

Protection or Productivity? Balancing Trade-offs in Security Policy

Chris MacLeavy

KXA262 Computer Security
School of Computing

Mentor: Jacky Hartnett

Abstract

There are many sophisticated techniques for improving the security of computer systems. When defining security, it is necessary to unambiguously state to users what is meant by 'appropriate use' with respect to a system-wide security focus. The awareness of these boundaries is best made clear through the technical implementation of a policy. Policies, like any link in security's chain, will always be about trade offs; management want a policy that ensures their computing infrastructure is secure, whilst users want security mechanisms that are transparent and do not get in the way of their duties. The compromise that policies create between productivity and protection will always be a delicate one and security needs will dictate the threshold at which these two requirements meet.

Introduction

There are many sophisticated techniques for improving the security of computer systems. Appropriate use of these techniques may require an understanding of cryptographic algorithms, network routers or wireless technologies. However, the problem lies in defining what is meant by 'appropriate' and creating the environment where the users are able to follow this appropriate use. These issues are addressed by defining security policies that encapsulate the security goals to be achieved and how they should be implemented. Legal and ethical controls are essential to computer security. However, the law is slow to evolve and technology continues to grow at a rapid pace. Security is not a product but a process (Schneier, 2000) and it must keep up with rapid changes in technology in order to be effective. Moreover, the knowledge of new security technology is only effective if it is applied to the practical issues surrounding computer security management.

This paper expands upon a case study submitted for assessment in KXA362 Computer Security. The case study was based on Clifford Stoll's "The Cuckoo's Egg" (Stoll, 1989) in which Stoll tracked the movements of an intruder who was, as a result of lack of policies regulating appropriate behaviour in their computing environment, able to move freely about the computer systems of Lawrence Berkley Laboratories. Taking examples from policies developed as part of the case study, some of the main areas of concern in computer security management will be discussed with the main focus on the selection and management of strong passwords enforced through the implementation of a good password policy.

Establishing a Policy

Security is about prevention (Schneier, 2003); whether it be preventing people from breaking into your computer, your car, or your home. However it is important to recognise that although the definition of prevention is to keep the threats from happening in the first place (the ultimate goal of security), realistically policies are implemented to reduce foreseeable threats to manageable

levels. Charles Pfleeger defines a policy as “a statement of the security we expect the system to enforce.” (Pfleeger, 1997). We can therefore deduce from this definition that a system should only be expected to protect the areas of security that are outlined in the policy. With this in mind, the process of developing a policy begins with an up to date list of assets, a clear establishment of how far the company is willing to go to protect those assets, and ends with putting those convictions to paper in a formal policy document. A policy may either be one document, or several smaller, specialised documents that define security goals, processes to achieve those goals, and their respective enforcement mechanisms.

Establishing where security is situated within the company goals is the first step for any company or institution considering security. Bruce Schneier, recognised computer security expert and CTO of Counterpane Internet Security Inc. states that security is “never black and white; and context matters far more than implementing the newest technology” (Schneier, 2000). This statement illustrates that each different security technology plays an important role in creating an overall security solution; cryptographic algorithms are significantly stronger than they were 10 years ago, but that does not mean a company should be lax in clearly defining appropriate behaviour (Guel, 2001). Moreover while new technologies are generally designed to provide improved protection over an individual aspect of security, the nexus between the security goals (the policy’s foundations) and the technology they are applied to must be considered, and success is measured through the application of these policies to effectively unify technology into a system-wide security focus.

At first, a policy may seem like a document that is concerned purely with the regulation of technology; mechanisms for the monitoring of security architecture such as the border protection that a firewall offers (Panko, 2004). Although this is true, a policy is also concerned with the managed security monitoring of what can be considered the non-technical aspects of security. Two of the most important non-technical aspects are physical access and people. The following examples will discuss each of these areas in more depth, referring to the policy statements submitted as part of the case study.

An Example Network Access Policy

When designing secure infrastructure, many look only to what currently exists. However, the rate at which technology evolves should instigate a constant search for something new - something better than the systems that have been compromised before. In his new book “Beyond Fear”, Bruce Schneier states that we simply need to learn “to be smarter, more sceptical, and more skilled about what we already know” (Schneier, 2003). Knowing the attackers, knowing the attacks, and knowing how far you are willing to go to protect your assets plays a vital role in the security decision making process. Therefore, a computer infrastructure should never be designed without appropriately considering security, and addressing the security trade offs that may be needed in order to achieve the desired level of protection.

Threats to a company’s network infrastructure can be broadly classified into two categories; external threats (think of these as threats from the internet), and internal threats (i.e. threats from the intranet). All third parties that wish to access the intranet, particularly computers that store sensitive information, must comply with the one or more policies set in place to govern user access. Figure 1 illustrates some general restriction criteria, taken from the case study’s network access policy.



1. No system, peripheral, or other network device may connect to the network without a necessary, valid and approved purpose.
2. Any connection must agree to be subject to monitoring (to prevent loss of confidentiality, integrity or availability).
3. Any user of such a connection (permanent or otherwise) must comply with the password policy (discussed later).
4. No system, peripheral or other network device may connect to the network without recognised and up to date virus protection software.

Figure 1: *Sample network access policy statements.*

Another contributing factor in the securing of network resources is a secure operating system. Everyone wants computer systems that are feature rich. However, it is true that the more complex a system is, the more vulnerabilities it is likely to have. Therefore, the more functionality an operating system contains, the harder it is going to be to secure. This is what is meant by trade offs: making (sometimes aggressive) decisions on what functionality can be discarded in order to better protect those assets declared in policy goals.

Thus far the technical components that make up the computer infrastructure have been discussed. Good security for these aspects is essential, but the security of a given technology is only as effective as the people using them. Unfortunately, people are the most uncertain variable in the security equation. The following example illustrates why it is so important to provide a clear policy together with good staff training in order to effectively maintain a secure environment.

An Example Password Policy

The placement and regulation of a water-tight password policy is absolutely necessary to guarantee the correct authentication and identification of users. In conjunction with a password policy, system administration should also set up an appropriate user privilege restriction mechanism to help facilitate differing levels of access aimed at preventing events such as unauthorised viewing of sensitive data and other losses of confidentiality, integrity and availability. In theory, the construction of a strong password is not a difficult task. The following examples seek an answer to why people are so inherently lax when it comes to security, and drawing on the case study provide some guidance with regard to regulating behaviour, particularly in the selection and management of good passwords. The following is an abridged list of policy statements and their rationalisations.

Common best practice indicates that user chosen passwords should have, as a minimum, the characteristics outlined in Figure 2. Password length has been increased to 10 characters (a step up from the old 6-8 characters) and should always be checked and enforced by the system upon creation (and rotation), however on its own, this mechanism is far from secure. Users inherently choose bad passwords; and depending on where security sits in an individual company's goals, selecting a password may not always be a trivial process.

A Strong Password:

1. should be a minimum of 10 characters in length.
2. should not be words found in the dictionary, derivatives of user IDs, and common character sequences like QWERTY.
3. should not be made from personal details such as a spouse or pet's name, licence plate numbers, or birthdays.
4. should never be any part of speech; proper names, geographical locations, common acronyms, or slang terms.

Figure 2: *Standard password policy restrictions*

Moreover, because technology changes and new attacks develop, policies must be under continual evaluation. Some examples of strengthening the standard password policy are outlined in figure 3. This goes a long way to help strengthen passwords against hackers who would try common password cracking attempts such as dictionary attacks; in which every word in the dictionary is tried, followed by the dictionary again in mixed case, then with numbers thrown in at random places in each word (including now common SMS talk such as ijust8).

All user chosen passwords must contain:

1. one or more alphabetic characters (with at least one upper- and lower-case)
2. one or more non-alphabetic characters (including special characters like punctuation).

Figure 3: *Password Policy Extensions*

Passwords must also be changed on a regular basis. The regular rotation of passwords is just as important for all users of the system, proven by incidents described in *The Cukoo's Egg* where a hacker returned to an account he cracked three months prior to find the same password was still active (Stoll, 1989). A common counterpart to this clause is the prohibition of password reuse. On multi-user machines, software can be installed to maintain an encrypted history of previously used passwords for each user, preventing a user from reusing an old password. This mechanism prevents any further loss of integrity if an account has been covertly compromised in the past, and aims to prevent any hacker who steals the current (encrypted) password list from cracking it in time for it to be advantageous.

This section has shown that when it comes to people, technical controls are needed to ensure trust is not violated (Guel, 2001). However, these stringent guidelines may not be particularly practical for an individual company, and therefore must be coupled with good staff training and careful screening of new employees. With this in mind, it is necessary to look with close attention at current security technology, and use each only for their intended purpose, remembering that security is not a product, but an ongoing process (Schneier, 2000).

Conclusion

Security has always been about trade offs; management want to know their computing infrastructure is secure, whilst the users want security mechanisms that are transparent and do not get in the way of their duties. The compromise between protection and productivity will always be a delicate one and security needs will dictate the threshold at which these two requirements meet.

A chain is only as strong as the weakest link, and therefore much focus is placed on the 'people side' of security. The greatest security system in the world – strong cryptography, flawless protocols and secure hardware – is no match for the user who chooses an easily crackable password. To overcome such problems, protection mechanisms can be built into the system, but this is where we must address the trade offs: everyone who tries to offer adequate protection for anything must do it at the loss of something else. For example, corporation may invest their time and money protecting confidentiality, but this solution may limit availability, thereby hindering willingness to use the system which has an adverse effect on the company.

This paper has discussed the need for the implementation of policies, and provided examples of important policy content. The main problem with security infrastructure is that it focuses on achieving a particular security goal such as protecting integrity but a system-wide security focus requires more than one form of security. To solve this problem one or more policies need to be implemented, applied, and coupled with the appropriate technology. However this is not without considering that trade offs (whether large or small, seen or unseen) play a significant role in making all decisions to protect the stated security goals.



References

- Guel, M. D. (2001). A short primer for developing security policies. [Online], The SANS Institute, site viewed 23/08/04, http://www.sans.org/resources/policies/Policy_Primer.pdf.
- Panko, R. R. (2004). *Corporate Computer and Network Security*. New Jersey, Pearson Education, Inc.
- Pfleeger, C. P. (1997). *Security in Computing*. New Jersey, Prentice-Hall, Inc.
- Schneier, B. (2000). *Secrets & Lies: Digital Security in a Networked World*. New York, Wiley Computer Publishing.
- Schneier, B. (2003). *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York, Copernicus Books.
- Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*, Doubleday.