees also think that they have nothing to hide so there is no personal risk for them if their password is compromised and even if someone is using their identities to do some damage on the corporate network. They think that they will not be punished because their boss trusts them (Weirich & Sasse 2001, 3-4). Security conscious employees may also perceived as

paranoid or not trusting their fellow co-workers. This puts some social pressure on the employees when it comes to sharing passwords, so it is better to give your password to someone even if you don't know him so well. But at least he will like me after this (Weirich & Sasse 2001, 5). This is one of the main human characteristics that crackers abuse with *social engineering* attacks.

Employees have a hard time coping with information security and there is research material about how employee attitudes towards passwords and information security in general affect the overall information security in an enterprise. Normal security policy violations are:

- Employees share passwords with their co-workers
- Employees use other people's user ids and password to access systems

But as said in many sources, employees are not the only ones to blame about these attitudes. There are technological barriers that employees have to face every day and most of the time these barriers are forced by increasing the technical security of computer systems. When system security is increased, usability suffers. This human-technology relationship is discussed in more detail in chapter 2.2.

2.2 Technology

Technology brings another set of problems for password management. Even in the modern world where computers are used everywhere; there are still a large number of people that see computers and information technology as an obstacle on their path of making their work done (Dourish et al. 2003, 2). Technical security is everywhere and employees have a hard time coping with it.

2.2.1 Technology overload

The number of diverse systems that global enterprises have to manage these days is huge. In the early days of corporate computing, there was only one computer to access so employees had to remember only a single user id and password, or they

didn't have to perform any authentication process because the computer was protected by a security guard who performed the identification and authentication of users. Over the years new kinds of computer systems were bought into organizations to solve specific business needs. Of course nobody considered how difficult the overall enterprise systems management would get or how this would affect employees who would have to access multiple systems always using a different user id and password. (Bohan 2002, 1)

Corporate mergers and acquisitions increased the number of systems one enterprise had to manage. It came clear at some point that in order to survive this jungle of computer systems enterprises would have to integrate these systems together and also provide help for employees so that they could navigate their way trough their own password mazes (Bohan 2002, 1). Although the above scenario is a generalization of systems management is large enterprises it reflects the situation the company in our case has nowadays. Looking at the numbers in Chapter 1.2, it is quite clear that this is exactly the case. The company has 40 global services that it offers enterprise wide and 22 mill sites that have their own local services and automation and production systems. Even if the actual number of different systems used is impossible to obtain, it is quite clear that the number is huge. The number of passwords employees have to use in their daily work was investigated in chapter 2.1.2. These numbers are too high and one big reason for that is that the company has too many different password based systems which all have their own authentication server and identity store.

2.2.2 Usability

Many organizations view technical solutions as the immediate answer to their information security problems. This attitude is fueled by system vendors who like to see their products sold. Technical solutions like firewalls, antivirus software and PKI systems are very valuable assets in the corporate security arsenal, but they do have drawbacks when the enterprise doesn't realize the role of those systems in the in the information security battlefield (Hinson 2003, 1). One of the most famous hackers, Kevin Mitnick, testified to US Senate that he had obtained more passwords by tricking people than by cracking systems (Poulsen 2000):

> *"The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and its money wasted, because none of these measures address the weakest link in the security chain."*

Until recently, research on password security has focused on designing technical mechanisms to protect passwords. Most of this kind of research has focused on the *crackability* of passwords, encryption, and use of one-way hash functions and protecting the password files on operation systems (see (Klein 1990) and (Morris & Thompson 1979)). The usability of password based mechanisms has rarely been investigated (Adams & Sasse 1999). For a few years now, crackers have paid more attention to the human link in the security chain, like using *social engineering* to obtain passwords rather than take the trouble trying to breach some system to steal password files (Sasse et al. 2001). Security engineers should also concentrate more on the human factors. Luckily the problem has been addressed already in several places (see (Conklin et al 2003), (Patrick 2002), (Holmström 1999) and (Brostoff & Sasse 2000)). The only problem is that this way of thinking should also be applied in practice.

If the technical security of a system is increased, for example the password length requirements is increased and people are forced to change their passwords more frequently, the technical security is truly increased, but overall the security of the system will suffer because employees will write their passwords down and sticks them on the side of their computer screen or under their keyboard. As said in chapter 2.1 employees will go to great lengths to get their job done. They will neglect security policies and try to go around technical security mechanisms just to get their jobs done without too much discomfort. Technical security is seen as an obstacle and is somewhere at the very bottom of employee's priority list.

2.2.3 Technology in the company

In (User survey 2004) any specific questions concerning system usability or number of different systems were not asked, but in the end of the survey there was an open question in which employees had the change to write down problems they have faced with passwords. There was couple of common comments that fall into this category. One was about the number of systems and how long it takes to change the passwords to all those systems. Some employees had a habit of changing all their passwords at once when a password in some system expired. This is a good practice, but it is very difficult to do in today's environment. There are a lot of systems to which the password must be changed and you must use a different password to some systems than others. This may sometimes cause the employee to immediately forget the password he had just changed or forget which passwords he had changed and which not.

A usual comment concerning system usability was that why some system needed a password at all. These included various production systems and employees didn't see the point of having a password on those systems, because they contained no sensitive data or functionality. Another comment on usability was that why there is so much security everywhere. A good comment was made by one employee:

> *"In the USA, we can access our bank, credit card and government information so much easier than we can access company stuff."*

Technical overload caused by huge amount of systems and technical security in large enterprises cause a lot of pain to employees. The bottom line is that until recently, the design of security systems has focused on the technical side of security. Security engineers have seen users as the weakest link in the security chain have tried to rule out that chain by increasing the technical security so much that it would negate all possible security threads that users produce. This obviously does not work in the real world.

Technically security issues can be solved with methods such as strong cryptography, digital signatures and secure communication protocol, but this is of no help if the user of the system fails to encrypt a confidential messages or switches to an insecure application because the security software is too confusing (Whitten & Tygar 1999). The same symptoms are shown with passwords; if users have too much trouble remembering their passwords, they will write the passwords down or choose easy to guess passwords.

2.3 Security

User identification and authentication is usually the first line of defense in information security. Using passwords is the most commonly used method for user authentication even tough it has been deemed by many security experts as one of the biggest security risks today (Anderson 2001, 36). In theory passwords would provide good security. They should be a long, random string only known by a single user. In practice passwords are a high security risk because they are not used as they are meant to be. In chapters 2.1 and 2.2 above, the problems that passwords cause in a large, global enterprise were discussed and some root causes for these problems from the human and technological point of view were also introduced. Now it is time to show what kind of security risks these password related problems cause.

2.3.1 Attacks on passwords

In this chapter, different types of attacks on passwords are described. To better understand the risks caused by passwords, it's good to know what kind of attacks one can expect.

Password file theft is probably the oldest form of password attacks. In this case it is assumed that the password file is not encrypted, so the attacker knows every password in the file. In modern operating systems and applications this is not a big problem since the password files or databases are always encrypted or hashed.

Dictionary attack is usually executed after an encrypted password file has been successfully stolen. Dictionary attack uses a large, exhaustive list of words against the password file. The attackers encrypt each trial value using the same algorithm as the system's login program and compare the encrypted value against the values in the password file. If a match is found, the password is also found. The list of password usually contains common words from dictionaries, hence the name dictionary attack. (Schneier 2004)

Log or dumb mining is a rather effective way of finding passwords. The attackers try find passwords written to log files or application memory dumps created when the application is crashed. Some applications use authentication logs to inform administrators about failed access attempts. Usually these logs contain the user id of the account that was accessed. Sometimes users mistakenly write their password on the user id field, causing the login to fail and the password is shown in the log file. (Allan & Witty 2003, 2) If an attacker spots a user id of the form "j3Ufk-df9" in the log file, he can be pretty sure it’s a password instead of a user id.

Network sniffing is one the most common ways to find out user ids and passwords. Attackers monitor the network traffic between clients and servers and can see, in clear text, all password transmitted between these end points. Of course this can be easily prevented by encrypting the traffic between the client and the server by using well known protocols such as Secure Sockets Layer (SSL).

Van Eck Phreaking (Emanations sniffing) is an interesting and probably the most unknown method of password attacks. Attackers eavesdrop on computer screens by tuning in to the radiation or "emanations" emitted by the video tube. This is similar to shoulder surfing, but the attacker can be on another room. (Schneier 2004)

Surreptitious password change means that an attacker is able to reset someone else's password without the actual user knowing about it. This can happen if a user leaves his workstation unattended and open or by calling the corporate helpdesk and pretending to be someone else. This is one reason why enterprises should consider

implementing a self-service password retrieval system, which could more securely, tough not perfectly, authenticate users in these cases.

Brute force password guessing is the simplest and probably the hardest way to get passwords. Attackers type in manually or use automated software to try different passwords directly on the application login process. This is similar to dictionary attack, but this time the attack is done online.

Duress means that attackers use threats or physical torture to force users to disclose their passwords. Although this may sound a bit far fetched, it is still a possibility. One way to prevent this kind of disclosure is to give users a *duress password* that they can give for the attackers. The use of this password would trigger alarms in the system they are used in. (BS 1995, 31)

Shoulder surfing is one way of getting passwords. The attacker just has to stand near a users when he logs on to an application and watch him type in the password. Normally the passwords are blinded on the computer screen, but attackers can see the length of the password and sometimes may be able to see on what the user is typing on the keyboard. (Anderson 2000, 45)

Social engineering is considered by many sources to be of the most effective way for malicious persons to get their hands on password files. Instead of going through the trouble of hacking into systems and stealing passwords, attackers simply ask people for their password (Anderson 2000, 37). Social engineering is about telling some plausible untruth and by appealing to normal human behavior as described in chapter 2.1.5. Considering the password sharing habits of users, they are likely to tell the password to the attacker.

2.3.2 Security risks

The password usage habits survey (User survey 2004) revealed several passwords related security risks. The following list summarizes these risks. The symptoms and effects these risks cause to information security are described.

Users write passwords down because they can't remember them otherwise. They write the password down on a piece of paper and stick on the side of their computer screen or store it under their keyboard. This totally eliminates the basic principle of passwords: it should be a secret known only by the user it is assigned to. Writing down passwords changes a password from *something you know* to *something you have* (Schneier 2004). From this point forward it should be treated as an access token, like a key or a smartcard. The only problem is that this token is very easy to copy just by reading the password. The piece of paper can also be stolen or lost, and when the password is written down, users usually don't remember the password without the piece of paper.

Writing down passwords is not necessarily a security risk if it is done properly. Many administrator and super user passwords are usually very long and random, so that they cannot be easily remembered or cracked using dictionary attacks. They are usually written down and stored in a company safe and taken out only when they are needed. This is good security, but normally when normal users write down passwords, they are not stored in a safe, they are wide open. To make the matter worse, there is no way an enterprise can enforce people not to write down passwords. You can train users and tell them not to write passwords down, but they will still do it, because that is the only way they can remember them. (Schneier 2004)

Users also share passwords with other each other and use those passwords to access systems. This also violates the basic assumption of password security, that the password must be secret. When users are willing to share their passwords, they are also a good target to social engineering introduced in chapter 2.3.1. If people would have the attitude of not giving up their passwords to anyone in any circumstances, this would not be a problem. But people do share passwords as shown in chapter 2.1.1, and by doing so cause a real security threat.

Another problem arises when people use these shared passwords to access systems. They use someone else's identity to access a system. At this point auditing is no

longer effective, and no one has any way of knowing who actually accessed the system and did the things that are listed in a log file or report. Malicious people can do whatever they want in systems and the real owner of the identity is the one who gets the blame.

Users choose passwords that are easy to guess and crack. This is another consequence of the fact that people can't remember good passwords. They usually choose a password that is related to their family, pets, cars, and hobbies. These kinds of passwords can be guessed easily by someone who knows the person or by someone who is able to collect information about that person. Even if users choose passwords that have a little variation like "p4ssw0rd", they are still easy to crack by using a good password cracker. This problem can be technically prevented by applying password rules to systems, but if they are too tight, users will write down their passwords.

Users use the same password at work and in the Internet. Users log on to Internet sites like chat rooms, internet e-mail and e-store using the same passwords (and even the same users ids) as they use at work. This is again common, because users don't want to remember so many passwords. The problem is, that Internet is no a controlled environment and therefore password may become easily compromised. There may be web sites that systematically collect user information and passwords. Again there is no way to force people from using the same passwords. It is a question of user training and user judgment.

All of the above are security risks that arise from the false usage of passwords. They do not in themselves breach system security but expose systems to many kinds of security threats like the ones presented in chapter 2.3.1. The real challenge to security engineers comes from evaluating these risks. What are the risks, what is the probability that this particular risk will come true and what are the effects if this risk comes true? These security risks are examined in the next chapter from the company point of view.

2.3.3 Security risk evaluation

In (Security survey 2004) 32 security persons were asked how they would evaluate the security risks of password related incidents. Figure 7 shows the results. The answers are pretty much what was expected, but one stands up from the figures: 72% of security persons think that it is a significant or intolerable security risk that users share their passwords with co-workers, but only 19% think it is a significant or intolerable risk that users tell their password to IT personnel. Apparently, the respondents didn't consider the possibility of social engineering attack at this point. They might have assumed that the user is talking face-to-face with the IT person and knows him personally, but in a large, global company this is rarely the case.

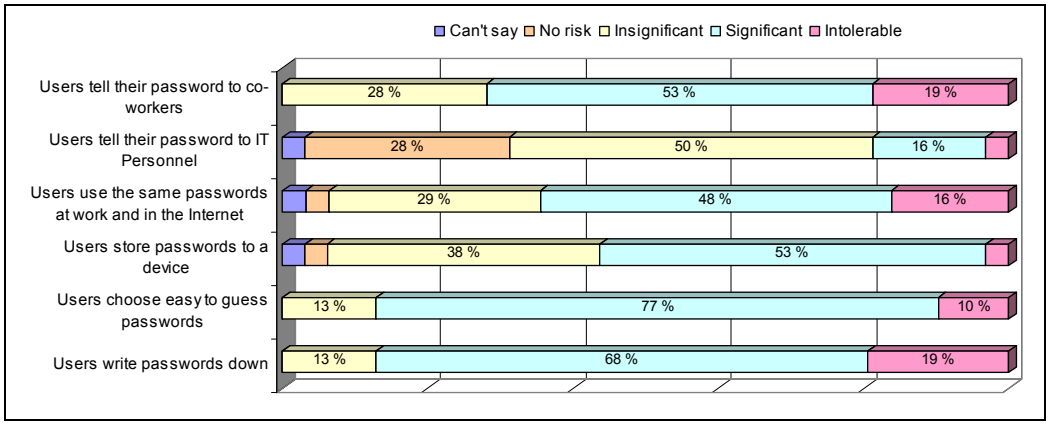

Figure 7: Company security personnel risk evaluation.

It would be nice to see the same percentage on both answers, because users should not share their passwords with anyone, not even IT or security personnel. There should be no reason for IT personnel to use user passwords, because they can do whatever they want in systems with administrative privileges. This is an important fact that should be emphasized in employee security training.

Password related security risks are real as shown by (User survey 2004) and all of those risks are considered to be significant or intolerable by over 60% of security persons. These are of course risk evaluations and the size of the risk depends on the

person's perspective, motivations and professional skills. Personally I would consider all of the above risks at least significant.

2.4 Business

When building IT solutions in a global enterprise, the need for a technical solution should arise from real business needs, not from some IT department's ad-hoc ideas. In other words we need to have a business case before we can even think about starting an IT project. Of course this is not always the case, but luckily when we talk about password management, we can build a business case by introducing the cost savings that can be accomplished by properly implementing a good password management solution.

2.4.1 Helpdesk overload

The main reason for password related problems for business comes from the helpdesk overload that password related problems cause. Employees forget their passwords and call helpdesk to get their passwords reset. Gartner research estimated in 2003 that 10% to 30% of helpdesk calls are password related (Allan & Witty 2003) and in 2004 the same estimation was from 15% to 35% (Witty et al. 2004). There are also talks about bigger numbers, like 66% (Reed 2004, 19). Each of these password related calls may consume 20-30 minutes of employee's time. In many organizations, users experience this problem 2-4 times annually (M-Tech 2004b).

In company with 35 000 employees the above figures would at minimum sum up to 70 000 password related calls to helpdesk per year. To count the actual costs for these contacts the cost of a single helpdesk call must be evaluated. According to (Allan et al. 2004) a typical helpdesk call costs 10€ - 30 €. Another estimation is about 51€ - 147€ per user per year (Brittain 2002, 4). This would be quite close to the first estimation, if every employee would call help-desk 5 times a year. If a rough estimate of 15 € per call is used, it will add up to 1 000000 € costs from password related helpdesk costs alone. This is surprisingly large sum, and it will be compared to the company estimates in the next chapter.

2.4.2 Company helpdesk

In this chapter, the costs that password related problems cause for the company are examined. From Figure 8 it can be seen that 53% of employees have contacted helpdesk more than once during the last year concerning password related problems. The company has 35000 employees worldwide. If the number of password related calls to helpdesk is counted based on these figures, the figures will be quite large.

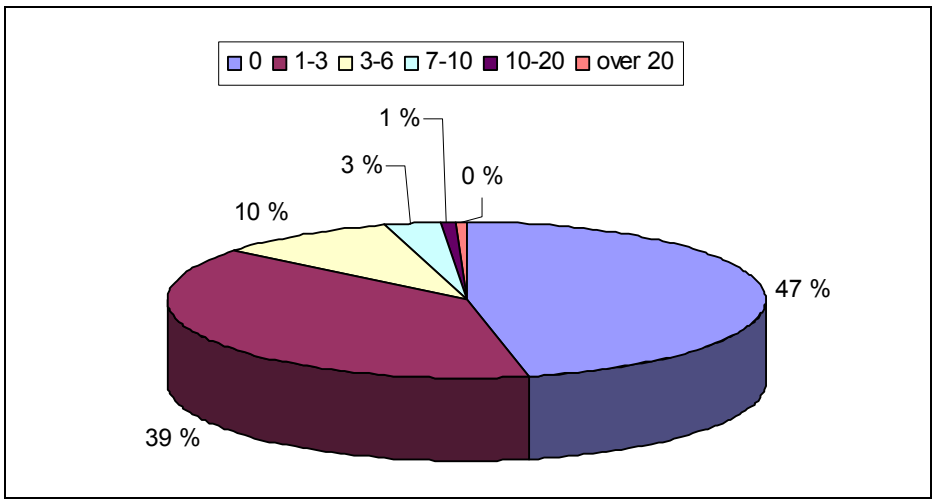

Figure 8: Number of password related helpdesk calls per employee in a year.

In the next calculations the figures from Figure 8 are used:

- 35000 employees
- 39% call helpdesk 1-3 times a year
- 10% call helpdesk 4-6 times a year
- 4% call helpdesk over 7-10 times a year

Minimum number of calls

$$(35000 \times 0.39 \times 1) + (35000 \times 0.10 \times 4) + (35000 \times 0.04 \times 7) = 37450 \quad (1)$$

Maximum number of calls

$$(35000 \times 0.39 \times 3) + (35000 \times 0.10 \times 6) + (35000 \times 0.04 \times 10) = 75950 \quad (2)$$

Average number of calls

(37450 + 75950) / 2= 56700 (3)

Formula (1) represents the minimum amount of helpdesk contacts per year and (2) represents the maximum amount of helpdesk calls per year. If these results are compared to the results in the previous chapter, it can be seen that the average helpdesk call rate is quite smaller than in the estimates. The total cost of these calls can be calculated by using the same cost per call as in the previous chapter.

Minimum cost:

37450 1/year x 15 € = 561750 €/year (4)

Maximum cost:

75950 1/year x 15 € = 1139250 €/year (5)

Average cost:

56700 1/year x 15 € = 850500 € / year (6)

Result of (6) should give us some kind of perspective on the costs that companies are experiencing. It is a bit smaller than in the estimation. If by using a password management solution these costs can be reduced, it would make a pretty good business case. Of course the purchase and deployment costs must be considered and the actual savings per year against the yearly maintenance costs must also be evaluated. These will be discussed in chapter 3.6.4. Luckily there are also other benefits for business besides costs savings. Employee satisfaction may increase because there are not so much passwords to hinder their work and information security is also increased. These are good goals to pursue and are worth the investments made. Table 2 is a summary of the password related problems introduced above and how they affect business.

Table 2: Summary of password related business problems (M-Tech 2004b, 2-4).

Problem	Symptom	Effect
Complexity	Users have too many password, too many systems to access and different kinds of password policies to remember	User dissatisfaction
User productivity	User who forget passwords waste time on: - Trying to log in - Calling the helpdesk - Waiting for a service - Proving their identity - Waiting for password reset	Each incident can consume about 20-30 minutes of working time. This generates a large volume of user problems and helpdesk calls.
Support cost	Users who forget passwords call the helpdesk to get their passwords reset.	Password related calls normally represent 20% to 30% of all helpdesk calls.
Security violations	In effort to remember large number of passwords, users violate security policies.	Security is compromised.

In Table 2, the complexity and security violations in the business problems are also included. After all, employee satisfaction and information security are important aspects of business as well.

2.5 Discussion

Passwords provide good security when they are used properly, but in reality there are a lot of security risks and problems related to passwords. Figure 9 tries to summarize these problems in a form of a problem tree. As it can be seen, the biggest "root causes" (blue boxes) are related to technological overload and to the human factor. There is also a proven deviation in the balance between security and usability of computer systems. These cause problems (white boxes) that are faced by employees in their daily work. On the end these problems cause harmful effects (red boxes) to users, business and security.

A solution in a form of a centralized password management system is introduced in chapter 3. The purpose of this solution is to get rid of or negate the problems caused by the "root causes" and by doing so diminish the harmful effects these problems cause. It must be emphasized that there are also other kinds of solutions for these

problems. These include things like employee training, which has a good purpose, but the real benefits received from it depend on the employees themselves. Even if you tell employees that it's a bad thing to share passwords or write them down, they will still do it because it is so much easier and does not intervene with their working routines. Evaluating the real security threats and finding the real balance between security and usability in systems would probably increase user satisfaction and they would be more willing to cope with security policies instead of trying to go around them.

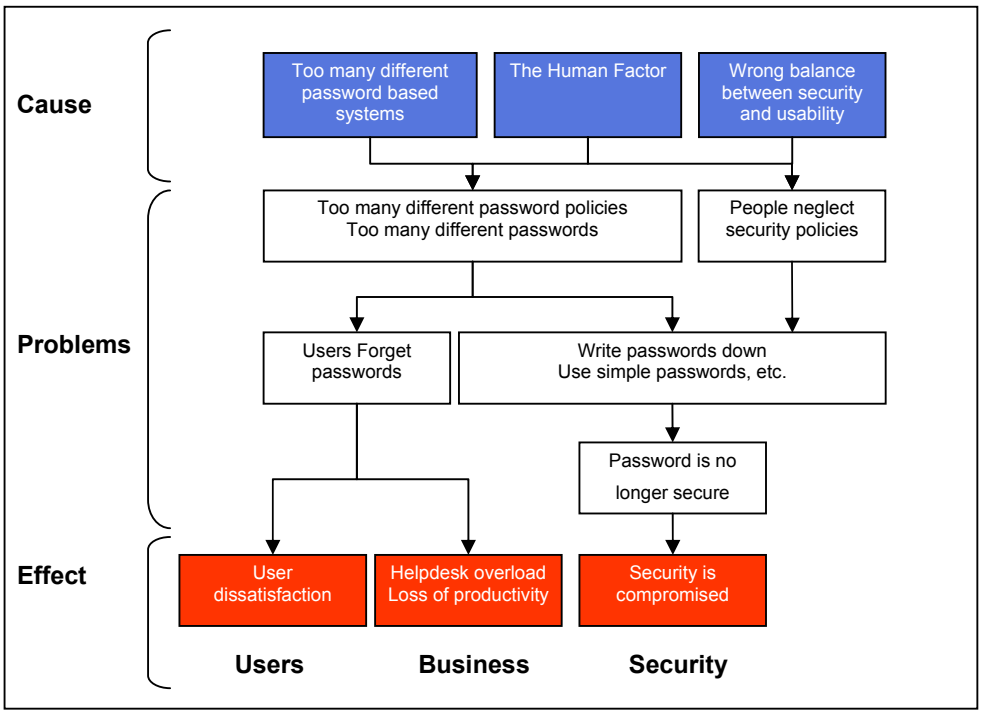

Figure 9: Password problem tree

To really get a rid of password related problems, enterprises should get rid of passwords all together and replace them with access tokens or biometric authentication methods. This is not a practical solution since it takes a lot of time and money to do so and other authentication methods also have their drawbacks. The bottom line is that companies are stuck with passwords and building a centralized password management system provides a solution to many of the password related problems in a large, global enterprise.

3 Centralized password management

This chapter focuses around the concept of centralized password management. The possible features provided by these kinds of systems are introduced. The ups and downs of these features are also investigated and how they can solve or reduce the problems and risks introduced in chapter 2. At the end of this chapter the reader should have a clear picture what centralized password management means, what features it offers and how it can improve security and user satisfaction in a global enterprise.

3.1 Reducing the amount of passwords

When it comes to reducing the number of passwords users have to remember, there are two rather similar solutions available for the enterprise to choose from; Password synchronization and Single sign-on (SSO). There is a clear separation between those vendors and experts that support SSO and those that support password synchronization. In this chapter both of these solutions are described and evaluated.

A common question is why do we need password synchronization in the first place? Why can't all systems use a single data store for user authentication? These are good questions. In the best case password synchronization is not needed. All user authentication data would be in a single, secure and robust data store which all applications use to authenticate users. Moreover, a single sign-on solution (SSO) could be used that would allow users to authenticate themselves only once during their working session and they would be automatically authenticated to all systems they are allowed to. The single authentication server approach is quite good and should be the first choice when considering decreasing the number of passwords users need to remember. Normally, the diversity of systems prevents us from completely integrating all applications to use a single authentication server. SSO on the other hand is a very good idea and would provide a great value for the users (only one password to remember and you would only have to type it in once), but it has some major drawbacks when looking at the deployment and maintenance of an SSO

solution. Password synchronization falls between these two approaches in usability, complexity and costs.

3.1.1 Password synchronization

The purpose of password synchronization is to allow users to change their password to multiple systems simultaneously through a single user interface. This means that a user has only one password to access all of the systems that are included in the password synchronization process. Usually the synchronization process is started through a web browser interface in which a user writes his old password and his new password and submits the request. The password management system propagates the new password to all target systems assigned for the user. The actual technologies and methods used to synchronize passwords vary, but in the end, the result is always the same. (Reed 2004, 18)

Another alternative is to use so called *native password change* procedure to synchronize passwords. In this case a software component grabs the password when it is changed in an application and sends it to the password management system which in turn propagates the password to all systems assigned to that user. Figure 10 shows a common native password change when a user changes his operating system (OS) password. The password is send to the central identity repository, but is caught before it reaches its destination and is propagated to both the synchronization engine and to the identity repository.

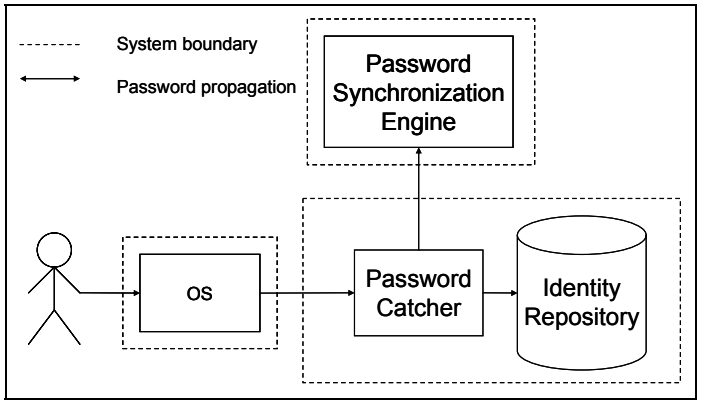

Figure 10: Native password change in an operating system.

Using both of the above synchronization methods together is called *bi-directional synchronization*. Bidirectional synchronization requires the synchronization application to support some form of password change notifications and for the password management system to be able to receive these notifications. (Reed 2004, 18-19)

Using password synchronization brings up a hot topic concerning single password policy where users have only one password to access (almost) all systems they are using. Some see this as a security risk (Protocom 2003b) and some claim that it increases password security (M-Tech 2003). The security risk perspective comes from the fact that if a user has only one password to access all systems, then compromising that password gives an intruder the access for every other system in the network. On the other hand password synchronization can increase password security by allowing the user to use a single password to access multiple systems. This eases the memory load for users with multiple passwords and they are less likely to write their passwords down (Allan et al. 2003, 3).

Password synchronization does have its limitations. If a password is synchronized between multiple systems, the password is as secure as the weakest system on the network. If the password is compromised in one system, it can be used to access all other systems as well. Also, stronger password rules can not be enforced than the weakest rules supported by some system (Reed 2004, 63). This means, that if some system only allows passwords to be 6 characters long and contain only lower case letters, a stronger rule cannot be enforced on any of the synchronized systems. Of course these kinds of systems should not be included in the synchronization process.

As said in chapter 2.3.2 it is impossible to prevent users from writing passwords down. When using multiple, unsynchronized passwords, the security of passwords is reduced to a level provided by a piece of paper. On the other hand, if password synchronization is used, the password security will not be dependent on the users but will be as secure as the weakest system in the network (M-Tech 2003, 11). This

means that users are no longer impose a security risk and technological means like encryption can be applied to improve the security of the weakest systems.

If password synchronization is taken into use, there are few guidelines that should be followed. First, very insecure systems should not be included in the password synchronization process. All systems should go through a security audit to determine the security of passwords on that system before they are allowed to be synchronized. Secondly strong password rules should be enforced on the synchronized password. Normally this is a problem with multiple passwords in different systems, but with only one synchronized password, users should be able to cope with it. Thirdly, password change should be enforced on a regular basis. These same kind of requirements for passwords were marked as a problem in chapter 2.1. The difference is that now users only have one strong password to remember, one type of password rules to obey and the passwords to multiple systems are always changed at the same time through a single user interface. This should bring a great value for the users and help them on their password related problems.

3.1.2 Single sign-on

Single sign-on (SSO) is said to be the holy grail of password management (Schneier 2004) and is also appraised by system vendors providing SSO solutions (Protocom 2003b). The idea behind SSO is that users only have one password that they use (like with password synchronization) but they only need to use this password once during their working session. That is, when they log on to their workstation. After the initial log on, the SSO solution will automatically authenticate the user to all systems he has to access. No more user ids and passwords. (Reed 2004, 18)

There are many types of SSO solutions. Type of SSO discussed here is called *enterprise single sign-on* (ESSO) or *universal single sign-on*. Other types of SSO solutions include web SSO, which is based on cookies and is pretty straightforward to implement. If you have ever logged on to a web site and told the web page to "remember my password", you are using web SSO. But web SSO can only be used in web environments like the internet or corporate intranets. There are also a number of

vendor specific SSO solutions that work only with a limited set of applications. ESSO has the ability to offer single sign-on functionality with any given software in the enterprise arsenal. Until recently, fully functional, true ESSO has been more myth than reality (Bohan 2001, 2).

A typical ESSO implementation uses a password replay mechanism. This requires all applications to be SSO enabled, so that the SSO engine can automatically notice when user tries to log in to the application and can then automatically handle the authentication process. User credentials (normally user id and password) are stored on a centralized server. SSO requires a user to authenticate themselves only once to a trusted system per session. Normally this occurs when the users logs on to his workstation.

The first time a user runs an application that is SSO enabled, they a prompted to enter their user id and password. These credentials are then encrypted and stored to a central password repository so that the SSO system can remember them. The initial authentication can be anything from biometrics to access tokens, but the point is that the authentication information is stored on a central server. The next time the user runs the same application, an SSO agent installed on the user's workstation notices this and automatically retrieves the stored credentials from the central server, provides the information to the application and the user is authenticated without any user intervention.

When a password would expire on some system, the SSO agent should notice this and automatically generate a new random password and store it to both the system and to the central password repository. This is seamless to the user and from the systems point of view it seems like the user is regularly changing his password. There a couple of nice benefits achieved with this feature. First, the user does only have to change his workstation password at regular basis; he doesn't have to worry about changing his passwords to other systems as well. Secondly, the random passwords generated by the SSO agent are very secure and are different on every

system. This eliminates the problem that one weak system could compromise the security of all other systems.

The idea behind ESSO is great, but the reality is quite different. For the end users SSO is a great solution, but from the system development point of view and maintenance point of view SSO has many drawbacks; ESSO is very expensive to deploy, it may cost ten times compared to a password synchronization solution. The maintenance costs are also high due to client side software components and complex technology. (M-Tech 2004a) The biggest problem facing ESSO is the fact that it is a real time authentication system. This means that all application authentications rely on the SSO system and if that system is down, no one can access any of the systems, because the SSO is the only system that knows the real passwords for these systems. An ESSO solution requires very high availability which in turn will increase the deployment and maintenance costs of the system.

3.1.3 A centralized password repository

The least appraised method of reducing the number of passwords is using a centralized password repository that many applications can use in authentication. This method is simple, but in many cases can be impossible to implement because of technical limitations. If an application doesn't support LDAP (Lightweight Directory Access Protocol) for authentication, then there is no way to integrate this application to a directory. It is surprising why everybody talks about SSO and password synchronization, but only one of the references used in this thesis mentioned this simple solution (Reed 2004, 19). The only explanation to this is that this solution does not bring any profit to password management solution vendors.

So to reduce the number of passwords, many systems are configured to use the same authentication server. As said in chapter 2.2.1 companies have multiple user repositories. Almost every application has its own user storage where user information and passwords are stored. This generates problems on many areas ranging from user management to systems management and password management. Because of the number of different user repositories, users tend to have multiple

different passwords. In order to reduce the number of passwords, common user storage should exist, which contains all user information and is accessible by multiple applications. Figure 11 shows the principle of the concept.

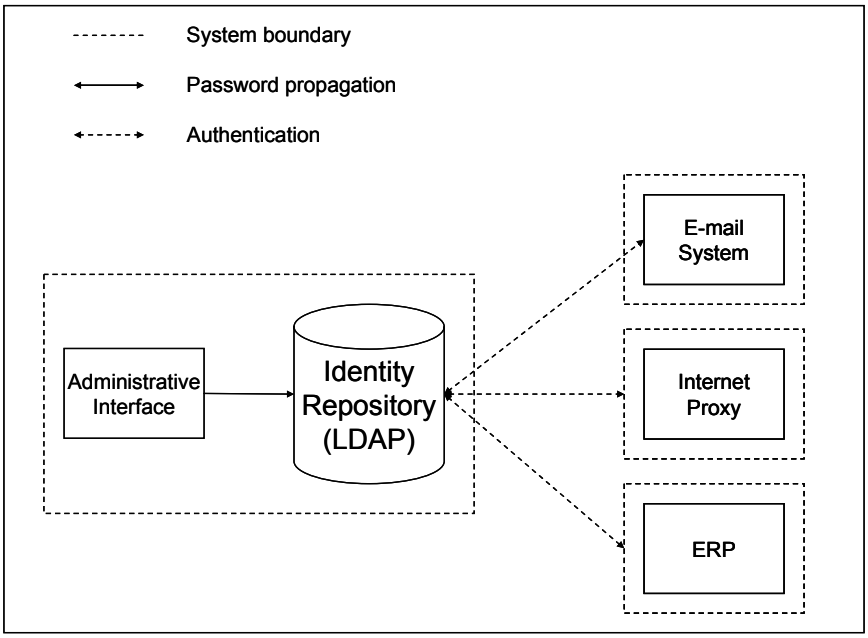

Figure 11: A centralized password repository.

This kind of approach would allow us to concentrate our technical security measures to single point instead of having to manage the security in many places and also only one password could be used to access multiple systems. Combining this type of solution with password synchronization would help to reduce the number of passwords dramatically. (Reed 2004, 19)

3.1.4 Comparison

Table 3 summarizes the differences between password synchronization and ESSO solutions. It clearly shows why ESSO solutions are not very practical to implement in a large enterprise even though it would offer the end users great usability. When it works, that is. Password synchronization is quite easy and cost effective to implement and deploy. It does not cause major problems for users if the system is offline and it allows users to use only one password to access all systems, even tough

they have to type in that password multiple times when accessing multiple systems. Password synchronization is clearly a better choice for large enterprises than SSO.

Table 3: Comparison of SSO and password synchronization (M-Tech 2004a, 2)

Topic	SSO	Password synchronization
Maturity	No existing implementation in a heterogeneous environment.	Has been deployed to large user communities in heterogeneous environments.
Cost	Expensive to deploy. Will cause expenses because of lost productivity.	1/10 of SSO deployment cost Will give ROI on lost productivity.
Maintenance	Expensive to maintain.	1/10 of SSO maintenance costs.
Reliability	SSO technology failure can shut all users out of the network.	Password sync failure will have only a small impact on users.
Intrusive technology	Software needs to be installed on every workstation.	Software needs to be installed on servers.
Usability	High usability if required software is installed on the used workstation.	Medium usability in all situations.

The third choice, centralized password repository, not showing in the table, can be taken into use without affecting the above solutions. In fact, centralizing user authentication to single or just few places should be the first target of an enterprise. If all systems cannot be attached to these central systems, then enterprises should think about password synchronization or even SSO when the technology is mature enough.

3.2 Recovering forgotten passwords

When a user forgets his password, the password must be reset by administrators or helpdesk personnel. This usually involves doing the password resets in multiple systems which may take a considerable amount of time. As seen in chapter 2.4, password related helpdesk calls create high costs and high load for helpdesks. There are two solutions that password management systems can offer to solve this problem; password helpdesk reset and password self-service.

With password helpdesk reset, helpdesk personnel or administrator can use the password management system's user interface to reset the user's password by only writing the new password once, and the system automatically changes the new

password to all the systems included in the password synchronization process. So there is no point of implementing password reset without password synchronization.

Using the password self-service feature, users can reset passwords themselves. This includes a web user interface in which the user is asked a number of questions to which the user, and only the user, should know answers to. If the user answers correctly to all questions he is allowed to reset his password. Again the password is automatically synchronized to all systems. Other authentication methods have been also studied, but there are little implementations of these methods (Brostoff & Sasse 2000).

There are still problems with self-service password reset. Biggest problem is to train users to use it properly. Before users can actually use the self-service functionality, they have to login to the password management system and select or type in their questions and answers. This can be too hard for computer illiterate employees. There is also security issues involved. If users are allowed to select their own questions or even allowed to type in their own questions they would probably use simple questions with simple answers (M-Tech 2003, 13). This would again make it easier for malicious persons to reset user's password and use it to access systems. These security risks can be minimized by using a group of pre-defined questions from which users should select at least three questions they need to provide answers for. These questions should be very personal and answers to those questions should not be found from any written records (like driver's licenses and birth certificates). (Just 2003, 4)

The answers that users provide should also be validated. Answers to all questions should be different and should be at least 3 or more characters long. But when these restrictions are designed for the questions and answers, it must be kept in mind that if when trying to increase the system security too much, usability suffers and users will probably not use this system anymore. (M-Tech 2003, 13)

While there exists a security risk involved in asking the users a group of questions to authenticate them it is worth noting that the manual processes used for password reset at many organizations are often completely insecure and subject to social engineering attacks. Normally the user authentication at helpdesks is done by calling back to the user on the phone number found in the corporate address book. If the same person answers, he is considered to be authenticated. (Witty & Brittain 2002) The above procedure is also used in our company.

3.3 Enforcing common password policies

One problem with large heterogeneous environments is the diversity of password handling in different systems. Especially older legacy system may have some restrictions on passwords, like not accepting some characters in passwords, limit password length and so on. Because of these limitations, the centralized password policy needs to be set to the lowest common denominator. For example, if a system that is part of the synchronization process can only handle at most six characters and can only handle alpha-numeric characters, this system sets the upper boundaries for password length and characters. In this case, strong password policies with at least 8 characters and mixed lower and upper case letters and special characters cannot be used. (Reed 2004, p. 63)

Users must be required to choose their passwords from the widest possible set of characters, subject to the constraints of the systems where those passwords reside. For example, most mainframes do not distinguish between uppercase and lowercase, and only allow three punctuation marks. This must be taken in to consideration when planning password policies, like shown in Table 4.

To set a password policy based on the smallest permissible set of legal password values – for example: 10 billion. To draw from Table 4, mainframe compatible passwords must be at least seven characters long to meet the requirement of at least 10 billion possible passwords. There are many different interpretations on what is the line between a strong password and a weak password. Like said many times before, it is impossible to make a password policy that would force the users to use strong

passwords but at the same time allow them to use memorable passwords. The following list adapted from (BS 1995, 26-27) contains the best practices for password policies that try to keep the passwords somewhere in the middle of secure and memory limits.

Table 4: Password character space (M-Tech 2003, 5).

Characters	5	6	7	8	9	10
0-9	1.00e05	1.00e06	1.00e07	1.00e08	1.00e09	1.00e10
a-z	1.19e07	3.09e08	8.03e09	2.09e11	5.43e12	1.41e14
a-z, 0-9	6.05e07	2.18e09	7.84e10	2.82e12	1.02e14	3.66e15
a-z, 0-9, 3 punct	9.02e07	3.52e09	1.37e11	5.35e12	2.09e14	8.14e15
a-z, A-Z	3.80e08	1.98e10	1.03e12	5.35e13	2.78e15	1.45e17
a-z, A-Z, 0-9	9.16e08	5.68e10	3.52e12	2.18e14	1.35e16	8.39e17
a-z, A-Z. 0-9, 32 punct	7.34e09	6.90e11	6.48e13	6.10e15	5.73e17	5.39e19

To ensure that the search space is sufficiently large:

- Passwords must be at least seven characters long.
- Passwords must contain at least one letter, and at least one digit.
- Passwords should contain at least one lower case letter and one upper case letter.

To eliminate easily guessed passwords:

- Passwords must not contain user's name or login ID.
- Passwords must not be based on a dictionary word, in any language.
- Password should not contain repeated patterns more than 2 characters long

These guidelines should be used for every system in the enterprise. Even if those systems should not be a part of the password synchronization process. It helps to keep the passwords in every system secure, and helps the users, since they only have to obey one password policy instead of many. If password synchronization is used, these rules are enforced at some central place, usually in an authentication directory or in the password management system itself.

3.4 Changing passwords

Changing passwords to multiple systems is time consuming and causes many problems to users as explained in chapter 2.1.4. One benefit of centralized password management system is that users have one place to change their passwords. Even if password synchronization is not in use, there exists only one place to change all your passwords. This is normally done through a web user interface offered by the password management system. If the passwords are synchronized, user only needs to write down his new password once, and the same password is changed to multiple accounts. Another method of changing your password when using password synchronization is to use some application's or operating system's native password change process, and the password management system will take care of the synchronization.

Normally users don't like to change their passwords because of the huge effort they have to put into the whole process of changing and memorizing new passwords. But from the security point of view this is something that cannot be taken away totally just to please the users. Users would, however, have a central place where they could change their passwords to multiple systems at once. To limit the usefulness of passwords that have been compromised, it is a good practice to change them regularly. Common practice on many systems is to force users to change their passwords when they login, if the password has not been changed for some period of time. In general, users should be required to change their passwords regularly, at most every 90 days. (M-Tech 2003, 7) For the same reasons, users should not reuse old passwords, as they may already have been compromised by an intruder. Many systems support this by using a password history to record some representation of old passwords and ensuring that users cannot change their password back to a previously used value. When password history is enforced, "smart" users may figure out the number of passwords in their history file. As this number is normally 10 or fewer, a user who does not really wish to change his password when prompted to do so may make several consecutive password changes, and finally return his password to its old value. (BS 1995, 30)

To defeat such "smart" users, some systems also enforce a password rule that limits the number of password changes that a user may make at any given period of time. By forcing users to spend several days, users are less inclined to defeat the password history mechanism. A better approach, though not yet available on many systems, is to simply maintain an unlimited number of entries in each user's password history. Since disk storage has become very cheap, this approach is now feasible. (BS 1995, 30)

3.5 Integration to target systems

For a centralized password management solution to work within the whole enterprise IT infrastructure, it must be able to integrate with a wide variety of heterogeneous systems. Password synchronization and password reset functionality require for the solution to be able to change user password to any given system. This sets a number of challenges for password management systems. There exist two types of approaches for integration; agents and connectors.

There are two main types of target system integration techniques. Some password synchronization solutions use connectors that connect directly to target system and uses application specific procedures and protocols to change the application password. Other solutions use agents at the target system end to enforce the password change. Both of these solutions have benefits and drawbacks and evaluation is required to decide the best solution to the given environment. As always, the best results would be achieved by using both technologies at the same time and choosing an agent or connector based integration depending on the target system being integrated. This of course requires the synchronization engine to support both mechanisms. (Reed 2004, 67-68)

3.5.1 Agent based solution

Agents are small software components that are installed on a remote system (from the password synchronization engine perspective) and they interact directly with the target system. There exists a common protocol between the synchronization engine

and all the agents in the environment through which all password change notifications are send from the synchronization engine to the agents or from the agent to the password synchronization engine if bidirectional synchronization is used. Figure 12 shows the common architecture for agent based integration.

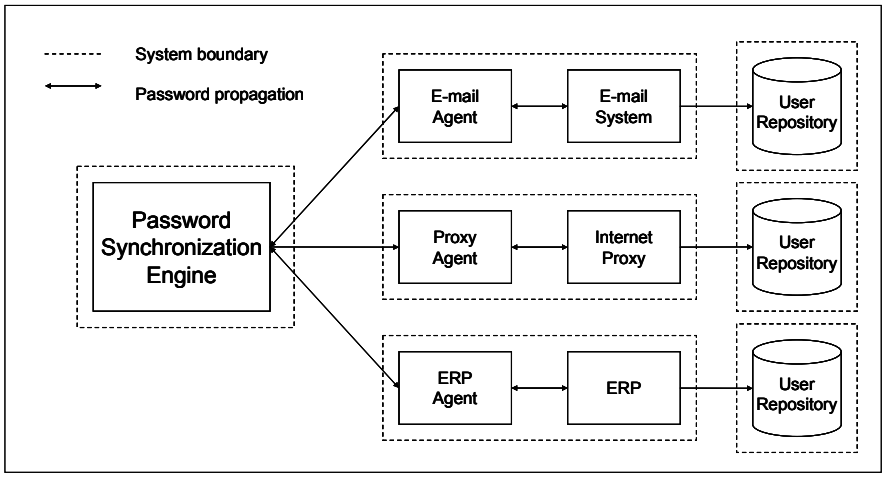

Figure 12: Agent based password synchronization

Agents have a common interface to the synchronization engine and usually use an application specific interface to interact with the target application. The application specific interface can be an Application Programming Interface (API), command line tool, direct database connection or any other kind of administration mechanism offered by the target system.

The biggest drawback of agent based solution is the deployment and management of the agents. If an enterprise has hundreds of applications or system to which the password synchronization solution must connect to, one agent must be installed and configured per target system. This usually requires lengthy change control processes and requires a lot of work and maintenance (M-Tech 2002, 8). Unless the synchronization engine does not take into account the possibility that an agent is broken, the agent can introduce a single point of failure in the password synchronization process, which may lead to unsynchronized passwords. (Reed 2004, 67-68)

The benefit of agent based solution is that it is always possible to secure the communications between the synchronization engine and the agent. After the password change notification has been securely send over the network the agent uses application native interfaces to force the change. This last interaction between the agent and application does not have to be secured, since there is no longer any network traffic between the two. When using connectors, the connector implementation or the target system may not support encrypted communications between remote systems. (Reed 2004, 67-68)

3.5.2 Connector based solution

Connectors are local software components from the synchronization engine point of view that communicate with the target system over a network using application specific procedures and protocols. Figure 13 shows the common architecture for connector based integration.

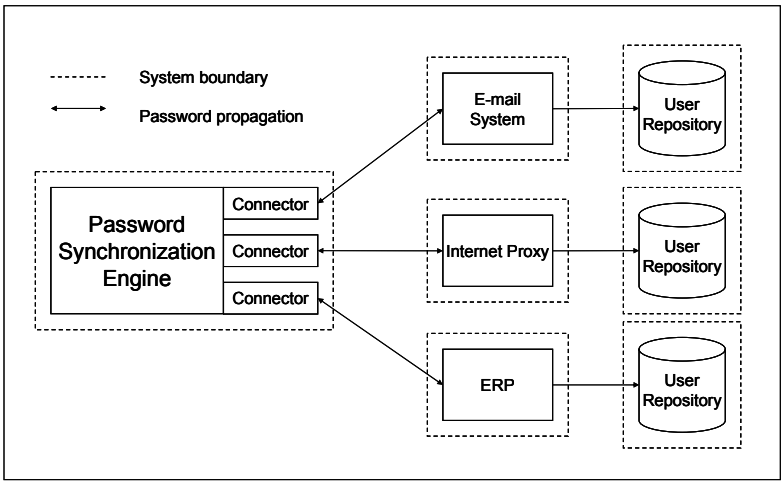

Figure 13: Connector based password synchronization.

Connectors are easily configurable and maintainable, because you don't have to install software components to remote systems. Another advantage of connectors is that the connections to the systems are manageable by the password management solution administrators. If a connection problem exists it can be handled by the password management system admin. If we are using remote agents, the problem

solving usually requires contacting the administrator of the target system. (Reed 2004, 67-68)

One drawback for connector based solutions is that some connectors may not support secure communications between the synchronization engine and the target system, or that the target system does not even offer the possibility to use secure communication protocols. In case of password synchronization, the passwords usually have to be transmitted as plain text over the network. Of course the encryption of the password can be handled by the connector, if it is possible and the target system knows how to handle passwords that are encrypted before they are changed. (Reed 2004, 67-68)

3.5.3 Combining different solutions

In order to support more target systems, a good synchronization solution should support all of the above methods. Figure 14 shows such a system.

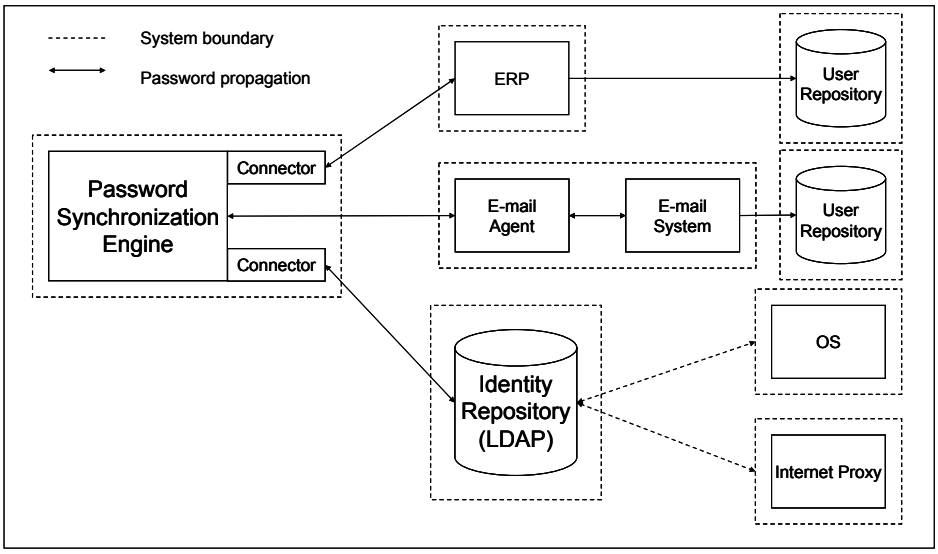

Figure 14: Combining synchronization mechanisms.

Centralized password repository introduced in chapter 3.1.3 is also included. If this kind of connectivity would be offered by a password synchronization solution, it

should allow the enterprise to synchronize passwords from many different systems quite easily.

3.6 Benefits

In this chapter the benefits achieved by implementing the password management features are introduced. Again, the same four perspectives are used to clarify the benefits gained by each stakeholder.

3.6.1 Human

The benefits received by users should be quite extensive. If implemented correctly, the centralized password management system reduces the number of passwords users need to remember by synchronizing the passwords between multiple systems. Not all systems can be included to the synchronization process because of technical difficulties explained above or because the system is considered to be too business critical to be using the same password as other systems. It must be noted that the target is not to have only one password to access all systems, but to reduce the number of passwords that users need to remember.

Another way to reduce the number of password is to change the way systems authenticate users by forcing them to use a single authentication server. By using a combination of these methods, the number of passwords can be reduced even further. Even if a system can't be included in to the synchronization process because of technical barriers, there may be a change to change the system's authentication process to authenticate users to a centralized authentication server.

Another important problem that users faced was the diversity of password policies between systems. If the number of passwords that users need to remember is reduced, the number of password policies is also reduced. By using password synchronization and the single authentication server approach, a single password policy can be created and enforced on all systems included in the synchronization process. It is clear that the number of password policies can't be greater than the

number of different passwords. Thus the number of password policies is also reduced.

The problem concerning different password expiration times was also a big issue for the users. When a centralized way of managing passwords is used, the password expiration times between the systems can also be harmonized. Now people will get an e-mail message or a pop-up message on their workstation screen that informs them of an expiring password. Users don't like to change their passwords on regular basis, so this may not please some users. But even if the need for users to change their passwords at regular basis is not totally eliminated, the number of password changes can be reduced and users don't have to change the passwords at different times. Moreover the users now have a single place and user interface that they can use to change their passwords.

Finally, users are less likely to forget their passwords. Now they have only few passwords to remember and they are using the same password to access also those systems that they are using rarely (e.g. once a month). This saves working hours and helps the users to remember the passwords. If for some reason, users do forget their password, they have two options to reset their password; they can do it themselves by using a web based user interface or call helpdesk that will reset the password for them.

In (User survey 2004) the employees were asked to evaluate the different features of a centralized password management and how they would think that these features would affect their password related problems. Figure 15 shows the results. 73% of users think that by reducing the number of passwords and allowing them to reset their own password through a web based user interface would help to solve problems. 78% would like the idea that they could change their password from their workstation using the native workstation password change mechanism and the password would also be changed to all other systems as well.

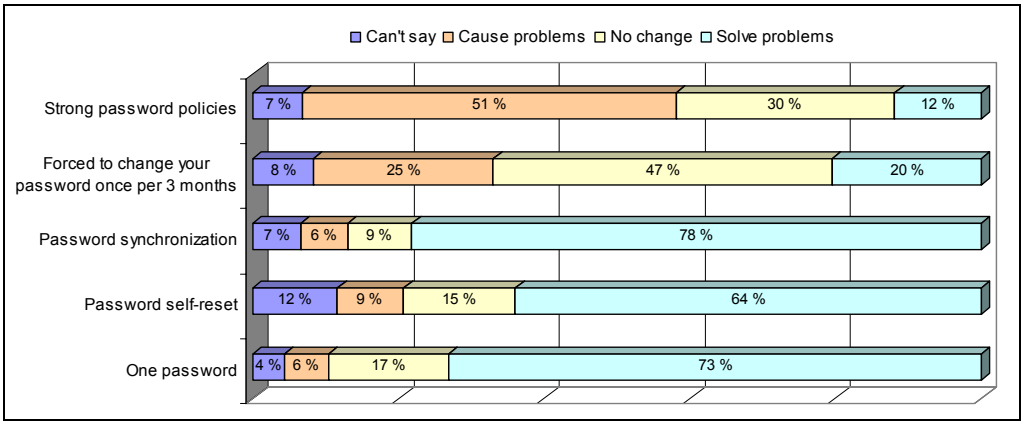

Figure 15: Employee estimation on new system features.

As discussed in chapter 2.1.5, users don't like too much security. This is shown in the values of Figure 15 when asked about how users would feel, if strong, centralized password policies were build and they were forced to change their password every 3 months. The latter would keep things pretty much the same, as 3 months is currently the expiration time of workstation passwords. 47% present thought it would bring no change to the current situation. Most likely, users didn't consider that the password would also be changed to many other systems as well, and they didn't have to change their passwords manually. 51% of users think that forcing them to use strong passwords would cause problems. This is very typical, but the same thing can be seen here as with the password expiration question; employees didn't realize that they would have only one (or few) of these strong passwords to remember.

Overall the results received were pretty much what was expected; users want to lighten on the security, decrease the number of passwords (preferably to only one) and manage their passwords from one single location. This is the kind of functionality that can be offered by implementing a centralized password management solution.

3.6.2 Technology

From the technology point of view, the biggest benefits are gained by integrating and harmonizing the password management functions of multiple systems. The number

of systems that users have to use on a daily basis can't be reduced, but when those systems are integrated to centralized password management, users can access those systems using the same password. This negates the problem introduced by the number of different password based systems which led to the problem of having too many passwords and different password policies between systems.

3.6.3 Security

It has been said in many occasions that humans are the weakest link in the security chain. By introducing password synchronization and password reset, that weakest link can be strengthened and by doing so we are strengthening the whole chain of security. There are also some security issues concerning centralized password management it self. The biggest question is whether it is a security risk that users only have one password to access multiple systems. After all, if a malicious person gets their hand on that single password, he is able to access all of those systems. But weighting the options, having only one secret and strong password is more secure than having multiple, weak and exposed passwords.

In (Security survey 2004) company security personnel had to evaluate the impact of centralized password management concept to current information security. Figure 16 shows the results of this evaluation.

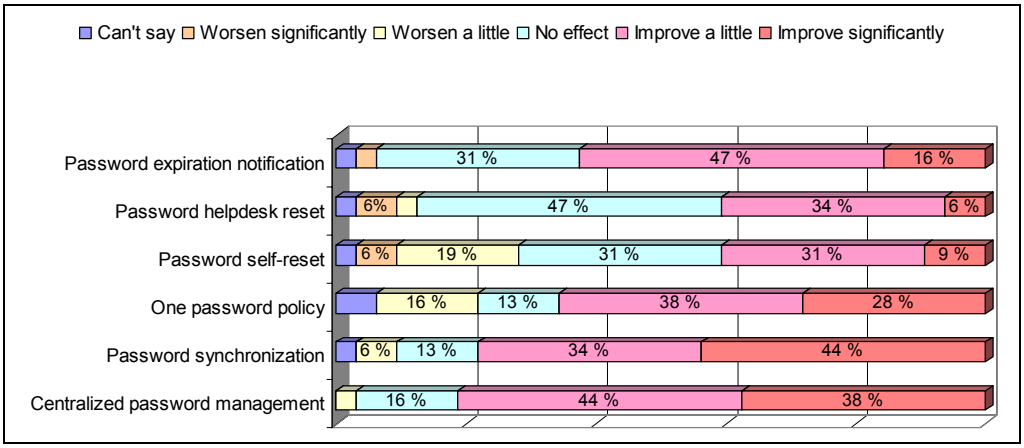

Figure 16: Security personnel evaluation of security risks.

The figures speak for themselves. There is a clear need for improving the security of passwords, and features offered by a centralized password management system seem to offer some significant improvements. Even using a single password policy, where users would have only one password to access all systems is considered to improve security by 64% of security personnel. Password helpdesk reset and password self-service are dividing security personnel the most. 47% think that password helpdesk reset would not have any effect on security, because that is what they are doing it already. The only difference is that with a password management system in place, the whole process of resetting passwords would happen from a centralized place.

3.6.4 Business

Gartner research estimates that password self-reset functionality will decrease password related helpdesk calls by 90% (Witty et al. 2004). This is a quit optimistic estimation. According to company estimates, the percentage is about 30% (Grön 2004b).

In chapter 2.4 it was calculated how much password related helpdesk calls cost to company as big as in our case. The numbers calculated were rather vague, but they gave a good idea on how big of a money hole passwords introduce. By implementing a centralized password management solution with the features presented above it is possible to reduce or at some cases totally negate the problems related to passwords. When employees have fewer problems with their passwords, the password related helpdesk calls will also be reduced. User productivity will hopefully also improve, but in my opinion if employees save that extra 30 minutes once in a while, that does not help to improve employee productivity that much. The increase in user satisfaction is probably more valuable for the business than time savings.

From the company point of view, the cost savings gained from implementing a password management solution would be approximately 490 000 € per year (Grön 2004b, 1). The license and vendor maintenance costs of a password management system would be 450 000 € over a period of three years. So the payback time of implementing this kind of system would be about one year. Of course the internal

costs of maintaining and supporting this solution must be taken into consideration. But overall in the light of these estimates, implementing a password management solution would provide a fast ROI for business, not to mention all of the other benefits provided by the solution. They are all good for business.

3.7 Discussion

Figure 17 shows the same tree as in Figure 9 at page 35. The green boxes added in the tree are solutions offered by a centralized password management system. As you can see, with this kind of system, all problems related to passwords can be affected.

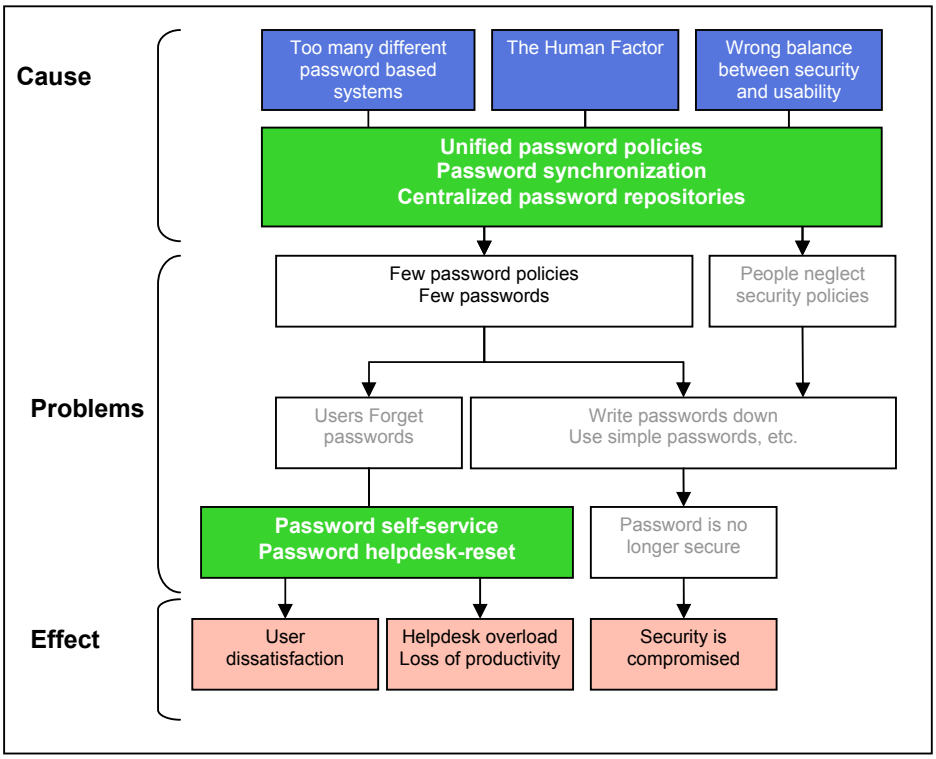

Figure 17: Password problem tree with solutions

It must be emphasized that the point is not to say that all problems will go away when starting to use this system, but the problems will be reduced. This is shown in Figure 17 with the lighter colors. The problems are still there, but they are not as big as they used to be.

Finding solutions to "root-causes" was discussed in chapter 2. As it can be seen in Figure 17, the upper green box does just that. It does not try to treat the symptoms of password related problems, but attack the problems at their source. Password reset functionality on the other hand is positioned right above the effects of password related problems. This indicates that password reset functionality treats the symptoms rather than provides a real solution to the problems. It can be questioned whether password reset functionality is really a needed feature of a password management system. If enterprises decide to implement a centralized password management solution, they should first see what kind of benefits password synchronization, centralized password policies and centralized password repositories bring out. If the users still forget their passwords and crowd the helpdesks, they should consider the deployment of password self-service functionality.

By studying the problems introduced in chapter 2 and the solutions to those problems introduced in this chapter, it is quite clear that a centralized password management system will offer a great value to a global enterprise. In chapter 4 a proof-of-concept type of implementation of a password management system will be introduced and evaluated.

4 A password management system

In this chapter the password management systems build as a proof-of-concept type of implementation is introduced. The purpose of this implementation is to demonstrate the features of a password management system in practice and also to demonstrate, that this kind of a system can be build rather easily from a technical point of view.

First the requirements set for this implementation are described. The requirements are split into two categories: functional requirements and non-functional requirements. The technical environment is also introduced along with the platforms and products used in the implementation. In the final chapter the complete implemented system is evaluated and compared to the specified requirements.

4.1 Requirements

This chapter describes the functional and non-functional requirements for the password management system. These requirements are gathered from the research made in previous chapters. The goal was to gather the "best practices" for implementing password management systems from the usability, technological and security point of view. The requirements are numbered and the numbers are used as reference in the implementation description below. A rationale is also specified for each requirement. The purpose of this rationale is to explain the reasons behind the requirement.

4.1.1 Functional requirements

These requirements describe how the system should behave and what kind of functionality it should provide for users and administrators. Table 5 shows a summary of the functional requirements for a centralized password management system.

Table 5: Functional requirements for the password management system.

#	Requirement	Rationale
1	Users must be able to change their password simultaneously to multiple systems from one place	Users need to have a single place to manage and change their passwords. This eases up password management from the user perspective.
2	The system must support native password notifications from AD	AD is used as the authentication store for Windows workstations and so is the best choice for initiating password synchronization.
3	User password should be synchronized to all systems the user has access to that integrated to the password synchronization process	This requires, that the synchronization engine contains up-to-date information about user's accounts or uses some other method for delivering the password to all account the user has access.
4	Users must be able to reset their passwords using a self-service web page.	Password self-service feature eases up helpdesk overload.
5	Systems must be able to enforce the same, strong password rules to all systems.	Users should not have to deal with multiple password policies.
6	System must be able to enforce the password expiration period on all systems.	Users should not have to deal with multiple expiration periods.
7	System should be able to force people not reuse old passwords.	For password expiration enforcement to be effective, users should not be able to reuse old passwords.
8	System should be able to limit the number of user made password changes on a given period.	For password expiration enforcement to be effective, users should not be able to change their password multiple times in a row, so that they could negate the password history.
9	Helpdesk personnel should be able to reset user's passwords using the system.	The ability to change user passwords from one place should also be available to helpdesk staff, to cause as little work load as possible.
10	Users should be notified of password changes	To increase security, users should be aware of all changes in their passwords.
11	Users using password self-reset should be authenticated.	Users should be authenticated to prevent illegal password resets.
12	Password reset should support admin defined challenge questions	Administrator defined questions are more secure than user defined.
13	Password reset question answers should be validated.	Answers should be validated to prevent users from using simple answers.
14	Repeated failed attempts trying to reset a password should lock the account and notify administrator.	This can indicate a possible malicious action and it should be prevented and administrator should be notified.
15	Password synchronization must not intervene with normal AD operations	The implemented solution should decrease the reliability or performance of the current system.
16	Password reset must be used together with password synchronization to provide good usability.	Password reset functionality is only usable, if the user has to reset the password only once and then it is automatically changed to all systems.

4.1.2 Non-functional requirements

These requirements are not directly connected to functionality but are general requirements for the system. Normally non-functional requirements contain performance and availability requirements, but because this is not an operational system, these kinds of requirements are not presented. The non-functional requirements for a password management system are shown in Table 6.

Table 6: Non-functional requirements for the password management system.

#	Requirement	Rationale
17	All stored passwords must be encrypted	Encrypted passwords minimize the risk of passwords being exposed
18	All communications must be secured	Encrypted communications minimize the risk of password being exposed while being transmitted over a network.
19	System should support commonly used and proven encryption algorithms and secure communication protocols	Only proven and widely used algorithms and protocols that are proved to be safe are used. Proprietary protocols can not be trusted.
20	User interface must be web based.	Web based user interfaces allow the users to access the system from virtually any machine.

4.2 The environment

The environment for the password management system consists of 6 separate servers which contain a total of 16 different software components. These systems are connected through the company's internal network. In addition a number of client computers can connect to the system through the self-service web-interface or by using operation system specific password change mechanisms. The overall system architecture of the password management system is shown in Figure 18.

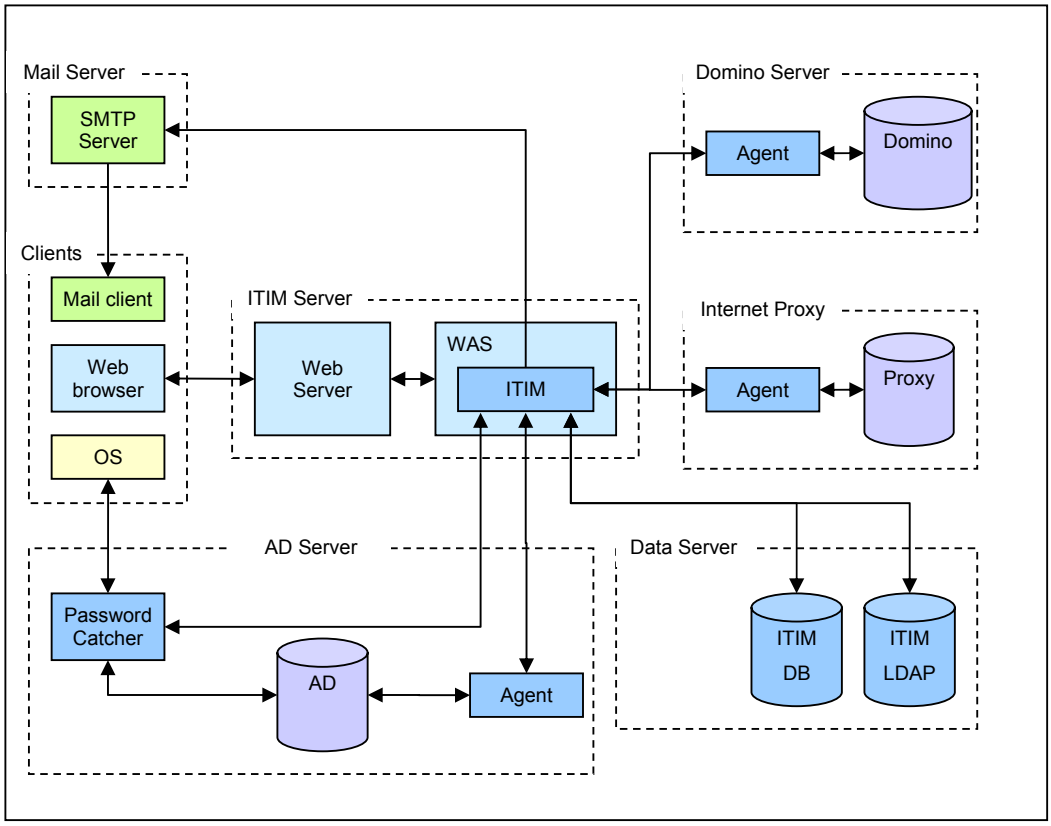

Figure 18: Password management system network diagram.

The dotted lines represent system boundaries, so that each of the dotted boxes resides on different physical machines and are connected through the company's internal network. The arrows represent data flows between these systems. The components shown in Figure 18 are described in more detail in following chapters.

4.2.1 Clients

The clients represented in Figure 18 are standard company workstations. Each workstation has a standard set of software components. The components relative to the password management solution are:

OS	Operating system, Windows XP with SP1
Mail Client	Lotus Notes mail client or Domino web mail
Web Browser	Microsoft Internet Explorer 6.x

These are all standard components and are installed on every company workstation. If a workstation has no mail client, the users can access their mail using a web based mail client through the web browser. The web browser is also used to access the web based user interface of the password management system. The connection between the client browser and the web server is SSL protected, so that all traffic between the components is encrypted. The mail client is used to receive notifications from the password management system. These notifications include password change confirmations in the case of normal password change or in the case of a password reset. If user receives access rights to new systems included in the password management system, a notification about adding this user account to password management system is also send to the user, so that user always knows to which systems the password is synchronized to.

The OS is communicating directly with the Active Directory (AD) server. When a user changes his password on his workstation, the new password is send to the AD server. The password is intercepted by the password catcher component which handles the password change notifications to the password management system.

4.2.2 Active Directory servers

The AD servers contain Windows domain controllers that hold information about the users, groups and settings of the whole Windows domain. When a user changes his operating system password the password is sent to the AD server. The password catcher component intercepts the password and sends it to the ITIM server for synchronization. The password is also directly stored in the AD server so that if there is a problem with the password synchronization, at least the operating system password will be changed so this will not intervene with normal password change operation.

There is also an agent present in the AD server. This agent is responsible for changing the password on the AD server if a user changes his password through the web user interface. The communications between the password catcher, agent and the ITIM server are all SSL protected.

4.2.3 ITIM Server

The IBM Tivoli Identity Manager (ITIM) server is the heart of the password management system. It connects to every target system through agents and also receives password change notifications from the AD server. It is responsible for password synchronization, password notifications and offers a web based user interface for users to reset or change their password. The web interface is described in more detail in chapter 4.3.1.

ITIM is a Java 2 Enterprise Edition (J2EE) application and runs on top of IBM WebSphere Application Server (WAS) platform, which is a fully featured J2EE platform. ITIM connects to a common SMTP mail server to send e-mail notification to users. The e-mails are not encrypted, so no passwords are included in the notifications. Only exception to this rule is when an administrator or helpdesk personnel resets user's password. The randomly generated password is send as clear text to users via e-mail. Users are instructed to change this kind of password immediately.

ITIM server uses two different data stores; a database for storing process related data and an LDAP to store user and account information. These data stores reside on a separate server for performance reasons. The communication between ITIM and the LDAP server is SSL protected, but the database connection is not encrypted since no sensitive data is stored in the database.

4.2.4 Data server

The data server contains two different data stores. These data stores are located on a separate server from the ITIM server for performance reasons. The database is used to hold ITIM specific data like process schedules, password change logs and other history data. The database product is IBM DB2. The LDAP server is IBM Directory Server (IDS) and is used to hold user and account data. Usually there are no passwords stored to the LDAP, but there is couple of exceptions. The password used to access ITIM through the web interface is stored in this LDAP. It is encrypted

using PBE (Password Based Encryption) algorithm. Also if a password history is maintained so that users can't use the same passwords multiple times in a row, the old passwords have to be stored in this directory also. These passwords are hashed using MD5 (Message Digest 5) or SHA (Secure Hash Algorithm) and stored for each account, although the passwords will be the same between every system.

4.2.5 Target systems

For each of the target systems connected to ITIM, an agent must be installed on the remote server. Each type of target system has to have its own implementation of the agent interface. There are three different target systems integrated to ITIM in this implementation; Active Directory, Domino and Internet Proxy. Like described in chapter 4.2.2, Active directory has two functions, first it operates as a target system in the password synchronization process and secondly it is used to notify the ITIM server about native password changes in the Windows domain.

Domino application server is used as a platform for e-mail, messaging services, WAS services and groupware application services. Company intranet is also build on top of domino application servers. Domino is a widely used platform and hosts hundreds of different applications enterprise wide. Some of these applications can be accessed through company intranet and some are only available through Lotus Notes application which is client software for Domino platforms.

The Internet proxy is used to authenticate persons who are accessing Internet from inside the company network. When users try to open up an outside web site for the first time, they are asked for a user id and a password. The proxy is implemented using Squid web proxy cache, which is free, open source software running on UNIX platforms.

4.3 Implementation

Implementation of the password management system is described in this chapter. Basically the implementation of the requirements presented in chapter 4.1 is

described as they are implemented in the environment presented in chapter 4.2. Design choices made during the implementation are also discussed.

4.3.1 User interface

Users can access the system through a web based Graphical User Interface (GUI). Through this interface, users can reset or change their passwords simultaneously to multiple systems. One of the most important features for the user interface is the ability to change the language that is displayed to a specific user. In a global company there are employees from many different countries and not all employees understand English so well that they could use this kind of a system. Although English is the official language at the company and all global applications should use English in their user interfaces, a lack of language support would prevent many employees from using this system. There are 19000 company employees in Finland and most of them are production level workers that are the most important target audience for this system. If the fact that some (or most) of them can't use this system in any other language than Finnish is neglected, those employees will probably not use this system at all. That would be a major setback for the whole system, especially when usability of computer systems has been strongly emphasized in chapter 2.2.2.

ITIM offers a Java based approach for changing the language of the user interface. IBM provides ready made language packs for most common languages. Finnish is not supported, so my own translation of the GUI had to be made. Adding a new language to the user interface only requires adding a group of property files to the ITIM directory that contain translations about the sentences and words used in the GUI. There are a lot of translation to be done, but it is still quite easy, no programming or special skills are required. In fact you could give the property files to someone else that can translate them and you would only have to copy them to the ITIM server. There is one quite irritating problem with the translation of the ITIM GUI; there are about 300 icons used in the GUI which contain text. To translate these icons, you have to draw your own icons or modify the existing icons somehow. Even though this was not hard, it proved to be a very slow process. Figure 19 shows the login page of the password management system in two languages; English and

Finnish. In order to translate this very simple screen, it required to translate 4 phrases in the property files and draw 2 images (the welcome and login images).

Figure 19: Password management login pages in both languages.

The overall translation of the user interface would include translating over 4500 phrases and modifying over 300 images. Because this would be an enormous task, I only concentrated on translating those phrases and images that were actually shown to the users. The administration related phrases and images were not translated.

4.3.2 Password synchronization

Password synchronization in ITIM is based on *accounts* assigned for the user in the ITIM directory. This means, that ITIM has to be aware of all systems integrated to the password management process. These systems in ITIM are called *services*. ITIM also has to know which users have access to which systems. These are called *accounts*. So ITIM contains *services* which contain *accounts* which are in turn owned by some user. ITIM needs to keep track of the user's account in the target systems. If a user is removed from some target system, the users account in ITIM must also be removed and if a new user is added to some target system, the account must be added for the user in ITIM. This seems a little complicated and the reason why ITIM uses this kind of implementation is the fact that it is also used for automated user account management. That is, centrally managing accounts in multiple heterogeneous systems. This causes the password synchronization to be a little bit complicated as

well. The functionality by which ITIM keeps track of users in different system is called *reconciliation*.

Reconciliation retrieves and compares user information stored on a target system with equivalent data stored in the ITIM directory. To determine an ownership relationship, reconciliation compares account information with existing user data stored on the ITIM Server by first looking for the existing ownership within the ITIM system and, secondly, looking for existing aliases defined for each account. Aliases are used only to determine if an account on the managed resource can be matched with a real person in the system. If there is a match of user login IDs to an alias, ITIM creates the ownership relationship between the account and the person. In our company systems, this user id is the same in almost every system. This simplifies the process of determining account ownerships.

From the user point of view, the complicated user and account management features of ITIM don't make any difference. There are two options for users to change their passwords. First, users can simply change their workstation password using the normal password change procedure used in Windows XP operating system (Windows XP is the standard workstation operation system). This will change the windows password to AD and also synchronize the password to all target systems assigned for the user in ITIM. The second option is to use the ITIM web GUI to synchronize the passwords. User needs to log in to the ITIM web interface and a screen showed in Figure 20 is displayed for the user. He can then type in his new password and a password confirmation to assigned fields. Users can also choose when the password is actually changed by defining the date in the "Effective Date" fields and un-checking the "Schedule Immediately" tap. On the bottom of the screen, user can see a list of all target systems the password will be changed to. On the left side of the system list, there is a column called "Rules". By clicking the icon users can see the password rules assigned to each system. In our case, the password rules are the same for every system and they must be the same as defined in AD. See chapter 4.3.4 for more information on the password policies.

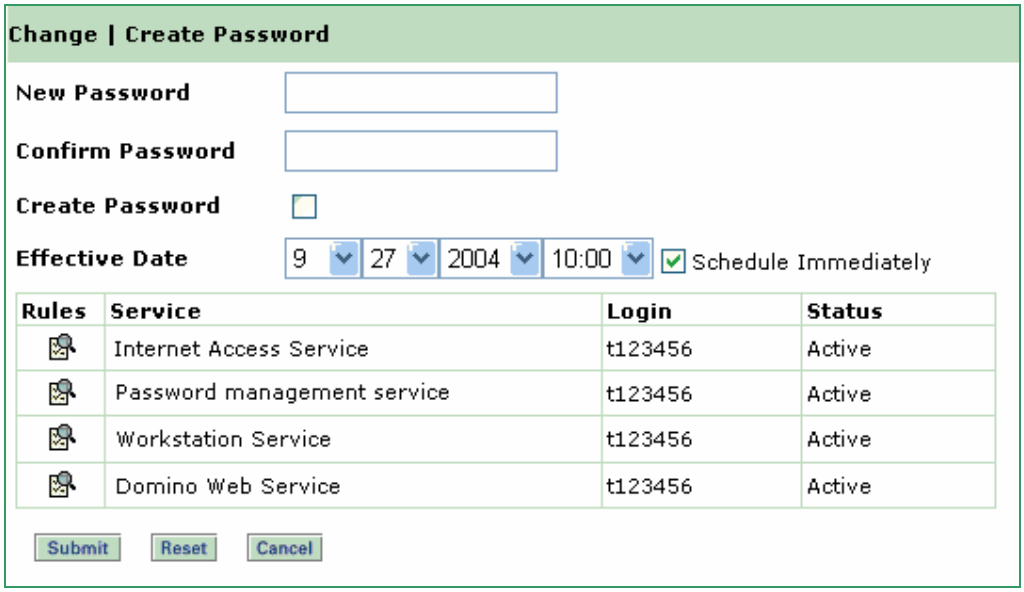

Figure 20: Password change user interface.

4.3.3 Password reset

Password reset can be taken into use quite easily with ITIM. There are couple configuration options regarding the questions and answers used in the password reset feature. ITIM lets you define whether the questions are *administrator defined* or *user defined*. The administrator defined questions can be *pre-defined*, *user-selected* or *random*. With pre-defined option, administrator defines a fixed number of questions that all users must configure. The user-selected option allows the user to select a defined number of questions from a large list of pre-defined questions. Random allows the user to select a number of questions from a pre-defined list, but only few of those questions are randomly selected to be answered on password retrieval.

User selected questions allow users to write their own questions and answers. The administrator may decide how many questions the users must define and how many questions they have to answer on password retrieval. Considering these choices, the user-defined questions are out of the question, because there are so many ways users can choose questions and answers that they might get too easy to guess. From the admin-defined questions, the best choice from security point of view would be random. This would force the users to define multiple questions, like 6, and then only

few of these, say 3, would be asked randomly on password retrieval. This would increase the question and answer space, but it would also require the users to come up with 6 memorable answers to the questions. From the user and security point of view, the best choice would be to define a group of questions and then let users choose 3 questions from them to which they should provide answers. These same questions will be asked from the user every time he wants to retrieve his password.

When a user wants to take password self-reset into use, he must first access the ITIM web GUI. If this is his first time logging in, he will see a message saying, that he must configure the password self-service questions and answers before he can use this functionality. Figure 21 shows the screen displayed to the user. On the left side is a list of pre-defined questions and user selected questions are displayed on the right side. Users can choose the questions by selecting them from the list on the left side and pressing the arrow buttons on the middle. When user has chosen the right amount of questions (instructions are on the top of the screen), he can press the "continue" button.

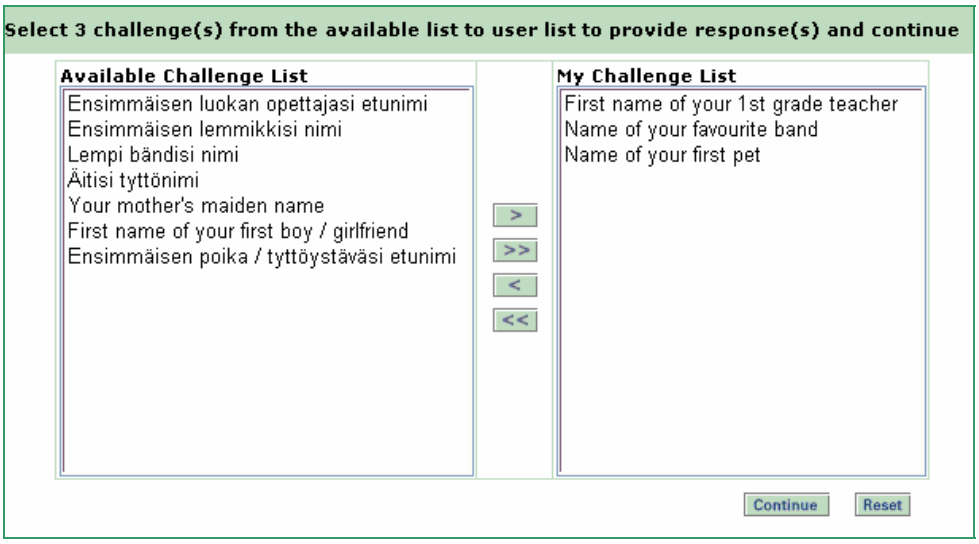

Figure 21: Challenge questions selection screen.

Notice that even if the language of the user interface can be changed like described in chapter 4.3.1, the questions can't be translated to different languages. This is major down side in ITIM password reset implementation. This problem was addressed by

defining the same questions in multiple languages like seen in Figure 21. This is not a good solution if more questions and more languages are needed. The list will be quite long and users should be instructed to find the questions on their own language.

After the question selection is made, user is presented with a screen as shown in Figure 22. It allows the user to define responses for the questions he selected. The answers are provided in the same way as passwords; the answers are hidden with dots and it must be confirmed in order to make sure it was typed in correctly. Unfortunately, ITIM does not validate the answers in any way. The answers must be provided and confirmed for every question, so the minimum length requirement is 1 character and all answers can be the same. This is not very secure, even if the questions are defined by the administrator, the answer to every question can be e.g. "1". This is a major defect in the password reset implementation. There is no point of applying strong password rules, if the password can be compromised through a weak password retrieval process.

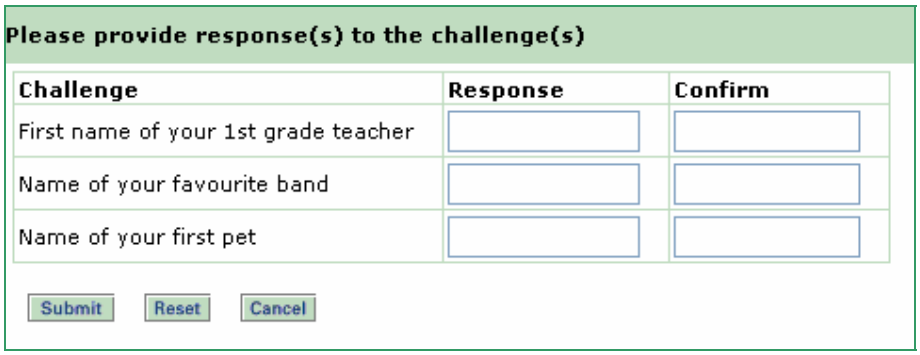

Figure 22: Challenge response screen.

The only comfort in the password reset functionality is that it sends an e-mail notification about a changed password to the owner of the account. So if someone else resets the password, the owner notices this immediately (hopefully) and can call helpdesk to reset the password again. If someone is able to reset someone else's passwords, the helpdesk should advice the legit user to configure the questions and answers again and to use proper answers this time.

After the configuration is done, users can use the system to reset the password themselves if they manage to forget it. Of course if a user has forgotten his password, he can't log on to any workstation in order to access the password reset web-interface. This has been addressed by creating a common password reset account in the Windows domain. This account's user id is "password" and no password is required, so all employees can use this same account to access a workstation. This account has no privileges in the Windows domain, and the workstation is used in kiosk-mode, which means that users can't do anything else with the workstation. As soon as this account is accessed a browser window with ITIM login screen is opened for the user as shown in Figure 19. User has to type in his user id and press the "Forgot your password?" link. A screen like shown in Figure 23 is displayed for the user and he must provide the correct answers for the questions. If provides false answers three times in a row, the user account is logged and an e-mail is send for the system administrators.

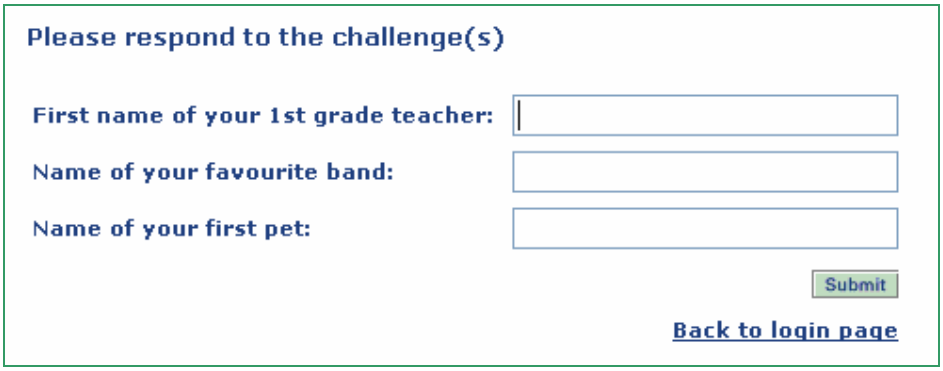

Figure 23: Challenge response screen.

If the answers are correct, user is allowed to change his password using the screen showed in Figure 20. There are also two other options for password retrieval after the user has authenticated himself by answering the questions. An e-mail can be send to the user containing the password, or a link to a web page containing the password can be send to the user via e-mail. The first option is not good, because the password would be send as clear text to the user's e-mail address. The second option is better, but not so usable. To access the web page with the password, user needs to have a *shared secret* defined in ITIM. This shared secret is a kind of initial password for the

system. This option was not used, because of the fact that it adds the number of passwords.

4.3.4 Centralized password policies

The password catcher component for Active Directory supports two types of password policy checking. First, it supports validating the password against password rules defined in AD. If those rules are not met, the password is not synchronized or stored in AD. Second option is to send the password to ITIM server for password validation. If the password is not valid, ITIM sends an error message back to the component and the password is not synchronized or stored in AD.

There is no difference between the two options from functionality point of view, but from availability point of view, there is a difference. If the second option is used where the password is checked in ITIM, there is a change that the validation will fail if ITIM server is not operational. This would mean that the password is not validated and so is not stored even to the AD server. This is against the requirement that password synchronization should not intervene with normal AD password change procedures. If the first option is used, the password is checked in the AD server and will be changed even if ITIM server is not operational. This would only prevent the password from being synchronized. The first option was selected to be used.

The expiration period of a password is now easily configurable, because it is the same as the Windows domain password expiration time. There is no need to force the password expiration in ITIM, although it is possible. The normal password expiration period of 3 months is used.

4.3.5 Target system integration

Primarily ITIM uses agents to connect to target systems. There is a possibility to develop custom Java-based connectors as well, but they were not required in this implementation. For each target system, the following steps had to be made:

1. Install the agent on the target system server.
2. Activate the agent as a service in the server.
3. Configure the agent to communicate with ITIM server
4. Install agent certificate to enable SSL secured communications
5. Ensure agent communications with ITIM server

There was an out-of-the-box agent for AD, but in addition, the password catcher component on every AD domain controller in the AD domain had to be installed so that password changes from all users could be caught. The installation procedure for the password catcher is same as for the agents.

There exists an out-of-the-box agent for Domino platforms as well. This agent knows how to manage user accounts (or person documents in Domino terms) on domino servers. There was a little complication implementing Domino password synchronization with the agent. This was caused by the two password used by Domino platforms. The first is so called *id-file password*, which is used together with an id-file stored on a client computer and is mainly used to access Domino servers with the Notes client. Changing this password also means that the id-file must be re-generated and stored in the client computer. This cannot be done very efficiently, because the id-file is generated at the ITIM server and it should be somehow transferred to the client computer. This is however the default password that the Domino agent tries to synchronize. The second password used by Domino platforms is so called *HTTP password*. All web based services offered by domino use this password:

- Sametime, a chat and a on-line meeting application
- Quickplace, a team room application
- Company Intranet
- All J2EE applications (at the time 3 applications were in production)

It took a little configuration on the agent side to get the HTTP password synchronized instead of the id-file password.

The Internet proxy did not have an out-of-the-box agent, but luckily the proxy uses simple password files to authenticate users. A custom made agent that was implemented using an agent application framework provided by IBM was used. The agent framework provides the interface to ITIM and the only things needed to be implemented are scripts or applications that are run when the agent receives a message from ITIM. The agent framework automatically calls the appropriate scripts and provides the parameters passed from ITIM to the application. This particular script was implemented with Perl and maintained a password file on the server. This file was copied from time to time to the actual password file used by Squid. The solution was not elegant, but it worked.

4.4 Results

In this chapter, the implementation results are analyzed. Each feature is looked from the user, technical and security point of view when feasible.

4.4.1 User interface

The web GUI provided by ITIM is quite intuitive. It is quite easy to easy to use from the user perspective. Not including the password reset functionality discussed more closely in chapter 4.4.3. The translation of the user interface was quite easy when only the parts normal users see were translated. Translating the whole interface including the administrative side is a pretty extensive task, but it is not even necessary, since all company administrators are assumed to understand English.

Overall there is not much to say about the user interface. Normally users would not even use the interface because they could change their passwords directly using their workstation user interface. If the password self-reset functionality was not taken into use, the user interface would be practically useless. From usability point of view this could be a better solution because users could continue to change their passwords through the workstation interface and would not be required to learn to use the ITIM user interface.

4.4.2 Password synchronization

Implementing the password synchronization with ITIM and AD is quite easy. There is not much configuration needed to be done on the default agent configurations and the password catcher component installation is also easy. Overall the agents used by ITIM are pretty much out-of-the box applications that do not need a lot of configuration or tweaking.

On the Domino side the agent needed a little bit tweaking, but in the end it worked fine. Internet proxy agent was implemented using an agent framework and custom scripts. Luckily the proxy used simple password files for user authentication, so that the agent could be used without any problems and it worked fine. It was good that even tough only three different systems were integrated, all systems had their own way of doing things and all implementations were little different.

The password synchronization was also tested quite extensively. There were both performance testing and availability testing. These tests showed that ITIM could handle relatively large amounts of password synchronizations in a short period of time and also it had the ability to endure component and network failures. Even if the password synchronization fails, the password is still changed in AD, which was required. Although password synchronization is not a real time system, it is good to know that the solution can handle error situations.

From the user perspective, password synchronization works like promised. Users can change their workstation password and the same password is changed to Domino and to Internet proxy. Users also get an email confirmation about these two password changes from ITIM. This is good, since it notifies the user when the passwords are actually changed and if they are changed at all. If there is an error in the password synchronization, the user can still use their old password to access the systems and the minute the passwords are changed, user is notified via e-mail. So there is not much damage for the user even if the system is not working.

As said in the implementation chapter, ITIM is quite heavy application to be used just for password synchronization. It is designed to be a complete IM solution with automatic account and user management features. ITIM includes two data stores and it must keep track of users and their accounts. This brings somewhat administrative overhead that is unnecessary for a simple password management solution.

4.4.3 Password reset

The usability of password reset functionality was doubted in chapter 3.2. This doubt was confirmed with ITIM password recovery implementation. First there was the fact that the questions could not be translated to multiple languages, but all questions had to be typed in with multiple languages directly to the user interface. If this would be an operational system, the number of question choices could be quite large and if all questions had to be defined with at least 4 languages, the list of questions would become very large and it would be difficult for the user to find the right questions from the list.

Also there was the implementation flaw that the answers were not validated in any way. This basically prevents us from using this feature in an operational environment, since it exposes a significant security risk. Even tough ITIM sends an e-mail message to users when their password is changed, the damage could already be done before the user notices this and contacts helpdesk. The password reset functionality provided by ITIM did not meet all expectations. The only positive thing was that the actual retrieval process of the passwords is implemented well. The user has to provide the answers he has previously configured and is immediately allowed to set his password. Unfortunately it could prove to be difficult for most users to even get this far.

4.4.4 Centralized password policies

Enforcing the use of centralized password policies works very well between the three synchronized systems. All of these systems allow the use of strong passwords, so there were no limitations on password policies used. Also the fact that these

password policies can be modified from one central place (AD server) without going trough the trouble of configuring each system separately, gives us good flexibility and ability to change these rules (mainly weaken if necessary) when new systems are brought on board.

The decision to use AD as the central password policy server also gave us the benefit of controlling the password expiration interval easily. None of the integrated systems have any limitations on password expiration periods, so the commonly used 3 months could be used. There is also another benefit of not having to send e-mails to user about expiring passwords from ITIM. The Window's own password expiration pop-ups handle the notifications efficiently. Moreover the synchronization process forces the password change process in systems that do not normally have password expiration functionality.

Overall the enforcing the password policies between these systems using a centralized server works nicely and it mainly comes with the password synchronization implementation without any additional configuration or implementations.

4.5 Discussion

A password management solution with password synchronization between three different systems was implemented. A password synchronization product called IBM Tivoli Identity Manager, or ITIM for short, was used. The implementation was quite painless and didn't take as much time as expected. From the requirements described in chapter 4.1 there were only few which were not fulfilled. These requirements (8 and 13) were related to the password reset functionality and to limiting the number of password changes users can make in a period of time.

While testing and analyzing the features of this system it was noticed that password synchronization and centralized password policies bring are the biggest benefits this kind of system offers. The password reset feature was not so usable or secure that it would be practical or wise to implement in a production environment. It was also

noted that providing users with a web based interface just for password synchronization is not necessary if there exists a possibility to use native password change from the workstations. This means that a password management solution that would not cause any visible changes to the way users are used to do things can be implemented. Usability can be increased without the users even knowing about it. From the usability point of view this means that no visible technical solution is provided for the users to learn and this solution is used to fix a problem that was caused by technology in the first place.

Impact on security is pretty hard to estimate from this implementation. Same applies for the business benefits. It would require an enterprise wide solution and a longer time frame in which to study the change in user behavior related to passwords. From the technical security point of view any weaknesses or improvements are not introduced by the systems. It uses strong cryptography to store passwords and encrypted communications to propagate password through networks.

The bottom line is that the solution offers most of the benefits discussed through this book. The products used in this implementation may be questioned, and enterprises thinking about implementing a password management solution should pay a lot of attention to selecting the right product for their needs and for their environment. Also they should consider whether to integrate a particular system to the password management process if the implementation proves to be difficult or costs too much compared to the benefits gained from it. This would happen is situation where the target system would use a proprietary technology and would have only a few users. This would probably make the implementation hard and the cost savings would be minimal.

5 Conclusions

In this thesis I have demonstrated that passwords cause a lot of problems in large enterprises and there is a real need, not just from the security point of view, but from the business and employees side as well to do something about these issues. I also introduced the concept of centralized password management that is promising effective solutions to these problems. The features and possible benefits offered by such a system were discussed and analyzed.

Proof-of-concept type of implementation of a centralized password management solution was made to demonstrate that it can be done in a large heterogeneous environment. Although the implementation was very small, the same requirements, architectures and best practices apply also to bigger, production level implementations. I was able to gather a lot of information which will help us one day, hopefully soon, to implement a production level centralized password management system in our company.

The concept of centralized password management introduced in this thesis seems to provide real-life solutions to many password related problems in large enterprises. The actual long time and enterprise wide effects of deploying a centralized password management solution; cost savings, impact on security issues and emplooyee satisfaction can only be verified by implementing a password management solution and take it into use as a global service that is available to all employees enterprise wide. Only then we are able to prove that this concept actually works.

Centralized password management does not make the problems go away completely, nothing does. If there is one thing that I have learned while working on this thesis, it is the fact that information security is not an exact science. It is about managing risks and finding the weakest links in the security chain and strengthening those chains. Security must be looked from many different angels and only by finding the real root causes of security risks we are able to enhance the overall security in a global enterprise.

REFERENCES

Adams, A. & Sasse, M.A. 1999. Users are not the enemy. Communications of the ACM, Vol 42, No. 12. Pages 41-46.

Allan, A. & Enck, J. & Wagner, R. & Witty, R. 2003. Identity and Access Management Defined. Gartner Research. 6 pages.

Allan, A. & Witty, R. 2003. Best practices for managing passwords. Gartner Research. 10 pages.

Anderson, R. 2001. Security engineering: A guide to building dependable distributed systems. New York: John Wiley & Sons. 612 pages.

Bohan, K. 2002. Everything you always wanted to know about choosing a password management solution. Technical Enterprises Inc. 4 [e-document][Retrieved September 20, 2004] From: http://www.proginetuk.co.uk/pdf/technicalsupport.pdf

Brittain, K. & Witty, R. 2002. Password reset: Self-service that you will love. Gartner research. 5 pages.

Brostoff, S. & Sasse, M.A. 2000. Are Passfaces more usable than passwords? A field trial investigation. In Proceedings of HCI 2000. Pages 405-424.

British Standard. 1995. BS 7799 Part 1: Code of practice for information security management. 51 pages.

Conklin, A. & Dietrich, G. & Walz, D. 2003. Password-based authentication: A system perspective. In Proceedings of HICSS 2004. 10 pages.

Dourish, P. & Delgado de la Flor, J. & Joseph, M. 2003. Security as a Practical Problem: Some Preliminary Observations of Everyday Mental Models. Proceedings of CHI 2003 Workshop on HCI and Security Systems 2003. 3 pages.

Grön, J-E. 2003. Orientation to Company Infrastructure. Internal document. 17 pages.

Grön, J-E. 2004. Automatic provisioning and Password management Cost savings. Internal document. 2 pages.

Hinson, G. 2003. Human Factors in information security. IsecT Ltd. 5 pages. [e-document][Retrieved September 23, 2004] From: http:// www.infosecwriters.com/ text_resources/pdf/human_factors.pdf

Holmström, U. 1999. User-centered design of security software. Helsinki University of Technology. Finland. In proceedings of HFT 1999. 9 pages.

Internal Security personnel password management survey. 2004.

Internal User password usage survey. 2004.

Internal. 2004. Group presentation 2004. 36 pages.

Internal. 2004. IT Global Service catalogue. 41 Pages.

Just, M. 2003. Designing secure usable credential recovery systems with challenge questions. CHI 2003 Workshop on Human-Computer Interaction and Security Systems. 4 pages.

Klein, D. 1990. "Foiling the cracker": A survey of and improvements to, password security. Proceedings of the United Kingdom Unix User's Group, London, July 1990. 11 pages.

Morris, R. & Thompson, K. 1979. Password security: A case history. Communications of the ACM, Vol.22, No.11. 6 pages.

M-Tech. 2003. Password management best practices. 17 pages.
[e-document][Retrieved September 20, 2004]
From: http://www.psynch.com/docs/best_practices.pdf

M-Tech. 2004. Case Study: Password synchronization vs. SSO. M-Tech. 11 pages. [e-document] [Retrieved September 20, 2004]
From: http://www.psynch.com/docs/password-synchronization-vs-single-signon.pdf

M-Tech. 2004. Password management project roadmap. 20 pages. [e-document][Retrieved September 19, 2004] From: http://www.psynch.com/docs/password-management-project-roadmap.pdf

Patrick, A. 2002. Human Factors of Security Systems: A Brief Review. National Research Council of Canada. 6 pages. [e-document][Retrieved September 24, 2004] From: http://www.andrewpatrick.ca/passwords/passwords.pdf

Poulsen, K. 2000. Mitnick to lawmakers: People, phones and weakest links. [www] [Retrieved September 29, 2004] From: http://www.politechbot.com/p-00969.html

Protocom Development Systems. 2003. Global password usage survey. 33 pages. [e-document][Retrieved September 21, 2004]
From: http://www.protocom.com/whitepapers/password_survey.pdf

Protocom Development Systems. 2003. Single sign-on password replay vs password synchronization. 13 pages. [e-document] [Retrieved September 20, 2004]
From: http://www.protocom.com/whitepapers/sso_vs_passwordsync.pdf

Rainbow Technologies. 2003 Password survey results. 3 pages. [e-document] [Retrieved September 21, 2004]
From: http://www.avnet.co.il/PasswordSurvey_Results-July20032.pdf

Reed A. 2004, The Definitive Guide to Identity Management. Realtimepublishers.com. [e-document][Retrieved September 24, 2004] From: http://www.rainbow.com/insights/IDeBook/index.asp

Sasse, M.A. & Tygar, J.D. & Weirich, D. 2001. Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. BT Technology Journal, Vol 19 No 3, pages122-131.

Schneier, B. 2004. Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons. New York. 412 pages.

Weirich, D. & Sasse, M.A. 2001. Pretty good persuasion: A first step towards effective password security in the real world. University College London. 8 pages. [e-document][Retrieved September 24, 2004] From: http://www.cs.ucl.ac.uk/staff/D.Weirich/nspw2001.pdf

Whitten, A. & Tygar, J.D. 1999. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Proceedings of the 9th USENIX Security Symposium, August 1999. 15 pages.

Witty R. & Brittain, K 2002. Password reset: Self-service you will love. Gartner research. 5 pages.

Witty, R. & Allan, A. & Brittain, K. 2004. Justify Identity Management Investment With Metrics. Gartner Research. 7 pages.

Yan, J. & Blackwell, A. & Anderson R. 2000. The memorability and security of passwords - some empirical results. University of Cambridge. 13 pages. [e-document] [Retrieved September 20, 2004] From: http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-500.pdf

Appendices

Appendix 1: Company employee survey

Foreword

Dear co-workers,

The purpose of this survey is to gather information on how employees manage their passwords and what problems they experience with passwords on a daily basis. The results of this survey are used in the development of an efficient, user-friendly, centralized and secure password management system that would lighten the burden passwords cause to employees.

Note that this is an anonymous survey, only your job description and expertise are recorded. If you feel uncomfortable answering to some of the questions or do not know how to answer, feel free to leave the question unanswered.

I would like to thank in advance all of you who participate in this questionnaire. By completing the survey you are helping in the development of our password management system, as well as helping me write a better master's thesis on a subject "Developing a centralized password management system for a global enterprise". Any suggestions and feedback on how to improve password management in this company are most welcome.

Best regards,

Mikko Ylén
Implementation Specialist

(Continued)

(Appendix 1 continued)

Background information	
Gender	Female Male
Age	less than 25 25-35 36-45 46-55 over 55
Location	Canada China Finland France Germany UK USA Other
Job function	Finance HR IT Communication General Administration Production Maintenance Logistics Sales & Marketing Safety & Environment
Job level	Manager Employee Trainee
How much do you know about information security policies at our company?	I have not heard about it I know something about it I am familiar with it Information security is part of my job

Personal password usage habits.
0 = No 1 = Yes
Have you ever written down your personal password(s) to a piece of paper?
Have you ever stored your personal passwords to a device such as a computer or a mobile phone?
Do you use the same password for many systems?
Have you ever logged on to a system using someone else's password?
Are you using some password that is shared between multiple employees?
Do you use the same passwords at work and at free time (e.g. in the Internet)?
Do you know who to contact if you have forgotten your password?
Do you think your passwords are good passwords?

(Continued)

(Appendix 1 continued)

Number of passwords
0 = 0 1 = 1-3 2 = 4-6 3 = 7-10 4 = 10-20 5 = more than 20
How many different work-related passwords you have in use (Notes, personal workstation, intranet, Internet etc.)?
How many different passwords you have to remember in total (work + free-time)?
How many times have you forgotten your password during past year?
How many times have you contacted helpdesk on password related issues during past year?

How often do you change your passwords?
0 = at least once per month 1 = at least once per three months 2 = at least once per six months 3 = at least once per year 4 = less than once per year 5 = Whenever the system says my password will expire

Have you ever shared your personal passwords with anyone?
Yes No
With who have you shared your personal password with? (Check all that apply)
I haven't shared my passwords My manager Helpdesk personnel Co-worker System-administrator Stranger Friend Family member Other
What methods have you used to share your personal password? (Check all that apply)
I haven't shared my passwords E-mail Face-to-face On the phone Shouted across the room Text message (SMS) Using a piece of paper Other

(Continued)

(Appendix 1 continued)

How do the following problems affect your daily work?
0 = Can't say 1 = Not a problem 2 = A problem 3 = Prevents me from doing my job
I have so many passwords that I can't remember them all.
I have to access so many systems that sometimes I forget what password is for which system.
Passwords in general are hard to remember.
It takes a long time to reset my passwords if I forget them.
I don't know what to do if I forget my password.

In your opinion, how would the following features affect your daily work?
0 = Can't say 1 = Would cause problems 2 = No change 3 = Would solve problems
You would have only one password to access all systems.
If you forgot your password, you could reset it your self from intranet.
When you change your personal workstation password, the same password would be changed automatically to all other systems at the same time.
You would be forced to change your password once per 3 months.
Your password is forced to be at least 8 characters long and contain mixed small and upper case letters and numbers.

If you have any experiences or problems related to password usage at work, please let us know
If you have any suggestions or ideas on how we can make password usage more user-friendly and efficient, please let us know.

Appendix 2: Company Security personnel survey

Foreword

The purpose of this survey is to find out security personnel's thoughts about password related issues from a security point of view and gather ideas and suggestions for improving password management in this company.

I would like to thank in advance all of you who participate in this questionnaire. By completing the survey you are helping in the development of our password management system, as well as helping me write a better master's thesis on a subject "Developing a centralized password management system for a global enterprise". Any suggestions and feedback on how to improve password management in this company are most welcome.

Best regards,

Mikko Ylén
Implementation Specialist

(Continued)

(Appendix 2 continued)

In your opinion, how big of a security risk would the following situations or actions create?
0 = Can't say 1 = Insignificant 2 = Significant 3 = Intolerable
Users choose hard to remember passwords and write down them down on a piece of paper.
Users choose easy to guess passwords.
Users store passwords to a device like personal computer, PDA or mobile phone.
Users use the same passwords at work and in the Internet (chat rooms, free e-mail etc.).
Users tell their password to IT personnel like Helpdesk or system administrators
Users tell their password to someone they know like co-workers, friends or family members.
Users have only one password that would be used to access all systems.
Users can reset their own password through a web interface by answering to a number of questions that only the user should know answers to (e.g. "What is your mother's maiden name?").
Helpdesk personnel resetting user's passwords.

Compared to current passwords management procedures and systems, would the following features of the new password management system improve or worsen security.
0 = Can't say 1 = Worsen security significantly 2 = Worsen security a little 3 = No Change 4 = Improve Security a little 5 = Improve Security significantly
Centralized password management system: One system which handles all password related functions such as password policy enforcement, password expiration notifications and password resets.
Password synchronization integrated to Active Directory: When a user changes his / her password from a desktop computer, the password would be synchronized to all other systems the user has access to.
One password policy: Users have only one strong password that would be used to access all systems.
Password self-reset: If user has forgotten his / her password, the user can reset their own password through a web interface by answering to a number of questions that only the user should know answers to.
Password helpdesk reset: If user has forgotten his / her password, helpdesk personnel can reset all their passwords using a web based user interface.
Password expiration notification: If a user hasn't changed his / her password in 2 months, the user is notified via e-mail about expiring passwords.

What is your opinion on "one password" policy? (Security risks, usability)?
What is your opinion on password self-reset (Security risks, usability)?
What is your opinion on centralized password management (What problems or benefits)?
What is your opinion on automatic password policy enforcement? (Is it necessary, can it be implemented in practice)?
If you have experiences or problems related to password usage, please let us know
If you have any other comments, suggestions or ideas about how we can improve password management, please let us know.