Global Information Assurance Certification Paper

SANS GIAC Security Essentials
GSEC

Option 2 – Case Study

"The impact of the unplanned business decision"

SANS GSEC Practical Assignment v1.4

Local Mentor Training
Melbourne, Australia
April 2002

Sam Campbell

Prepared by:
Sam Campbell
Infrastructure and Security Architect
treegum@hotmail.com
Date Prepared: 16 September, 2002

Table of Contents

Table of Figures

1 Abstract

I was involved in the design and implementation of a system that combined a public key infrastructure (PKI), email, web delivery of data as well as a number of other electronic services. The authorization system built around the PKI, and other authentication techniques were fundamental to the operation of this electronic data delivery service that is responsible for the sharing of sensitive information between a group of companies.

Due to reasons outlined within this paper, there was a fundamental flaw in the original design of the system – however the resolution of that flaw by business management was on course to increase the risk to the provisioning of the service, by increasing the number of vulnerabilities in the system. The system design is addressed in line with the business constraints imposed by the owners of the system. This paper examines the process followed and the results observed in the new system.

2 Introduction

This paper goes into some level of detail to describe a system that has been built, and a change to that system some time after deployment.

This system started with a user base of 200 users, and is now approaching 2000 users. Per head costs that were initially low have increased by an order of magnitude. Running costs have been very low, and customer feedback regarding the use of the system has been positive.

But…

Downsizing has struck. Unnecessary costs are being stripped from the program, due to budgetary cutbacks. And as this is a production system now, the project group has moved on to other tasks. The business has made moves to eliminate some system controls that are in place to reduce their costs, and have not addressed the security implications of those choices.

There is also a general feeling amongst the user base that the certificates are unnecessary, and get in the way of them doing their jobs. There have been issues with companies having to buy client software to enable the reading of the SMIME mail attachments[1], and other usability issues. The feedback around the 'user experience' indicates a dissatisfaction with the usability of the system – even though in three years there has not been any unplanned outages.

Turning back the clock, the system was originally built to a budget, and a timeline, managed by the business owners. An independent consultant was

[1] Many customers use Lotus Notes which did not support SMIME mail when this system was activated.

brought in to advise on security and technical implementation issues – but like all areas in computer security there were tradeoffs made to meet various constraints. The author is that 'independent consultant'.

The original problem that the system was intended to solve was the sharing of reports run from a database with business customers of the company. The company owns the data (about 2 Tbytes[2]) and have provided a data mining tool to generate the reports for the business customers.

Users are provisioned by generating a key pair, and the production of a user certificate by the third party managed certificate authority[3]. An important factor here is that the certificates are browser based certificates, known as 'soft-certificates'.

Once a user is provisioned, there are various methods through which the user may access the data within the database:

- A web interface, to a java applet style application that communicates through http(s) with the backend application
- Email may be sent from the system to the user, which contains an encrypted report, or other encrypted content (to the users private certificate
- A report may be dropped into a subdirectory on the application server, which the user sees as a windows style 'share' on their desktop. These smb communications are facilitated through the use of samba4 software, an 'smb proxy' package, some client software, and authenticated through the users PKI certificate.
- Other offline modes, driven through the web, such as custom CD generation, tape delivery etc

As you may be able to guess the above project was very large, with many parties involved, from the company owning the data, to the application vendor for the data mining product, to the database vendor, to the managed service provider for the PKI, and so on. This paper will not attempt to describe the interactions, structure or design of the components of the system, except where necessary to discuss issues relevant to the subject of this paper – I want to keep it under the several hundred pages that were necessary to design and adequately document the system!

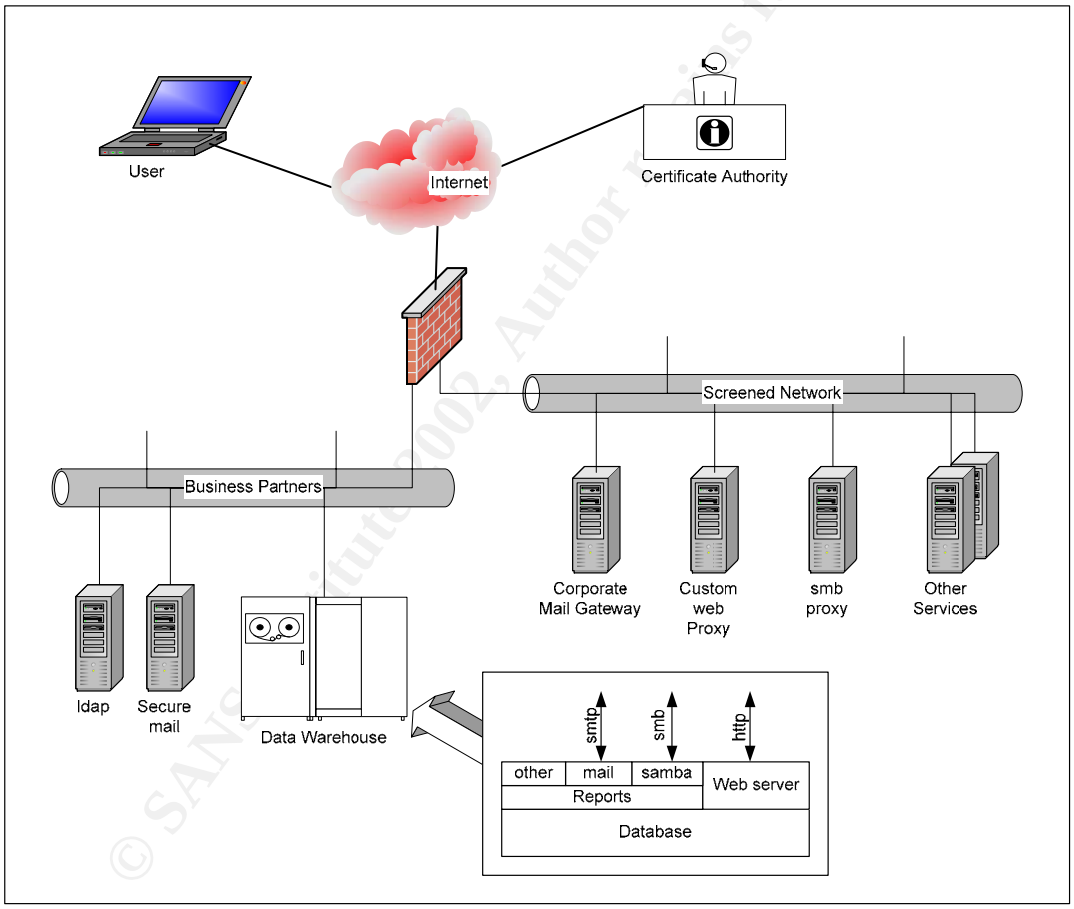
As you may also gather, although I have used the headings before / during / after, you will see that due to the primary security issue I address the lines are blurred between the section names and the desired contents – this is unavoidable, as I trust may become clear to the reader.

[2] 2000 MBytes
[3] Certificate Authority – A full description of a PKI system is beyond the scope of this document, and the reader is expected to be familiar with the operational model. Please refer to websites listed in the section 'Acknowledgements, References'
[4] Samba – www.samba.org - A software package to allow a unix server to appear as an SMB (or Windows) server.

3 Setting the scene (Before)

A diagram of the initial system, as outlined in the introduction, is presented in Figure 1 on page 5. The initial service provision is outlined in the introduction so I will not restate that here, but I will go into a little more detail about how the certificates are used, and some subtleties of information flow within the system.

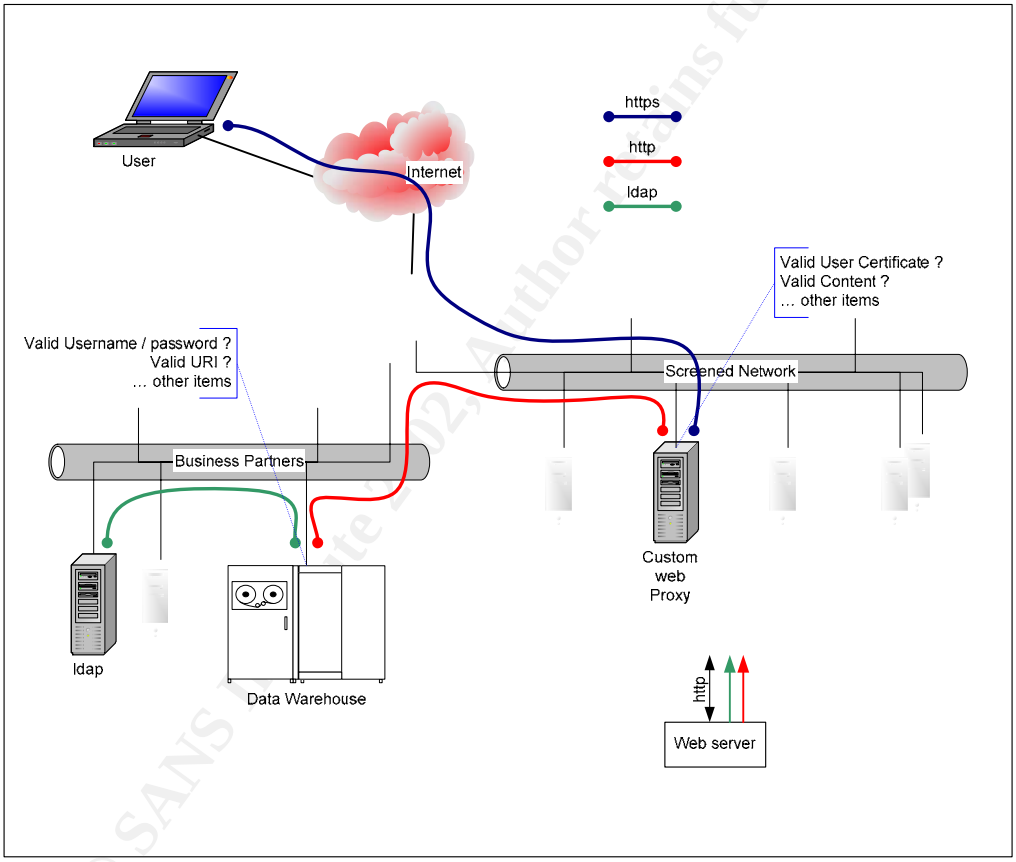
This understanding of the system will then be followed by a discussion of the fundamental flaw in the system, and what the business has decided to do about it.



• Figure 1 - Initial Implementation

3.1 Information flow – http(s)

The primary use of the service is through the web interface. The web interface is presented by the web server on the data warehouse. This is only an http server, which is locked down to only allow http communication with the 'custom web proxy' in the DMZ. The custom proxy transfers the data into https, makes decisions based on certificate content, and some content inspection. Communication with the proxy is only allowed with a valid user certificate, issued by the CA[5]. If the user has a user certificate, they get a session with the web server on the application server – note that the user then needs to authenticate with the web server using a username / password combination to use the service. This data is kept in the LDAP.



• Figure 2 - web traffic flow

A useful side effect of this design is that no activity from the Internet can pass to the data warehouse without a valid certificate – and the only methods of gaining a valid certificate are through:

[5] CA - Certificate Authority – refer to links in the references section for further information regarding PKI

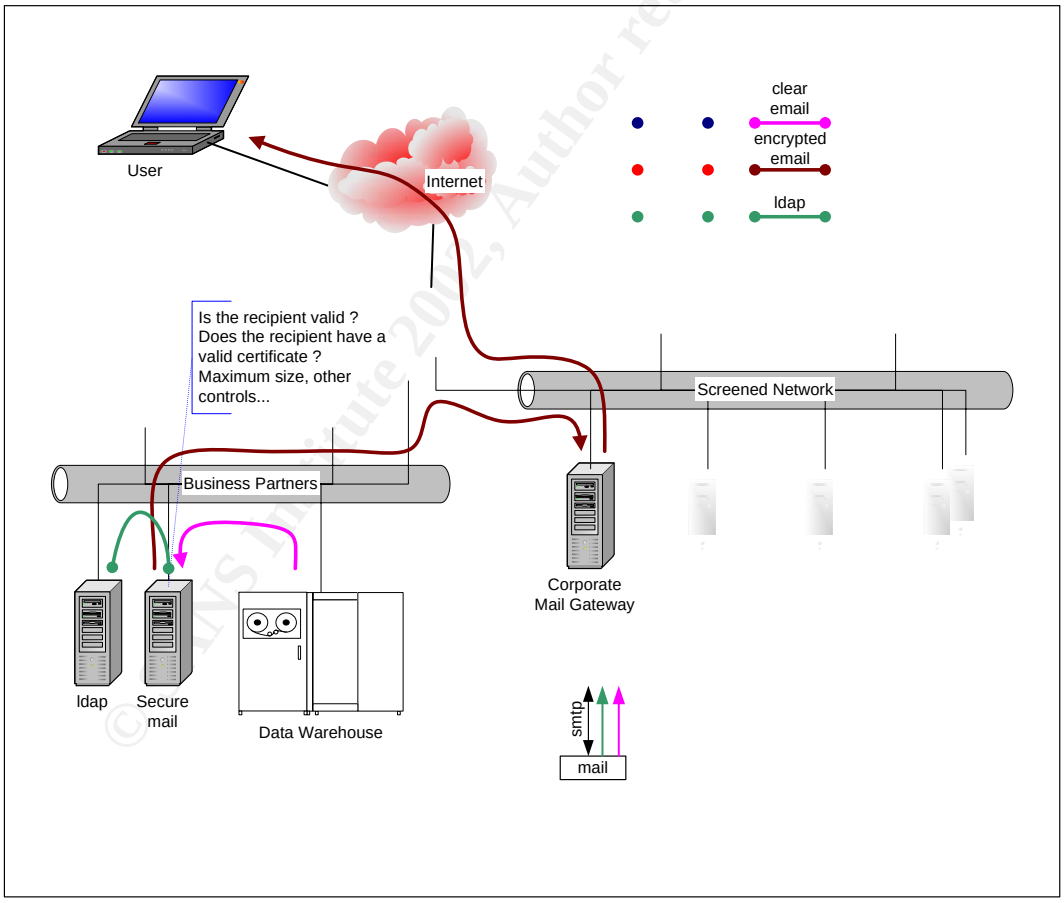
- Using the RA (Registration Authority) process, which involves positive identification of users via known staff.
- Stealing a certificate
- Compromising the CA

This requirement lessens the risk that a content level attack can be applied to the data warehouse, as the number of users that can get to the backend is lowered.

The model for access to the windows shares is comparable, with no access beyond the 'smb proxy' being available without a valid certificate.

3.2 Information flow – email

Another use of the system is the generation of reports that can be sent via email to other people. The components and data path used here are indicated below.



• Figure 3 - email traffic flow

The application has been 'hardwired' to send email output (in MIME format) to the 'secure mail' server, as its default mail gateway. The application makes a connection directly to port 25 on the mail gateway.

The device then finds a valid public key for the recipient in the LDAP, and encrypts the mail (to SMIME standard – Secure MIME), as well as signing it with a private key assigned to the mail server. This way a user can send a report to a registered third party, and the data is 'stamped' as originating from the service. By the use of controls in the mail server individual users can only send allowable quantities of data per month, and other limitations may be imposed.

If a certificate has been revoked, or expired, the email will not be sent.

3.3 Security in general

In the interests of readability, and to avoid digressing too much, I have not gone into detail regarding versions, configurations etc – suffice to say:

- There is a written security policy governing the use of the service.
- Access control is monitored and governed at the application layer (application configuration), infrastructure layer (web server and proxy configuration based on source addresses and other available data), as well as the network layer (source network) wherever possible.
- The concept of 'deny all but that which is explicitly allowed' is applied everywhere
- All users individually sign a standards of conduct style (clear English and one side of paper!) agreement that covers their use of the service.
- The Employers of the users of service are covered by commercial agreements
- The application is capable of protecting users from one business from the data reports generated by another business – there are no 'shared' areas between groups of users.
- IDS is not displayed on the diagram, however there are NIDS in place, as well as log file monitoring on all components.

3.4 So – what is the flaw?

Interestingly enough the flaws were known on design, but mitigation steps were not agreed due to budget constraints (feel you've heard this on every project run?).

The ability for users to change passwords was implemented, however no forced password change (or other password management principles for that

matter) were ever implemented. So we have a system effectively with 2000 users with static passwords. The system is protected however to some extent by the requirement of using digital certificates. I will not cover here the issues surrounding static password schemes and other password management issues, however the reader might find references such as the SANS reading room on authentication[6] useful.

Digital user certificates – stored on hard disks – otherwise known as soft certificates: It is argued by some in the security field that these are of little value. They are easily stolen, backed up routinely by corporate managed systems etc – so I am inclined to call this 'something you know' a opposed to the usual nomenclature 'something you have'. 'Something you have' often is used for token devices, smart cards and other physical devices – you need to be able to hold the device.

The reference below, from Bruce Schneier's[7] Counterpane website asks the question 'Who is using my key' – despite advice to users otherwise, it has been observed that users of this system have shared their *private keys* from this system with other users. Anecdotal evidence suggests that at the user level they were not too concerned about a third parties privacy – and the certificate registration process was cumbersome.

Risk #2: "Who is using my key?"

One of the biggest risks in any CA-based system is with your own private signing key. How do you protect it? You almost certainly don't own a secure computing system with physical access controls, TEMPEST shielding, "air wall" network security, and other protections; you store your private key on a conventional computer. There, it's subject to attack by viruses and other malicious programs.

Ref: http://www.counterpane.com/pki-risks-ft.txt

The protection of the key pair itself is irrelevant when the keys are freely shared by users.

The major flaws that we are concerned with here are based around authentication. I will address these by looking at the vulnerability and the risk that it may be exploited.

3.5 What are the risks?

Risk: There is no true match between the user certificate and the username / password supplied to the database. There is a risk that the user of a certificate is not the owner of the certificate

[6] http://rr.sans.org/authentic/authentic_list.php
[7] Bruce Schneier – Author, and Founder of Counterpane Internet Security Inc – see References.

Implemented risk management:

- Accepted by business.
- Mitigated against to not be a major risk as the log files between the components are combined on a regular basis to detect the compliance level by the IT staff
- Mitigated against by an education process

Risk: Users may share passwords / certificates. The risk is modeled by the business to be equivalent to the previous risk.

Implemented risk management:

- Accepted by the business
- Mitigated against by an education process

Risk: Due to poor password management systems, users may crack a username password combination by brute force.

Implemented risk management:

- Mitigated against by only allowing connection to any system with a valid user certificate
- Mitigated against by monitoring failed authentication attempts in the event that a malicious individual obtains a valid user certificate.

Risk: Users may email reports and data to arbitrary recipients

Implemented risk management:

- Mitigated against by only allowing email addresses registered with the CA to receive email.
- Mitigated against by application level controls as described in section 3.2

3.6 So – what's the big deal?

It appears that there has been a security plan and policy setout. The risks are quantified, and a trained group of individuals were involved in the design of the business and technological issues surrounding the system. The risks above are not all the risks / vulnerabilities discovered about the system, but are sufficient for the case study.

But … the world turns … things change … people change … someone misses something in the process…

The contract is soon to expire for the PKI service provider. The per user costs have increased, the number of users has grown rapidly due the increased flexibility users are seeing in the service, and the business sees little value in the PKI. It has been noticed that some clients are liberally sharing certificates despite educational efforts against this model. This risk was accepted and mitigated against to a degree, but the business has decided that the benefits gained by the use of the PKI have diminished.

The new owner for the system has just decided that the PKI has to go – so, an external consultant has been engaged to remove the user certificate checking from the web proxy, and stop the email server.

The consultant is not familiar with some of the components, and I am contacted by the company to lend assistance. Time to make the changes…

4 Time to address the issue (During)

So what is the actual problem here? Easy – the PKI linkages need to be broken, to enable the PKI to be removed from the infrastructure. Not a really hard exercise – but not an easy one either. Or is it?

Its time to sit down with the design documentation, refamiliarise yourself with why design decisions were made, and how any of those decisions may be impacted by this change – are the risk to the system the same as before – are new vulnerabilities exposed. What rapidly became apparent is that in the push to reduce costs the new business owner had neglected to seek informed comment regarding the security impact of the proposed changes. My recommendation was to stop making the planned changes, and extend the contract with the PKI provider until a full risk assessment was performed.

4.1 Impact on web traffic

With the use of client certificates gone, users gain access to the web proxy directly from the Internet. The protective mechanism is gone preventing connections with a valid certificate. As username / password validation happens in the backend server, ALL web traffic requests now touch the backend server – unauthenticated traffic now gets through the system effectively to the backend at the content level, with the exception of traffic that is filtered out at the proxy, that is now mainly doing the https / http conversion.

The risk assessment from section 3.5 will now be repeated – but include steps suggested to counter effects mentioned above. The diagram can be seen on page 13 below.

Risk: There is no true match between the user certificate and the username / password supplied to the database. There is a risk that the user of a certificate is not the owner of the certificate

Implemented risk management:

- No longer applicable.

Risk: Users may share passwords / certificates. The risk is modeled by the business to be equivalent to the previous risk.

Implemented risk management:

- The same as before

Risk: Due to poor password management systems, users may crack a username password combination by brute force.

Implemented risk management:

- This is now a much higher risk, as more users, as well as worms coded to talk ssl over http, can now gain access to the backend system
- Mitigated against by monitoring failed authentication attempts at the backend server.
- Mitigated against by fully implementing password management controls into the system, administered by the LDAP server, and accessed through custom web pages.

Alternate risk management:

- Recode the web proxy to either use SecurID (true two factor authentication), or at the very least to perform the username / password authentication function – to prevent direct access to the backend system

New Risk: There will be a lot more 'noise' in the system – it may be more difficult to recognize attacks.

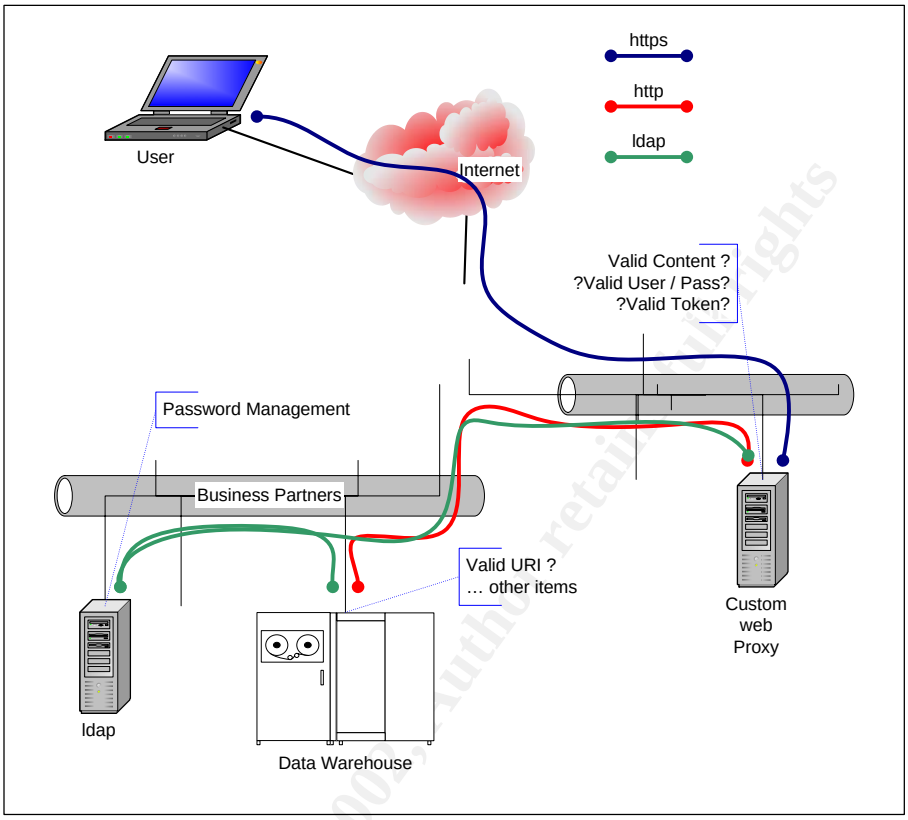
Implemented risk management:

- Acceptance

New Risk: LDAP authentication now needs to be passed through to the screened network.

Implemented risk management:

- Acceptance – it should be managed with existing IDS technology – other mitigation techniques are too costly.[8]



• Figure 4 - Web traffic without certificates

The smb proxy is handled similarly.

4.2 Impact on email traffic

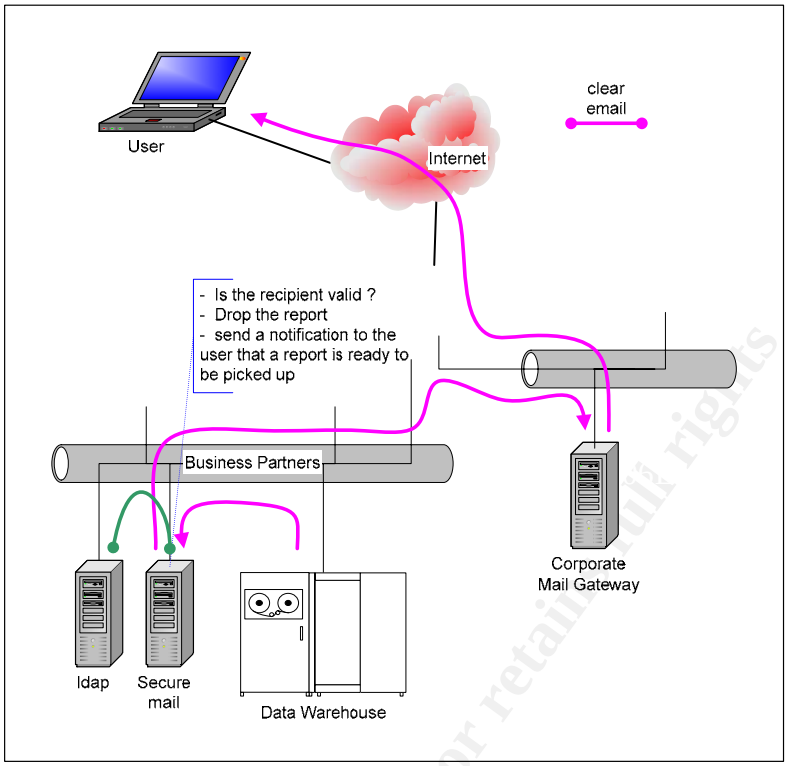
The impact on the secure email system is quite dramatic – without client certificates it is no longer possible to send encrypted email. Due to the sensitivity of the information, secure mail will stop – but the system will be modified to send notification of report completion to the user – this will contain no sensitive information. The notification emails are still applicable as some data mining reports may run for 24 hours or more. This is outlined in the diagram on page 14.

The Risk: Users may email reports and data to arbitrary recipients

Implemented risk management:

- Risk avoided – the system no longer sends sensitive information.

[8] Such as a customer LDAP proxy could be created to only pass 'bind requests' for example.



• Figure 5 - Email traffic without certificates

4.3 So what gets done?

By this stage in the process the new manager has been involved in the discussions and presentation around solving his issue. Debate ensues, the budgets get discussed, and the resultant agreed changes are:

- The PKI is to be removed.
- Code is to be written to move the username / password function to the web proxy.
- The secure mail system is to be recoded to send notification.
- An action plan is instigated to monitor logs for a period of 3 months to determine the increase in manpower required to keep up with the expected increase in load that the systems may be exposed to. If required staffing allocations may be made
- Code is written for web pages to facilitate full password management requirements.
- A project is drawn up to investigate increased activity on the servers and to make a recommendation in one year as to whether true two factor authentication be built into the system – whether it be PKI tokens or SecurID

- *The change management process for the organization is to be revisited and a security trained person, familiar with the infrastructure, is to be consulted prior to (and involved in if necessary) any change to Internet connected systems or processes*.

4.4 Is the security enhanced?

Now that is a hard one! I believe it is – the fundamental security issue here is the human factor – an untrained interested party set about making fundamental changes to an existing service, without full realization of the consequences. The system is believed to be fairly secure[9], and that was nearly undone through no fault of technology – and no choice of technology would have avoided the issue.

If the business manager had asked a technical engineer capable of removing the PKI without asking for assistance, the removal may very well have been done – without any analysis being performed. A level of luck has prevented this system from being made very insecure.

Onto the security of the system as it stands today – is the security enhanced in the system following the risk analysis and suggested changes? It *is* believed that the system is actually *more* secure. This is because mail is no longer sent from the system. Data was traveling out at the rate of 50 MB per day – this is now down to 'notification emails'. The chance of undetected information leakage is substantially reduced. If the logs on the web server and the IDS do their jobs then it is believed that there is slightly more chance that a web attack may be undetected for a longer period of time. In the eyes of the business the privacy of the data is more important than the integrity of the data (the data is a warehouse that is refreshed from a master image on a regular basis). The privacy may be considered to be breached if too much data flows from the system.

Accurate base lining of the network infrastructure is expected to assist in the likelihood of showing up someone successfully hacking into the system and stealing data. Of course if the malicious hacker is dedicated and careful he can sneak under this one. This is expected to be little different from the situation when the PKI was connected.

Following the process of addressing vulnerabilities, based largely on an initial risk assessment done as a part of the original design of the system, and assessing the risks associated with those vulnerabilities allowed us to prioritize those that immediately needed fixing, and those that could wait.

5 Time to pack the bag, and move to the next task (After)

It's now a short time after the system redesign has taken place. The business has recovered from the alarm bells ringing in the backs of peoples minds as they have realized what nearly happened – their prize application

[9] You don't know what you don't know! Any security person must realize that its what they don't know that is the real risk ☺

that they share with their business partners may have become a newspaper piece, had the changes gone through as planned – they want a post incident review.

A panel of managers is assembled with the charter of evaluating such things as 'what (nearly) went wrong', 'how do we avoid it happening again', and 'are we better off'? They discussed the incident with the business manager concerned, they discussed the incident with myself, and also brought in the project manager for an hour interview who was responsible for the original project.

5.1 The findings of the panel

In order of priority, what actions have contributed most to the learning of the company and/or increased the security at the present time?

- The change management process for the organization was flawed, and has been addressed
- The secure mail system is to be recoded to send notification.
- Code is to be written to move the username / password function to the web proxy.
- Code is written for web pages to facilitate full password management requirements.
- Code is easy to implement to integrate SecurID into the custom crafted apache web proxy, as there is a plug-in to do this – if the company chooses to take that route[10].

The business is under large pressure to reduce costs, but -

- If the flagship product is compromised, there is no business

The PKI has had usability issues, that have caused more public comment than any other part of the system

- The business will take ownership of sociability testing if PKI tokens are used, as well as supplying client side software if necessary to users, rather than the previous method of leaving it to the customers to resolve.

It was found by the panel that the company had learned a large lesson in this event, by uncovering a flaw in their business process. In effect, the immediate issue was addressed as soon as the new risk analysis was initiated.

[10] http://www.rsasecurity.com/products/securid/techspecs/apache.html - RSA code to integrate SecurID and the apache web server

Good security is like the principles of high availability in computing: there should be no single points of failure in a system. This parallels the principle of 'defence in depth'.

6 And in closing...

It is the feeling of this author that PKI may be an integral component of a user friendly secure service – if used correctly. Don't cut corners if you can avoid it, and be VERY aware of your user base, and how they relate to your business (friendly, unfriendly, internal, external, business partner, compartner[11], unknown). When I designed the system some years ago, it would be fair to say that much hype surrounded the technology, with little true real world implementation experience to be found outside of 'full integrated solutions' from a single vendor. Integrating applications and infrastructure components from different vendors contained not insignificant implementation risk for the project team.

Many software components did not work together out of the box, but knowledge of the underlying technology went a long way in the resolution of issues. Microsoft IE had a bug which made life very difficult when using client certificates[12] – there are many components that cause issues. Get the right combination of skill sets when you head down this path if you want to achieve success!

A key driver for implementing PKI is a move towards unified login procedures – anything to ease the password issue cannot be a bad thing. The following is taken from the document "Best Practices for Secure Development"[13].

> Help the Users
>
> - Do not annoy users by uselessly asking for security information. Repeated login prompts instead of temporarily caching credentials do not increase the security as it might be expected. On the contrary, users become insensitive to password prompts and will automatically type in any prompt resembling the known dialog box, thus increasing the risk of vulnerability to malicious code. [Peteanu]

Security technologies and security processes go hand in hand.

[11] Competitor / Partner

[12] http://support.microsoft.com/default.aspx?scid=kb;en-us;Q265369 - the issue is that session keys time out every two minutes, which isn't normally a problem, however if the user has selected 'Enable strong private key protection' then he will be asked for his password every 2 minutes to unlock the private key.

[13] Best Practices for Secure Development - Razvan Peteanu, available from http://members.rogers.com/razvan.peteanu

7 Acknowledgements, References and further reading

This page lists some sites referred to for this paper, and which may be useful for a reader who would like to do additional research. Where specific extracts are used these are referenced on the appropriate page.

PKI Resources:

The NIST PKI program - http://csrc.nist.gov/pki/

Counterpane whitepaper regarding the risks of PKI: http://www.counterpane.com/pki-risks.html

An Open-source project to document the current PKI standards and practical PKI functionality: http://ospkibook.sourceforge.net/

Samba:

The Samba home page: http://au1.samba.org/samba/docs/

From the Samba website: Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients. Samba is freely available under the GNU General Public License, and allows files to be shared as if from a Microsoft Windows host. This has been used on the application server.

RSA Security

RSA Security are suppliers of SecurID tokens. RSA code to integrate SecurID and the apache web server http://www.rsasecurity.com/products/securid/techspecs/apache.html

Schneier

Author, and Founder of Counterpane Internet Security Inc.

“Secrets and Lies – Digital Security in a networked world” John Wiley & Sons; ISBN: 0471253111

Apache

The apache home: http://www.apache.org

The apache open source web server is a useful base for many applications. In this paper it forms the basis of the web proxy device.

Microsoft:

http://support.microsoft.com

You can expect to spend some time here when researching security – ref footnote 12 on page 17 regarding user certificate prompting issue. The

Microsoft knowledge database entry makes no reference to why it may be an issue for users…

General

SANS training course notes – "SANS Security Essentials".

SANS Reading Room. Of particular interest are papers associated with authentication, to be found at http://rr.sans.org/authentic/authentic_list.php

"Best Practices for Secure Development v4.03", by Razvan Peteanu, location of document: http://members.rogers.com/razvan.peteanu