Information Security: Securing a Network Device with Passwords to Protect Information

M. Ahmed [*]
L. Sharif [**]
A. Issa-Salwe
A. Alharby

ABSTRACT

Information security is a complex and critical subject, conventionally only tackled by well-trained and experienced professionals. The importance of an effective password policy at the device level is obvious and often entire networks can be brought down due to the lack of simple password security on a single device. Typically, there are numerous devices on a network but the router is at the heart of any network which connects Local Area Networks (LANs) to the outside world (Internet). The Internet is essentially a collection of different Internet Service Providers (ISPs) and routers using Border Gateway Protocol (BGP) providing connectivity between different ISPs around the globe. The Internet is expanding at an enormous speed and secure exchange of information is needed by organisations and individuals alike. This paper emphasises the need for an effective device-level password security as an essential component of a more comprehensive organisational security policy. As an illustration, a practical implementation of effective password security is carried out using one of the most widely deployed routers in the industry.

KEYWORDS
Information Security, Password Policy, Border Gateway Protocol (BGP), Internet Service Provider (ISP), Local Area Network (LAN)

PAPER TYPE *Empirical*

INTRODUCTION

Theoretically information security is seen as the branch of information technology that deals with the problems associated with either intentional or accidental misuse, unauthorized access, loss, disclosure, destruction, modification or disruption of data or information. According to Carnegie Mellon University's CERT Coordination

[*] ***Professor of Computer Networks and Communications Engineering, College of Computer Science and Engineering, Taibah University, Madinah, Kingdom Saudi Arabia. mahmed@taibahu.edu.sa***
[**] ***Senior Lecturer, London College of Research, U.K. l.sharif@lcrl.org.uk***

Centre, the number of cyber security incidents reported has roughly doubled every year since 2000. **(Business Software Alliance, 2002)**.

The paper focuses on the importance of device-level password security in a network. Although device-level security is an important subject in itself, we emphasise an approach that takes account of the wider organisational security policy and attempts to present device-level security as an important constituent of this more comprehensive policy. A survey of ten organisations was carried out to understand what approach is taken in the creation and implementation of the organisational security policy in general and device-level password security in particular. We found that most of the organisations surveyed expressed some level of ambiguity about the content and the role of their security policy. In this paper we have discussed some of the relevant guidelines and important issues that need to be considered in the creation and implementation of a good security policy.One important issue that came to the fore during the survey was the apparently laidback approach taken by network administrators with regard to password security on critical devices such as routers. The use of simple text and unencrypted passwords was a common theme despite the availability of appropriate tools on such devices to enforce more stringent security. Routers are typically at the heart of most modern networks performing the all-important function of routing traffic between networks. In today's Internet economy, any disruption or loss of such a vital component of the network will undoubtedly have catastrophic consequences for an organisation. In this regard, we have carried out a practical implementation of password security on a widely used router to illustrate the relative ease with which such devices can be secured.

THE EVOLUTION OF THE INTERNET

The modern Internet was born in the late 60's under the name ARPANET which was primarily a research tool for those carrying out research for the U.S. government under the course of the Advanced Research Project Agency (ARPA). Universities, military, U.S laboratories and researchers at different locations were able to exchange files and electronic messages with each other via ARPANET. As the network grew, it was divided into two: MILNET for military use, and ARPANET for experimental research. In 1980s, a standard for ARPANET communication protocols was specified which later became TCP/IP suite of protocols and remains the foundation of almost all the network traffic today. In 1987 the National Science Foundation (NSF) funded a project to connect six supercomputer centres resulting in a countrywide network that was called NSFnet. The original NSFnet was run over 56K leased lines and NSF also importuned proposals to build a new high speed network. The winning proposal was submitted by different organisations and the backbone of the modern Internet was built. In 1990's, the backbone of this network grew by the accumulation of different long-haul carriers providing leased line connections and ISPs providing local access and short-haul connections. This created a worldwide network in which access is provided to a virtually unlimited amount of resources spanning the entire globe.

INFORMATION SECURITY IN A NETWORKED WORLD

Today millions of people around the globe are connected through the Internet and this allows for instantaneous communication and access to an apparently limitless quantity of information. Almost every single type of communication travels across the Internet including data, video and voice. Communication is the life blood of any business. However,

businesses cannot grow and partnerships cannot be formed without a guarantee that confidential information will remain confidential. The industries cannot utilise the Internet to expand their services and to cut costs unless there is a guarantee that records and information can remain confidential. In order to understand the concept of secure communication over the Internet, envisage the Internet as a gigantic city which is crammed with populace. Endeavour to communicate a secret in such a milieu is complicated, and the chance of someone eavesdropping a conversation between two people increases as the distance between those two people increases. The Internet is truly global and no secret of any value can be communed on it without the assistance of cryptography.

As the Internet grows, its usefulness also increases. For a company to engage in electronic commerce – the sale of goods and services over the Internet – security is a must. Sensitive information such as credit card numbers must be protected and a business must be able to substantiate each and every sale. In addition, businesses can use the Internet to cheaply connect different offices. Inter-office electronic mail and even phone calls can be routed over the Internet. Because sensitive corporate information would most likely be transmitted over these links, the need for security should be obvious. Truly speaking the growth of the Internet depends on security **(Doraswamy & Harkins, 1999)**.

SECURITY POLICIES

A security policy is a document that plays a very critical role in protecting an organization's information while its users share and access the information on a network. In general, many organisations have security policies to manage the company's resources and help to keep authorised users and resources secure.

The focus of this paper is device-level password security and as such it is important to emphasise that device-level security must be understood and implemented within the context of a comprehensive security policy. Networks and applications are constantly expanding. Factors which may impact information security are constantly changing and therefore, technically the security landscape is very fluid. This means that risk management processes and controls must also be planned beforehand to manage the risk associated with this constant change. The significance of risk management lies in its ability to help decide the most cost-effective ways to protect our system while at the same time it also helps in meeting corporate business goals.

A questionnaire was distributed to ten different organisations to ask how their security policy was created and implemented and what it actually contained. Amazingly, it was found that most of these organisations reported that they did not really have a security policy in place. As for the very few that did have some kind of security policy in place, they were candid enough to reveal that it was conveniently adapted from templates found on the web. All of these organisations recognised that the establishment of a security policy was very important but at the same time they conceded that they were not sure how they should address the issue. By way of some brief guidelines, we will discuss some of the important aspects of a security policy.

It is often found that security policies are difficult to understand and require interpretation. The key features of a good security policy are that it should have a good foundation, which is clear, concise, easy to read, effective, meaningful and enforceable. Security policies are often written in an unrealistic manner encompassing ideals but not necessarily addressing the real challenges of businesses. The lifecycle of this

document is between three to five years, requiring reviews on a yearly basis to ensure consistency and alignment with the business goals. It is important that the security policy has full support from the senior management otherwise there is a danger that the document will not be enforceable and no disciplinary action can be taken. The guidelines pertaining to actions and consequences need to be very clear. Both senior management and human resource (HR) involvement is vital in keeping the living document enforced. Also, if the security policy is issued by senior management of the organisation, there is less likelihood that it will be contested and ignored. HR will also need to be involved and will be able to advice on the legal aspects that need to be provisioned and will be able to ratify the policy.

A comprehensive security policy will require the involvement of all business entities. A careful co-ordination of the policy will result in less exposure to risk. It is also a good idea to departmentlise the security policy so that different parts of the policy apply to different departments. The policy should be written in a simple and clear manner so that it can also be used to prove in a court of law that due diligence was performed by the organisation in order to prevent loss and reduce risk. It also proves that the organisation is aware of its ethical and legal responsibilities to protect data and information relating to its customers and employees.

The security policy should be written to be aligned and consistent with business goals. A security policy cannot stand alone; there must be supporting documentation that refers to guidelines and procedural documents. This documentation will define the expected user behaviour so it needs to be written very clearly. The various elements of the policy should be made simple and achievable. If the policy is perceived to be too unrealistic and complicated, it may not be taken seriously and at worst

completely ignored by the users. It is important to highlight and clarify the guidelines and mandatory parts of the security policy. If this is not clear, the users may feel that some parts are optional when in fact they are not and it creates confusion. Some security policies may have sections that exclude certain users; these exclusions should be in the appendix and not in the main body of the document as it could cause confusion. The security policy should apply to all the users of the organisation. This includes consultants, permanent employees and senior management, no matter how remote or local they may be. Failing to consider a user can result in exposure, so it is important that before an entity uses the facilities that they read, agree and sign to the policy document. **(Bellovin, 1989: April; Windowsecurity, 2008: Dec 03,)** It is also important to consider third parties and service providers within the security policy to ensure that these parties abide by good practice and do not expose the organisation to unnecessary risk.

ISO SECURITY FRAMEWORK

In addition to some of the recommendations discussed, the ISO 27000 series consists of an international document series that offer some very useful guidelines in policy creation. It is important to note that this is a vast and open document, as such it is recommended that professional guidance is sought **(Windowsecurity, 2008: Dec 17,)** Some of the more pertinent guidelines and components of an organisation's policy are listed below:

- Base the policy on an international framework (e.g. ISO 27000 series)
- Be clear, direct, specific and concise
- Make the policy enforceable
- Do not use legal terms and difficult to understand jargon

- Involve HR and legal teams and get senior management signoff
- Get senior management to issue the policy
- Involve all the company departments
- Ensure that users have read and signed the policy
- Ensure that the policy encompasses the people factor
- Achieve business goals whilst complying with laws and regulations
- Update the policy at least once a year
- Define everything (this can be placed in the appendix)
- Keep the policy independent of software and hardware solutions
- Cover all the elements from layer one to layer sever of the OSI model
- Authenticate policy for both remote and local access (for logical and physical assets)
- System maintenance policy to be adopted
- Backup policy need to be given high priority
- Antivirus policy
- Antimalware policy
- Anti piracy policy
- Disaster recovery policy
- Business continuity policy
- Vulnerability assessment policy
- Software update policy
- Password policy
- Data confidentiality policy
- Internet usage policy
- Email usage policy
- Information flow policy
- Desktop security policy
- Guest user policy

- Physical security policy
- Mobile computing policy
- Wireless access policy

Although the guidelines and constituent policies discussed may appear to be complex at first, they can be brief and concise and can form part of the same document ensuring that a clear understanding is conveyed.

DISCUSSION

Information security is an issue of critical importance since the modern economy depends on the secure flow of information within and across organisations. A vulnerable system can potentially cause huge damage to an organisation, especially when an organisation is engaged in critical activities; the stakes can be extremely high. On the other hand, a secure and trusted environment for stored and shared information greatly enhances business performance and productivity **(Business Software Alliance, 2002)**.

The paper emphasises the importance of security at the device level. One of the simplest ways to achieve this on network devices such as routers is through setting up encrypted passwords. The importance of device-level password security is blindly obvious and yet many organisations often ignore it at their peril. The study revealed that many network administrators often do not bother to secure devices such as routers even through the tools are easily available. The practical implementation carried out **(Appendix)** illustrates that this can be achieved in a few relatively simple steps. A good device-level password security is of even greater importance for critical devices such as network routers, switches and servers since these devices form the core of most networks today.

The loss or disruption to one of these devices could have fatal consequences for an organisation.

In the survey, when asked about password policies for users, most of the network administrators revealed that IT staff required users to use passwords but did not place any specific restrictions on those passwords such as minimal password length or complexity requirements. A common misconception amongst some of the administrators was that strict password security did not really make any difference since the users did not really have the relevant rights and privileges to access critical parts of the network.Here, we would like to take the opportunity to explain why having an almost non-existent password policy is a bad idea, even when the users have minimal rights. The first reason why password security is important is because the users *do have rights to something*. If this was not the case, the users would not even have accounts on the network. So, whatever resources the users have access to, they must be protected no matter how trivial it may seem.

In order to further understand the importance of password policies, let's look at a simple business model: a small mail order business. In such a business, the orders would typically come in either through the web or by phone or fax. The users are responsible for entering the order into the system so that the customer's order can be shipped out. If a user is only performing order entry, it may not seem that important for them to have a strong password. However, imagine what would happen if the user's password fell into the wrong hands. For instance, in the hands of a cyber-vandal, a bunch of bogus orders might be entered to overwhelm and render the system useless. Even worse, the entire customer database might be deleted, or posted on the Internet or sold to competitors. Likewise, any sensitive customer information such as credit card numbers

could also be stolen and abused. In essence, a seemingly innocent account could be used for malicious purposes. Suppose that a hacker logged in as a user who is normally responsible for order entry and started to manipulate the order entry system. If the orders are deliberately deleted, the user whose account was compromised could potentially be cheated out of commission related to deleted orders, not to mention the angry customers whose orders are lost.Another possible implication of a hacker or an intruder gaining access to an account password (even if the account has very limited privileges) is that this account could be used as a launch pad to gain deeper access into the network and cause potentially immense damage to the organisation.

CONCLUSION

Some important factors need to be considered when writing an effective security policy. The study looked at the importance of device-level password security as an essential component of the overall organisational security policy. A practical implementation of password security using a router was carried out to demonstrate the level of complexity involved. It is easy to see that even for a small organisation, with a relatively simple business model, the absence of an effective device-level password security policy could have very dire consequences. This paper has provided sufficient background on information security and some general guidelines to help organisations appreciate the importance of device-level security and incorporate this into their wider security policy.

APPENDIX

The implementation has been carried out using a widely deployed Cisco router to demonstrate the concept of password security and encryption. It

is important to note that although the configuration steps may be different on other router platforms, the principles behind password security are common on most platforms used in the industry. In general, a Cisco router can be secured using passwords to restrict access. Passwords can be established for both physical and virtual access to the router. There are 5 main passwords associated with a Cisco router. These include:

- ***Enable password:*** Used to restrict access to the privileged EXEC mode on a router. Enable passwords are not encrypted, so they can easily be viewed in plain text via the configuration files from privileged EXEC mode. This type of password has now been super-ceded by the enable secret password.
- ***Enable secret password:*** Also provides access to the privileged EXEC mode on a router, but is stored in encrypted form using the Message Digest 5 (MD5) algorithm. It is strongly recommended that enable secret password is used in all configurations. When both types of passwords are configured the enable secret password takes precedence.
- ***Console password:*** Used to restrict access to a router's physical console port. If a password is not associated with the console port, anyone could walk up to the router, plug in a rollover cable and create a session, gaining access to at least user EXEC mode.
- ***Auxiliary password:*** Much like the console port, a password can also be used to restrict access to the auxiliary port, which may be configured to allow access via an external modem. Whether you're using it or not, it's always a good idea to set a password on this port.
- ***Telnet password:*** A router allows telnet sessions via what it considers to be virtual terminals. Generally, 5 virtual terminals are provided, named vty 0 through 4.

Although the enable secret password is the only one encrypted by default, any of the passwords discussed can be encrypted as required. The first important step in configuring the router is setting a password to control access to privileged mode. Without one, the router's configuration is fair game to anyone with a rollover cable and only a tiny bit of know-how.Passwords are generally configured from global configuration mode, although the console, auxiliary, and vty ports are configured at the line configuration mode.To set the enable password on the router, simply issue the enable password command.

```
Router(config)#enable password mysecret101
```

This will set the enable password to *mysecret101*.

To set the enable secret password, use the enable secret command:

```
Router(config)#enable secret mysecret102
```

The console password is configured as follows:

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password mysecret103
```

The auxiliary password is configured as follows:

```
Router(config)#line auxiliary 0
Router(config-line)#login
Router(config-line)#password mysecret104
```

The telnet password is configured as follows:

```
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password mysecret105
```

ENCRYPTING ROUTER PASSWORDS

All passwords other than the enable secret will appear in the configuration files in plain text. Even though one needs to be in privileged mode to view the configuration files, encrypting all passwords is still a good idea. Eventually, the configuration files are backed up to a network

server, which means that other people may have the ability to access and view them.The command used to manually encrypt passwords is *service password-encryption*. Any password can be encrypted manually by first issuing this command from global configuration mode, and then changing the relevant password as illustrated earlier. Once complete, the *no service password-encryption* command can be entered. In the following example, both the console and auxiliary port passwords are encrypted.

```
Router(config)#service password-encryption
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password mysecret103
Router(config-line)#line auxiliary 0
Router(config-line)#login
Router(config-line)#password mysecret104
Router(config-line)#exit
Router(config)#no service password-encryption
```

Next, the completed configuration can be viewed by issuing the *show running-config* command. The output below is truncated to show only the pertinent information.

```
Router#show run
Building configuration...
Current configuration:
line con 0
password 7 01100F17580457
login
transport input none
line aux 0
password 7 03075218050070
login
transport input all
line vty 0 4
password mysecret105
login!
end
```

Notice that both the console and auxiliary passwords have been encrypted. The vty (telnet) password has not been encrypted since we did not specify it while configuring the encrypted passwords.

REFERENCES

Bellovin, S. (1989, April). Security Problems in the TCP/IP Protocol Suite. *Computer Communication Review*, 19 (2), 32-48.

Business Software Alliance. (2002). *Information Security Governance: Toward a Framework for Action*. Retrieved April 29, 2009 from http://www.bsa.org/country/Research%20and%20Statistics/~/media/BD05BC8FF0F04CBD9D76460B4BED0E67.ashx

Harkins, D., & Doraswamy, N. (1999). *IPSec: The new security standard for the Internet, intranets, and virtual private networks*. NJ: Prentice Hall.

Windowsecurity.com. (2008, December, 03). *Writing an Effective Security Policy*. Retrieved April 20, 2009 from http://www.windowsecurity.com/articles/Writing-Effective-Security-Policy-Part1.html

Windowsecurity.com. (2008, December, 17). *Writing an Effective Security Policy*. Retrieved April 20, 2009 from http://www.windowsecurity.com/articles/Writing-Effective-Security-Policy-Part1.html