Why to implement security in Home Environment

Teppo Jalava
Helsinki University of Technology
Teppo.Jalava@hut.fi

Abstract

The homes connected to the Internet are getting more and more common these days. At the same time the Internet related crime has increased and it has become clear that no one using the Internet is left uninvolved with these issues. The protection of the home environments is essential to assure the confidentiality, integrity and availability of the data and the services these environments provide. But when concerning the home users, that are themselves responsible for the security implementations, the amount of effort and financial resources to actually implement the security is not infinite, far from it. Hence, the big question concerning the security in home environments becomes *"how much security is enough"* and *"how much will it cost"*.

1 Introduction

In the past ten years or so we have seen the rise of the homes connected to the Internet. The Net is no longer a priviledge of companies and organizations, almost every PC used at home is also to be connected to the Internet, by modems, ISDN, cable modems, ADSL etc.

And while computers become more and more common, their prices come down and their technologies grow old at ever increasing rate, families realize that they would have use for, and they also could afford more machines than just one. And to get all the computers at home connected to the Internet, the natural thing to do is to join them together in a residential Home Environment.

The existence of these home environments, in connection with already very common high-speed, always-connected Internet accesses brings a new class of security concerns to be solved. Unlike a big, wealthy company, a private home user lacks the money and motivation to invest very much in the security of his home environment. But there's clearly a need for some degree of security, as this paper is going to discuss.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

2 Home Environments

2.1 The Definition

The definition of Home Environments has two slightly distinct meanings. In some cases it refers to an environment that provides services to the user. For example in the context of the third generation mobile phone standard UMTS, Home Environment, or more precisely Virtual Home Environment stands for the centralized point for the users to access to the services they're subscribed to. In the other context, the concept of Home Environment refers to a networked home, with few computers, some other network devices and possibly some electronical appliances connected together and to the Internet in a sense of a computer network. For example there could be a few machines forming a local area network by themselves and sharing a common gateway to the Internet. The environment provides services to the members of the family and maybe a way to use these services from outside, via a network connection or maybe by a mobile phone.

The main distinction between these definitions is that the latter network is implemented and administrated privately by the users at home, while the former is taken care of by the Service Provider.

This paper concentrates on the latter of the two meanings, concidering the implementation of security for a residential local area network, the costs and the effort needed to implement a robust protection for such environment.

3 Security in Home Environments

3.1 How important it is to maintain the security?

How important the security is to a common home user? After all, most of us aren't storing any trade secrets or other extremely classified, and thus interesting material on our home networks. Why should any cracker be interested in breaking in to my system when there are hundreds of thousands more fascinating and valuable places to go.

But it's not that simple. Every user connecting his home environment to the Internet is vulnerable, even the ones still using the telephone lines and a modem. The net is full of malicious hackers and crackers, viruses, trojans, script kiddies etc. that constantly scan the networks to find an unprotected machine to exploit. It doesn't matter that there's no important or interesting documents stored on the machine, the exploiter could search the machine for any kind of confidential information, such as stored passwords, credit card numbers saved in the cache of the web browser or email addresses. Or he could use the home environment to launch new attacks against other systems, either to cover his tracks, or to use the computing power and the network resources of the compromised system while sporting a massive distributed DOS attack against some major Internet service. Also some viruses, like Nimda and Code Red effectively use the infected machines and their network connections to spread and infect even more machines. The intruder could also use the cracked-in home machine to store and distribute illegal material or just delete data from the machine, for fun. As Jay Beale, one of the developers of Bastille Linux says in an

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

article at Newsforge.com: *"They're not coming after us because we're interesting, they're coming after us because we're vulnerable."* [4]

All the data processed in secure and usable computer systems have three basic qualities, confidentiality, integrity and availability. [2] Protecting the personal information from disclosure or destruction is a matter of fact in an everyday life, as it is in networked computer environments. And what value has the data, if the authorized users can't access it? The availability needs to be considered as importantly as the other two qualities of the data.

Confidentiality

To maintain the confidentiality of the home environment means that all unauthorized access to personal information stored in the system is denied and the data is well protected. In addition, the data that is been moved in and out of the home environment, or within it should be protected as well. There's an analogy to this from the "real" world: people send their letters closed in envelopes when using the traditional posting services to maintain the confidentiality of their messages. [11] Why should they act differently in the information networks, where the messages are now traveling by email?

Just concentrating in securing the home environment from the threats coming from outside is not necessarily enough. A home environment could consist of multiple computers, one for each family member, for example. Such network could provide to an unauthorized user an access to the system. A guest of the house could accidentally see some confidential information, like company documents stored in the home environment for working purposes. Then there is always a possibility of a plain and simple theft of the computer, which evidently compromises all the data stored in it.

Integrity

The integrity of the data is crucial to the whole information technology. The whole society is dependent on different databases, like population registers, bank accounts, train schedules etc. and should they get corrupted, the whole system could fall.

The integrity of data is easily compromised after a successful intrusion to a computer, it can be altered while in transfer to another system or it can be damaged when the media device storing it fails, e.g. hard disks in computers are vulnerable to power failures.

Availability

Attacks against the availability have been reported a lot in the newspapers in last few years. The notorious Denial of Service-attacks (DOS) have lately brought many big services to their knees, causing big damages as lost revenues. The DOS-attacks, or Distributed DOS-attacks implemented in those cases need a little more planning and preparation, but to launch a minor scale DOS-attack doesn't ask for money or brains, even a ten years old computer "geek" could succeed in it. And unfortunately, these attacks can bring a badly configured home environment down. [6]

Other security compromises, such as unauthorized use of the computer, hardware failures, power outages etc. can also cause the system to become unavailable. Some computer viruses, like Nimda and Code Red can also consume so much computer resources and network bandwidth that the system becomes unusable.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

Security concerns

Connecting the home environment to the Internet or enabling the access to it from outside can have different applications. A person could use the home environment for work and needs the access to the company network from home, while some other connects home to access his email and phonebook from all over the world. The home environment could be integrated to other electronic equipment at home and the person can control the air-conditioning, VCR or his sauna remotely, by mobile phone or computer. All these possibilities of accessing the system brings new threats to security that need to be carefully considered and evaluated before they are actually implemented.

3.2 What can happen if the security is compromised?

The consequences of an attack varies from a minor annoyance, like congested network to a serious disclosure or loss of confidential information, total denial of services or even some physical damage to the environment. Not even the poorest, amateur-like attempt to break the security should be taken too lightly, since it could only be a prelude to something bigger and more damaging attack.

Usually the attacks reported in the newspapers concern big companies that provide services to the Internet. The attacks are executed by taking advantage of security holes in these services or by abusing the fact that in order to provide any services at all, the level of security must be lowered. It would seem that these threats weren't a big concern in a common home environment where there are no public services. But that is not the whole picture. A mandatory requirement for a remote access to the home environment is that there is a way through the defense. While it may not be publicly open and only authorized persons know how to pass it, it is still a hole in security and there's a good chance that someone, someday will try to break through it and compromise the system.

Maybe the clearest and most commonly understood consequence of a succeeded break into the home environment is the disclosure of the confidential material on the target machine. In addition as there are usually no protection inside the home environment, other machines and devices connected to the target machine are also in great risk. Whatever data a computer user at home can store on the machine, email adresses, phone numbers, password, even the codes to access the on-line banking system, they're all available to the data burglar to take advantage of. Besides, as the modern operating systems and computer programs are so eager to store often used information in all kinds of caches and proxies, the computer could be full of stored credit card numbers and passwords just waiting to be found.

Usually a successful attack against a public service provider or organization costs them a lot of money in data losses, system updates and the extra work expenses. For example in the TCB-case, the first major legal action against a cracker in Finland, the University of Helsinki, one of the victims in the case, claimed for 326 000 mk (55 000 €) remedy. [3] The reason why this could concern a private home user is that these kinds of attacks can be launched from a compromised home environment. The attacker could be clearing his tracks by using a low-protected private computer, where usually no audition takes place. The attacker could also be using the resources of the home environment to launch a distributed DOS attack. And, in the worst case, the innocent user could get into a lot of trouble, should his machine be compromised and used for such an attack. After all, the attack seems to be

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

coming from the user's home environment, and if the attacker hasn't left any evidence that prooves otherwise, the user could be held responsible for the attack. There are also certain circumstances where the user is expected to take the security very seriously. For example processing of company confidential data at home could be vulnerable to prosecution if the necessary security concerns are not taken into account. [9]

The Denial of Service -attack (DOS), besides its affect on the availability of the system, could also mean a financial loss. Some Internet Service Providers that provide the connection to the home environment, charge according to the amount of data moved to and from the client. The DOS-attack can cause big amounts of network traffic and so, even if your system is not otherwise affected by the attack, it could show in the expenses of the internet connection.

Same affect on the bandwidth usage can occur if a misconfigured or otherwise poorly protected home environment enables someone to install an FTP-server to the system and use it distribute files across the Internet. [10] In addition the unsuspecting user could be prosecuted for distributing illegal or copyrighted material.

There are also threats to the home environments that don't concern the access to the Internet, but that should still be taken into account when securing the home environments. These include power outages, hard disk failures, hardware malfunctions and a physical theft of the equipment. [2] Securing the home environment against these risks is also very crucial, but often overlooked as not so important part of the security.

The home environment can be integrated with some common electronic devices and this enables a centralized point of control to all the home equipment, VCR, television, refrigerator, freezer, sauna etc. The idea of remotely controlling your sauna or VCR, or checking the contents of your fridge is sounds great, but it also reveals a whole new category of security threats in home environment. Unauthorized control of your sauna may not necessarily burn down your house, but surely shows on your electricity bill.

The access to the home environment could also be made possible by phone. It could even be the only connecting path. So, is it a safer configuration than the conventional access from the Internet? Not necessarily. As easily as the crackers scan IP adresses, they can call through phone numbers, and when they get an answer, they've got no problems in breaking into to the system, if no countermeasures are taken.

4 The costs of implementing and maintaining the security

It is clear that home environments should be protected against all kinds of threats, but the big question is "how much will it cost?" Big companies spend millions to protect their environments and still they are successfully attacked every other day. How could a low budgeted home user even imagine of implementing a bullet-proof protection against the big bad world.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

4.1 How much time, effort and money users are ready to invest in home security

Basically, all the information stored on the home machine has some kind of value. The value of the bookmarks in the user's web browser may be difficult to measure, but the user has spent hours gathering them, and will spend even more, should they get lost. An interim report the user has brought home from work to read through a day before the publication could be worth a fortune in the stock markets. Evaluating the value of data, how much did it cost to create and how much will it cost if its lost or exposed is important when the implementation of security means is planned. These evaluations need to be compared to costs of the security implementations and if the cost of installing the security is greater than the value of the data protected, it may not make sense to implement the protection. There is also a third dimension to this analysis, availability. Usually, the security of the system is inversely proportional to the usability of the system [8] and taking this into account may dramatically increase the costs of a secure home environment. After all, the cheapest and easiest way to protect yourself is to not allow any access from anywhere to the system. But then again, how usable would the system be then?

When measuring the total cost of some security implementation there's many aspects that affect the final cost. Not only the hardware and software are those that cause expenses, the installation, learning to use the system and solving problems. Everything costs something, not necessarily money, but man hours and a lot of coffee, for example. Somehow there has to be a way to measure these expenses as well to get the big picture of what the security implementation will cost. There is a fundamental difference in terms of currency when comparing the costs of buying a hardware firewall/router or configuring a single Linux box to do the same, but the overall expenses, when taking into account all the sleepless nights and the uncertainty of a really effective configuration may turn the whole situation upside down.

How much is enough then? When does a user know that he has spent the necessary amount of time, money and effort and his home environment is now as secure as it needs to be? Well, there's no absolute answer to the question, instead it is heavily dependent on the balance of the three aspects, security, usability and cost. And this balance is not static, it can shift rapidly when the circumstances change. For example, a new application is deployed in the home environment or there's a serious security hole found in the security implementation. Therefor the requirements and implementations of the security need to be reanalyzed from time to time to keep them up to date. [5]

A useful guideline to follow when analyzing the costs of implementing the security is called the Mayfield's Paradox. [8] The paradox states that *"to keep everyone out of an information system requires an infinite amount of money, and to get everyone on to an information system also requires infinite money, while costs between these extremes are relatively low."* It is proposed by professor Ross Mayfield and there are some mathematical proofs that it stands. Fig. 1 depicts the paradox with the costs of the security presented on the vertical axis and the percentage of humanity access on the horizontal.

In other words, it is impossible to deny access to the system from all of the humanity, regardless of the resources available. And it is also impossible to grant access to everyone, no matter how much money you possess. This makes it easier to understand that instead

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

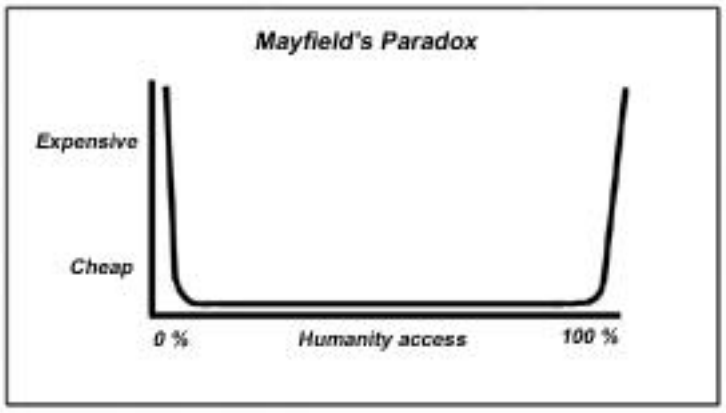

Figure 1: A depiction of Mayfield's Paradox
[8]

of concentrating on a question of *"how to keep everyone out of my system"* when implementing the security, the real question should be *"how to keep most of the humanity out of my system"*. There is a big difference, and with a little exaggeration it could be a choice between building a ferro-concrete bunker surrounded by armed guards around your server room and changing the line "ACCEPT" to "REJECT" in your firewall configurations file.

To answer the question *"how much time, effort and money to invest"* we can start by defining the amount of money needed. The baseline could be that the implementation of the security shouldn't cost more that the value of the data protected and the possible costs that a compromised system could bring. Also the time aspect can be associated with the financial costs, since everybody is able to measure the value of the time spent on implementing the security. The effort is balancing between too little and too much. Too little leads to a badly implemented security, which can be even more dangerous that no security at all, it can create a false illusion of total security, which makes people to act more carelessly and leave the system much more valuable to the attacker, with unprotected passwords, documents, unrestricted gateways to protected enviroments etc. And too much effort can be ineffectual, trying to secure something that already is secure enough can mean a loss of resources and money.

In the real life, the price of security that people are ready to pay for their home environment can't be very high. The costs of a home network are relatively low, so paying thousands of euros for protecting it would seem a bit exaggerated. Most of the users also are more interested in using the home environment than to configure it, so the time and effort spent on implementing the security remain low. But this trend could be changing soon. The homes are getting increasingly connected to the Internet and new applications for a home environments are created all the time, while the news tell us more and more of new Internet related crimes, viruses etc. People are getting more conscience of the threats of the Internet and concerned of the security of their homes. So maybe the amount of resources they are ready to invest for their security is about to increase in the near future.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

4.2 The costs

The actual costs of implementing security in home environment is strongly dependent on how big part of the implementation the user is planning to do himself. Building the security infrastructure from scratch can be a big operation that can consume a lot of time and money if it's done without proper knowledge of security and implementations fulfilling the requirements. Using the services available at the market the user can have a functional and safe security system up and running in no time, but the user has to be ready to pay for this kind of luxury. On the other hand, there are also many freeware or low priced solutions for security, but they very often lack the valuable user support. Of course, nowadays almost every kind of information is available in the World Wide Web, but accessing it needs patience and time, and the question of weather it is wise to trust the instructions got from some unknown authority when implementing the security is indeed very important.

Taking as an example a simple implementation of a firewall between the home environment of the user and the Internet. Basically, there's three options the user can choose from. Installing and configuring a software firewall, buying a hardware one or buying a firewall service from the Internet Service Provider, should it be available.

For less demanding environments, a workstation based software firewall could do the trick. They are pretty simple applications that run on a workstation and monitor all the network traffic on that machine, possibly denying all unwanted connections. Their prices range from free to a few dozens of euros and they're usually easy to configure and use. They serve good when protecting a single, personal workstation, but for protecting the whole home environment from the threats of the Internet, they could prove to be a bit clumsy.

Assuming that the security level to be implemented requires a heavier protection than what is provided by cheap software firewalls available for a workstation computer, a quite good choice is to install a dedicated machine to act as a firewall. What it requires is a spare computer. Even an old one is suitable for this task and those are usually quite cheap to achieve. As of the firewall software, Linux operating system has the functionality of firewall built into it and it is free, so it is a good choice. The problem in this scenario is the amount of work and knowledge needed to install and configure the firewall to meet the requirements of the home environment. In fact, a misconfiguration could lead to a serious security threat that can be very hard to track.

Buying a hardware firewall saves the user from a lot of configuration. The only task left is to set up the settings to the firewall, there's no need to install anything. These firewalls are also usually small in size so they should be easy to hide into the closet, for example. Some level of knowledge of a security systems is still needed though, and the price for this scenario ranges from 500 € to 1500 € and up. [7]

The third option requires no knowledge of computer security from the user. The firewall is configures and maintained by a service provider, usually the same company that provides the Internet access. The user states what services he will need and the provider limits the access to the user's environment following these guidelines. The price of this service varies from a provider to another, but the costs for a home user shouldn't be more than a maximum of ten euros a month.

The drawback in the outsourced security is the lack of control of the security implementa-

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

tion. It could be compared to giving some authority a permission to control what kinds of mail a person is allowed to receive. And how can the user be sure that the protection he's paying for is adequate for the needs of the home environment. The service may block an access to some service, while it lacks the protection against some newly discovered vulnerability. To change the configuration can also be an unconvenient task, including queuing on the customer service phone line and fighting through the bureacracy of the company. These annoyances may give a big advantage to the fact that the old 486 PC gathering dust in the corner of the room is perfectly suitable to act as an firewall between the home environment and the Internet.

5 Responsibilities of securing home environments

So who should be held responsible of implementing the security to the home environment? It would seem obvious that the user is the one who has to take care of security of the system, but that is not the whole picture.

The Internet Service Provider (ISP) is mainly in charge of the security of the system that connects home environments to the Internet. The responsibilities of ISP range from securing the traffic inside its networks to providing secure gateways for accessing the networks outside. For example, in cable modem networks, the users living in same area, or on the same apartment building basically share a common network segment. The messages sent from one machine are basically readable by all the other machines in the segment, much like in the LAN-based networks. This kind of unconfidentiality can be avoided if the ISP enforces the use of cable modems that encrypt the traffic. [1] It should be clear that no home environment can be considered safe if the ISP can't be trusted.

Another possible party interested in security of the home environment is the employer of the user, if the user is to be doing work from the home. Protecting the company confidential material processed by the user at home should be a high concern in the company security policy and it would be wise if the company offered some financial and technical support in the security implementations conducted at home.

6 Conclusions

The generalization of the home environments connected to the Internet and the ever increasing amount of crackers who try to take advantage of them should state clearly that the security implementations are essential in home environments. But these implementations can't cost very much, since it would be nearly impossible to convince the home users to spend thousands of euros on the security, particularly when they don't even fully realize the threats they're faced with.

When implementing the security to the home environment, an analysis of the security needs should be taken, for example what is the value of the data inside the home environment, what kinds of losses can a succesful attack against the home environment cause, not only financially but also in terms of the time, effort and personal annoyance.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

The actual security implementations should be scaled so that no more time, effort and money is spent that is enough to meet the analysis. But it is good to take notice, that when implementing the security, less money often means more time and more personal effor.

References

[1] Anon., DOCSIS 1.0, Baseline Privacy Interface Specification, SCTE [referred to 26. February 2002], <http://www.scte.org/standards/pdf/webdocs/SP-BPI-C01-011119.pdf>

[2] Anon., Home Networks, CERT Coordination Center: Carnegie Mellon University, 2001 [referred to 24. February 2002], <http://www.cert.org/tech_tips/home_networks.html>

[3] Aarnio, E., TCB-tuomio luo suuntaviivat oikeuskäytännölle, Digitoday, 5. February 2001 [referred to 25.3.2002], <http://www.digitoday.fi/digi98fi.nsf/pub/md20010205145631_pka_38387731>

[4] Gasperson, T., Out of the box, Linux is 'dreadfully insecure', The Register, 31. January 2002 [referred to 24. February 2002], <http://www.theregister.co.uk/content/55/23901.html>

[5] Hernandez, E. D., Network Security Policy - A Manager's Perspective, SANS Institute, 22. November 2000 [referred to 24. February 2002], <http://rr.sans.org/policy/netsec_policy.php>

[6] Houle, K. J., Weaver, G. M., Trends in Denial of Service Attack Technology, CERT Coordination Center: Carnegie Mellon University, 2001 [referred to 26. February 2002], <http://www.cert.org/archive/pdf/DoS_trends.pdf>

[7] Hämäläinen, P., Pientoimiston palomuurit, Tietokone, 2001, Nro. 9

[8] Johnson, J. A., The Cost of Security: Mayfield's Paradox, SANS Institute, 21. November 2000 [referred to 24. February 2002], <http://rr.sans.org/start/paradox.php>

[9] Pounder, C., Homeworking: No Longer And Easy Option?, Computers & Security, 1998, vol. 17

[10] Ryder, J., Castles Built on Sand: Why Software is Insecure, SecurityFocus Online, updated 30. January 2002 [referred to 24. February 2002], <http://online.securityfocus.com/infocus/1541>

[11] Zimmerman, P., Why do you need PGP?, [referred to 27. February 2002] <http://www.no.pgpi.org/doc/whypgp/en/>