Global Information Assurance Certification Paper

Clear Text Password Risk Assessment Documentation
The course/certification I am taking is **SANS Security Essentials (GSEC).**
The version of the assignment is GSEC Practical Requirements (v.1.2e).

Introduction
The risks of sending clear text passwords on an enterprise network may be clear to you as a Security Officer or Security Analyst; but the security implications are not always clear to senior management or business leaders. This paper will present a risk assessment on sending clear text passwords across an enterprise network.

About the Risk Assessment Process:
The Risk Assessment Process used here is not my own creation. I have heavily borrowed from other Risk Assessment processes in determining the risks of sending clear text passwords across a network. Most notably, I have used portions of the Facilitated Risk Assessment Process (FRAP), designed and published by Thomas Peltier.[1] His process is simple and elegant, and a must-read for anyone looking for a risk assessment process.

Process Steps:
Based on project team discussion, the Security representative requests input from persons who can assist with the assessment based on the issue being assessed. Together these resources agree to perform the risk assessment for steps 1-5:

- Step 1 – Determine the risk assessment scope statement.
- Step 2 – Determine required research needed and assign tasks to resources.
- Step 3 – Brainstorm possible risks using the research gathered above.
- Step 4 – Determine the priority.
- Step 5 – Identify controls that will mitigate the risk.

After these steps are complete, the Security representative will do the following:

- Step 6 – Schedule meeting with stakeholders to review results from steps 1 – 5.
- Step 7 – Work with project team to document an agreeable solution and an action plan.
- Step 8 – Generate final risk assessment report and obtain appropriate signoff.
- Step 9 – Determine final course of action to complete risk assessment.

Step 1 – Determine the risk assessment scope statement.
When implementing an application or service that stores and/or sends passwords in clear text, this will introduce vulnerabilities to the enterprise. In this document, these applications or services are hereafter referred to as "the vulnerable application." This risk assessment covers applications to be used on the LAN or on an organization's Intranet. Additional vulnerabilities can be discovered for applications sending clear text passwords over the Internet. A sample risk assessment scope statement for clear text passwords would be as follows:

Scope: This risk assessment addresses sending electronic passwords in clear text using the organization's information resources and enterprise network.

Step 2 – Determine the research and assign tasks to resources.

By questioning the project team responsible for implementing the application, it is possible to determine the reasons or myths behind the reluctance to implement an encryption solution. Potential questions include the existence of actual vulnerabilities in the enterprise's switched network, the likelihood and ability for an unauthorized user to obtain the clear text password, and about potential performance impacts on the system and application being implemented. As a result, it is necessary to gather input and research to document the answers to these questions. Some questions may be technical in nature, and others can be political. The questions and answers will be different for each organization. Here are some of the questions and some sample (sanitized) answers:

How do the proposed safeguards for the new electronic process compare to existing safeguards for the existing paper process?
Future uses of products should be taken into account during initial design to keep security in mind. The traffic will now flow across the network. The data within a packet is what requires protection. And if the network is vulnerable, then the application is vulnerable. The vulnerable application and the process it replaces may be a low risk by themselves, but the vulnerability will now be intertwined into the computing environment.

Why do we need encrypted passwords when we have a switched network?
Even though we have a switched network, sniffers can still be installed on individual machines to see the traffic to and from that machine.[2] Although a portion of the environment is a switched network, this does not always hold true for the rest of the network. It is important to note that if not all network segments are point-to-point private connections (i.e., switched or encrypted) promiscuous mode sniffers can still be installed and used on any portion of the network that is not switched.

How tough is it to get the password?
Two ways that an unauthorized user can obtain user passwords is by accessing the operating system's password file or by eavesdropping on the network.[3] Server vulnerabilities could result in obtaining a password file from a system in the organization. A network sniffer can obtain passwords by eavesdropping on the network. The use of SNMP as a management protocol to configure devices such as switches, routers and other network devices also presents a potential vulnerability.[4] SNMP is a security problem: easy to spoof, and itself does not use encrypted passwords. If a user knows or can obtain the private string, they can make any change on the device. Then the user can configure a switch to allow all ports on the switch to be mirrored to a single port. Once this is done, the user on the mirrored port will be able to sniff all traffic across the switch. If you can use SNMP to trick a device into thinking that you are sending it an update, you can reset passwords to vendor defaults. Once you get the password to the device, it is just a matter of time to be able to reconfigure the device.

What could someone get to with the clear text password?
Due to the fact that there is no industry-wide single sign on and security policy solution, most users use the same password across applications and platforms. This results in a good deal of passwords that never get changed as well as use of the same password for everything.

Why have we implemented other systems and applications that send clear text passwords?
Identification of other systems sending clear text passwords is valuable and should be brought to the attention of the Security department. As an organization, we are moving forward with the intention of securing the transmission of all clear text passwords. If a vendor does not provide a supported method for securing passwords sent in clear text, we should find a method of managing the risk until the supported secure configuration is available.

Step 3 – Brainstorm possible risks using the research.
In our Clear Text Password scenario, the vulnerability is defined as the fact that that passwords can be obtained. The overriding risk is defined as someone obtaining the password for use affecting the availability, integrity and confidentiality of the organization's data, applications and network(s). Scenarios that would illustrate these threats to non-technical senior managers or business leaders are as follows:

Risk	Category	Example / Scenario	How would this happen?
Unauthorized user obtains the password and uses it to cause system outages.	Availability	Unauthorized user causes system outage to financial applications.	A password is obtained for an employee who is using the same password in the vulnerable application and a financial application.
	Availability	Unauthorized user changes system configuration in e-mail preventing access to the application.	A password is obtained for an e-mail administrator or an admin on the e-mail server who is using the same password in the vulnerable application and the server.
Unauthorized user obtains the password and uses it to modify or corrupt data.	Integrity	Unauthorized user modifies web page causing embarrassment to officers of the organization.	A password is obtained for an authorized user of a web server who is using the same password in the vulnerable application and the server.
	Integrity	Unauthorized user sends email from Manager or Manager's staff to newspaper employee with false information.	A password is obtained for a Manager's staff member or e-mail administrator who is using the same password in the vulnerable application and email.
Unauthorized user obtains the password and uses it to gain access to confidential information	Confidentiality	User gains access to confidential information in the HR application by using the password that was stolen.	A password is obtained for an employee who is using the same password in the vulnerable application and the HR application.

Step 4 – Prioritize risks.
When determining priority, it is important to get concurrence on definitions of the criteria for vulnerability and impact.

This has been rated a high vulnerability, which indicates a significant weakness in the application. It could also be considered a medium vulnerability, which would indicate a lesser weakness in the application. Low Vulnerability indicates a well-designed system that is working properly.

In most organizations, the exploitation of a clear text password is unlikely to be a high impact, if high impact is defined as something that will put the organization out of business or severely damage the business functions. It is much more likely that exploitation of clear text passwords could cause a medium impact, causing significant damage and cost. The impact would probably not be considered low, because low impact is not significant enough to be considered unusual or outside of the normal daily operations. In today's heterogeneous environment of multiple platforms, databases, and applications that all require authentication, multiple passwords are needed. Because of this, the password a customer uses in an application is also probably the same password used for the e-mail and network password. Helping customers to manage their passwords ultimately lends itself to using the same password on every system. With inadequate controls for passwords across all applications, some passwords can remain static for long periods of time. Therefore, if an application stores and sends passwords in clear text; it can have further reaching ramifications to other business functions.

Different organizations will have different priorities for the risk of clear text passwords. This priority is only a suggested rating. Actions based on this rating system can be determined using the following Vulnerability Matrix, taken from the Facilitated Risk Assessment Process.[1]

High Impact Medium Impact Low Impact		**A**—corrective action must be implemented **B**—corrective action needs to be implemented **C**—requires monitoring **D**—No action required
	High Vulnerability	
A		
B		
C		
	Medium Vulnerability	
B		
B		
C		
	Low Vulnerability	
C		
C		
D		

Our scoring process indicates that the Priority would be rated at "B," and corrective action needs to be implemented. Possible corrective actions are addressed as controls that can be used to mitigate the risk.

Step 5 – Identify controls
The following is a sample list of controls to mitigate the risk of clear text passwords:

1. Use external (network) hardware encryption to secure applications without native encryption

Pros: • Accomplishes the goal of encrypting passwords • Encrypts traffic from the application server	Cons: • Costly • New technology • Could pose a potential interoperability issue between the OS and hardware
2. Use internal (server) hardware encryption to secure applications without native encryption	
Pros: • Accomplishes the goal of encrypting passwords • Server h/w offloads encryption from the OS, freeing up OS processing • Encrypts traffic from the application server. • Potential to use same brand of encryption device and server to minimize chance of interoperability issues	Cons: • Costly • New technology
3. Use Operating system encryption that encrypts stored and transmitted passwords	
Pros: • Accomplishes the goal of encrypting passwords • Secures the entire OS and applications residing on the server • Built-in functionality of the OS • Does not depend on application supported encryption • Planned migration to W2K would support OS encryption	Cons: • Performance (server, client and network) • Relies on vendor to implement error free • NT does not support encryption with non-NT integrated applications • Unknown degree of difficulty for implementation
4. Work with vendor to supply encryption of passwords in application	
Pros: • Accomplishes the goal of encrypting passwords • Inherent to the application	Cons: • Possibility of weaknesses in vendor proprietary encryption • Reliant on the vendor to implement error free. • May be vendor “vaporware”, with an indeterminate amount of time before it is released • Does not address the risk until implemented
5. Purchase of software encryption package to integrate with application	
Cons: • Accomplishes the goal of encrypting passwords	Cons: • Unknown implementation difficulty • May not support integration with multiple vendors
6. Training for user awareness	

Pros: • Raises user awareness of good security practices • Small increase in the likelihood of a user not having the same password for all applications and the network	Cons: • Does not meet the goal of encrypting passwords • No way to enforce • Creates an additional level of complexity for managing users passwords
7. Develop proprietary software encryption method	
Pros: • Accomplishes the goal of encrypting passwords	Cons: • Unknown degree of difficulty for implementation • Relies on programmer knowledge of encryption to implement properly

Step 6 – Schedule meeting with stakeholders to review results from step 1 – 5.
After reviewing the documentation from steps 1-5, stakeholders should discuss any additional questions.

One question from business leaders for which I am still seeking an answer, is "What is the **probability** that this vulnerability could be exploited?" This illustrates one limitation of my risk assessment. It contains Impact and Vulnerability, but is missing that third piece of the puzzle…Probability. In the Octave Risk Assessment process[5], the assumption is that since there is limited data on the threat probability, it is assumed that the probabilities are roughly equal. In looking for articles on the Internet documenting the exploitation of clear text passwords, I found that few reports delve that deeply into what specific vulnerabilities caused the weakness that allowed a hack to occur. I can only imagine that it is not something an organization wants to have released as public information. Any information on determining likelihood or probability that does not require a degree in mathematics would be greatly appreciated.

The Security Representative's recommendation could be a specific control, or set of controls, or it could be as simple as the direction to use an encryption methodology or device to be determined by the project team. Once the direction is determined, an action plan that includes names and dates should be documented.

Step 7 – Work with stakeholders to document a mutually agreed upon solution an associated action plan.
A sample action plan might look like this:

Owner Action	Assigned to	Date	Additional Comments
1. Implement control number 1, to Use external (network) hardware encryption to secure applications without native encryption.	Security Representative and Network Representative	9/01/01	The encryption method or device will be tested and benchmarked for performance.
2. Implement control number 6, Training for user awareness for all current pilot users.	Training Representative	09/01/01	Users will be instructed not to use the same passwords across multiple platforms.
3. Implement control number 4, Because we have worked with the vendor to supply a supported encryption of passwords in the application	Security Representative and Project Technical Lead	10/01/01	The secured configuration will be implemented as soon as it becomes available and will be tested and benchmarked for performance.
4. Once encryption solutions have been tested and benchmarked, the project team will determine if one or both should be implemented in the production environment.	Security Representative and Project Technical Lead	TBD	The project team will report back to the Security Team and stakeholders to share the results and discuss the final course of action.

Step 8 – Generate final risk assessment report and obtain appropriate signoff.
There should be a simple letter with a statement of understanding that is signed by the person accepting the risk and the controls. The risk assessment, the action plan, and the statement of understanding should be attached together with the statement of understanding as the cover page. The owner of the business process should sign this.

Step 9 - Determine final course of action to complete risk assessment.
Due to our risk assessment, we now have a documented understanding with the CIO that in future, all clear text passwords should be encrypted by some method. It will also be included in all bids and requests for proposal that applications using encrypted passwords are preferred to those which do not encrypt passwords. Other examples of future action items could include a standard or policy, published to the correct audience via the Intranet, documentation, or e-mail.

Sources

[1]Peltier, Thomas R., Facilitated Risk Analysis Process (FRAP), Auerbach Publications, CRC Press LLC., December 2000.

[2]Graham, Robert, Sniffing (network wiretap, sniffer) FAQ, September 2000. http://www.robertgraham.com/pubs/sniffing-faq.html.

[3]Franklin Smith, Randy, "Protect Your Passwords," Windows 2000 Magazine. October 1998. http://www.win2000mag.com/Articles/Print.cfm?ArticleID=3844.

[4]Seifried, Kurt, Overview of SNMP, June, 2000. http://www.securityportal.com/lskb/10000100/kben10000107.html

[5]Alberts, Christopher and Dorofee, Audrey, An Introduction to the OCTAVESM Method, Software Engineering Institute, Carnegie Mellon University. http://www.cert.org/octave/methodintro.html.