홈네트워킹을 위한 보안 대책에 관한 연구

김정태* 류대현, 허창우
목원대학교, 한세대학교, 목원대학교

A Study on the Security Requirements for Home Network Application

Jung-Tae Kim, Dae-Hyun Ryu, Chang-Woo Hur
Mokwon University, Hansei University, Mokwon University
E-mail : jtkim5068@hanmail.net

요 약

인터넷을 이용한 정보가 모든 정보 전달의 기본이 되고 있다. 따라서 이러한 정보 전달의 보호를 위한 정보보호 산업이 급성장하게 되었다. 다라서, 본 논문에서는 향우, 2007년 경에 IPV6를 기반으로 하는 유비쿼터스 환경 하에서의 각 가정의 홈 네트워크를 구성할 때 필요한 보안적인 측면의 방법에 대해서 제시하고자 한다. 이러한 다양화된 디지털 매체가 디지털 가전, 정보통신 시스템과 접속하여 새로운 메카니즘의 보안 설계 대상이 필요하게 됨에 따라서, 새로운 정보보호의 접근이 필수적이다. 본 논문에서 제시하고자 하는 내용은 암호학적으로 안전한 홈네트워크의 구성과 이를 실현하기 위해서 요구되어지는 다양한 고려사항등을 분석하여 차세대의 멀티 컴퓨팅 환경 하에서의 정보보호 시스템 구축에 이해를 돕고자 한다.

I. Introdution

First, there was a single personal computer in as few homes with no connection to the outside world. Now, we have computers in most homes and most have internet connections toe outside world. The next step, already happening, is not one computer but rather a large network of sevices in a home. Some of these are mobile devices, which will be brought into the home guest, friends, hired employees, maintenance personnel employed by service providers, and pther strangers. As these changes happen, the security needs of the home user also change. In the days of the disconnected single PC, the primary security threat was from virus contamination on floppy disks. With continuous connectivity to the Internet, many new attack channels have been opened, while floppies have all but disappeared, closing that older channel. To the extent that these existing threats are understood, there are products available to help users defined hemselves against them However, the future home will have not one computer connected to the Internet but rather a network of many devices within the home, and that network might be connected to the Internet. In such environment, the potential for attacks is greatly increased. Since this is still in the future, there are no products to counter thsese attacks. We briefly address the present state of affairs regarding the security of home computers. In this paper, we discusses the new home environment, in which there are theats not only from outside but also from inside. Those threats are characterized, and security mechani는 that can be built into products to secure the home user against these threats are described.

II. Securing the existing home network

Any home computer connected to the Internet is in danger of being attacked. A broadband connection leads to probes preparatory to an attacks every few minutes. A sial-up connection, behind the firewall of an Internet Service Provider, leads to attacks from machines that are behind with one ISP, probes came once or twice week. There exist many papers, both

academic and practical, on how to use existing products to secure current home computers from attacks via the Internet. It is not the purpose of this paper to reterate that advice, but to summarize it.

1. Computers owners should have a firewall and allow no responses to any attempts to connect into the home from outside. A Firewall must have external administration disabled, and any passwords with which it was shipped need to be changed to very secure, hard to guess, passwords. These passwords can be written down, because they are defending against network attackets rathe than in-home attackers.
2. A computer should have a modern virus scanner, which is enabled to scan all inputs to the computer, as well as automatic updating of virus signature files, at least daily.
3. Computer owners should update operating systems and applications with the least security patches and scan for new patches daily.
4. Security setting should be sent to maximum on the both browsers and e-mail agents
5. If one uses wireless networking at home, the wireless access point must be placed outside the home firewall, rather than inside
6. For each operating system, there are numerous setting that must be properly to maximize security

III. Elements of Security

It is a popular misconception that "security" is synonymous with "encryption:, In many cases, confidentiality via encryption is that least important element of a security solution. Network security involves a number of different elements.

1. data origin authentication
2. command authorization
3. message integrity protection
4. message replay prevention
5. data confidentiality
6. key distribution
7. trust versus trustworthiness

IV. Home Network Security Requirements

The requirements for security in a home network depend on how "home" is defined. It also depends on what is envisioned as the network within that home If the network is just a link from a cable moderm to a single PC, then one length of networkcable would accomplish all the network security that the homeowner needs. However, we think ahead to a time in the not-too-distant future when a home contains dozens, if not hundreds of networked devices, some belonging to the entire household and some belonging to individuals within the home. We summarize the security definitions of the previous section in two categories: authorization and confidentiality. For each device in the home network, we need to concern ourselves with two questions:

1. Authorization: Which things are authorized to do what actions or access what data on each device.
2. Confidentiality: Which thins are allowed to read the messages being transferred to a given device from somewhere else?

V. Key Distribution Mechanism

It is not possible to say that one element of a security solution is more important than another, with the implication that you can do just the important parts. Doing 80% of a security solution is like closing 80% of a submarine's hatches and diving. That said, key distribuion is the first and arguably the most important part of a security solution. Included under the term "key distribution" are the following:

1. passwords
2. DES, AES or WEP kwys
3. PKI

VI. Authorization Mechanism

Once a key for a given device or component or user has been learned, that entity can be authenticated, but a security decision cannot be made based onlyon authentication. A device must how what each authenticated entity is allowed to do. Devices cannot be manufactured with that knowledge built in, so it is the job of the device owner to implant that information. There are many mechanism available for this, but the three predominant ones are an Access Control List(ACL), an authorization server, and an authororization certificate.

6.1 Access Control List

An ACL is a proteded table residing in memory in the same device as the resource whose access is being protected. It is an array of entities, and each entry contains th following:

1. subject: an identifier of the entity being granted access
2. authorization: an indicator pf the rights being granted that subject
3. delegation: a flag, indicating where the subject may futher delegated these rights
4. validity: optional conditions on validity of the entry such as a "not-after" data and time

Some ACL entries contain fewer than all four of these fields, but these are enough to cover any home network authorization decision we have encountered. A device can control access by an ACL alone. This makes programming easier and also allows an access entry to be deleted with ease, assuming one can access the deviceholding the ACL. It has the disadvantage of requiring a great deal of ACL editing if there are a large number of ACLs or a large number of subjects. It also could require a large amount of ACL storage. Since ACLs must survive power failures, this memory must be non-volatile.

VII. Security Products

The products avalable in 2002 tend to support the hardened perimeter model of security. This is appropriate to most basic concept of home but not to the more complex forms of home environment. These products also tend to have been designed based on reqiirements of industry rather than of the home, making their administration difficult and sometimes assuming the existence of both physical security and a group of on-call support professionals. Universal Plug and Play security, describd below, is a new standrad designed for home use, but is too new to have products for sale as of the fall of 2002

7.1 Firealls/Gateways

An Internet gateway or firewall secures an internal network from the Internet, to the extent that it blocks unsolicited traffic from the outside. As long a there is a single security domain inside the home, the home can be secured by a single firewall. However, if there is more than on security domain inside the home then a single firewall would not help guard the interests of one internal security domain from other internal nodes. One might create a separate wired network for each security domain and give each of those networks its own firewall. However, that solution gets expensive as the number of domains increases. Even in homes in which there are multiple security domains whose securityis defined through mechani는 other than firewalls, one will probably wnat a firewall to protect the collection of domains from hostile outside entities.

7.2 Wireless Security

Wireless networking is becoming popular at home. It relieves the homeowner of the work of running network wires through and within finished walls. It can also reduce the clusterof wires within a room. However, ith this benefit comes a security drawback. By relieving the homeowner of the work of individually running network wires to each device in the home, wireless networking prevents the homeowner from selecting which devices should connect to a given network as might be accomplished by running wires. Instead, with wireless networks, cryptographic keys need to be used to individually choose which devices should be connected to a network. Devices allowed onto a network would be given the key to use that network. The choise of wide area coverage networking, as with wireless or power-line networking, might also restrict the numberof networks the homeowner could define. With individual wires, the homeowner can set up separate networks for only the cost of some hubs and wires. With 802.11, each separate network would required a separate access pint and separate channels. Since there are fewer than seven 802.11 channels that can operate in the same area without getting in each other;s way, this limits the number of networks that can be declared in a small space like a home and implemented by 802.11

7.3 WEP

Wire Equivalent Privacy(WEP) was the original security measure for 802.11. It has been shown to have a flaw in key usage that allows an attacker to recover the key used after usage that allows an attacker to recover the key used after eavesdropping on a few thousand messages. Therefore, for real security, WEP is not useful. It can be an annoyance for a casual attacker, but not for a determined attacker.

VIII. Conclusion

One conclusion of this paper is that with proper security against the insider threats in the home environment, the security of the home network against threats from outside is increased. Securing the home network is not the easy job some people would like to believe. A home network security policy can be much more complex than a corporate security policy. The homeowner would have to implemente via network security policy controls what the corporation implements via door guards. Most network security thinkin to date has assumend that networking access is binary: that one would allow access to the network or not. The idea of controlling access to individual components is relatively new to network security sedign. While we adjust our product design process, this will produce a period of gradually increasing security and there will be a graadually increasing security and there will be a gradually lessening tension between th desire for ubiquitous computing and connectiviti on the one hand and the desire for real security on the other.

References

[1] Ellison, et al., "SPKI Certificates Theory," RFC2693
[2] http://www.upnp.org
[3] http://www.theory.lcs.mit.edu/~cis
[4] http://world.std.com/~cme