integrity, much like a tripwire, so that unauthorized changes cannot occur (or are at least extremely unlikely to occur). We may no longer be able to afford the luxury of having firewalls placed at a fixed point in a network's infrastructure.

Firewalls of the future may need to become more like network agents, capable of distributing themselves where they are needed (and in all likelihood moving themselves when they are attacked). These firewalls should be able to govern not only traffic originating from outside the network in which they are located, but also traffic originating from within. Finally, firewalls must make the process of reading and analyzing logged data less cumbersome.

Conclusion

Despite numerous limitations, firewalls are a strong network security control measure. The proverbial smokescreen surrounding the firewalls arena is unfortunately very occlusive, so those who employ firewalls or who consider employing firewalls must learn what these devices can and cannot do. Learning what they cannot do is at least as important as learning what they can do. The proverbial smokescreen now needs to dissipate — to clear the misconceptions about firewalls that serve as an obstacle to gaining the maximum benefit from them and to establishing effective network security practices.

References

1. Cheswick, W.R. and Bellovin, S.M., 1994. *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley, Reading.

2. Ranum, M.J., 1995. How Not to Build a Firewall. *Computer Security Journal, Vol. 11 (1), 1995, pp. 1-10.*

3. Rogers, R., 1995. Posting on com.security.unix, August 12, 1995. (Cited with Mr Rogers' permission.)

4. Schultz, E.E., 1995. The State of the Hack. Paper presented at 25th International Information Integrity Institute Forum, Brussels, Belgium, June 1995.

5. Schultz, E.E. and Longstaff, T.A., 1995. Internet Sniffer Attacks. In Proceedings of the 18th National Computer Security Conference, 1995.

6. Trowbridge, D., 1995. Firewalls Frustrate Vandals Seeking to Break In. *Computer Technology Review*, Vol. 15 (7), 1995, pp. 1, 6, 8.

This paper was presented by Dr Schultz at Compsec '95 International the 12th World Conference on Computer Security, Audit and Control, Queen Elizabeth II Conference Centre, Westminster, London, UK, 25-27 October 1995.

Physical Layer Network Security: What your LAN can do for you

D.W. Banes

The basic simplicity and ease of use of Local Area Networks (LANs) has produced an explosive growth in connectivity over the past few years so that today they have become an integral part of most business organizations. This growth has been in spite of some fundamental problems that the technology highlights in the area of security. However, these issues have almost been totally ignored in the past mainly because of a lack of understanding of the issues rather than complacency.

More reliance is being made on electronic media for our work, word processing, project management and finance all rely heavily on Personal Computers (PCs) and for network file access. A loss at any point, disk failure, network failure etc. can be catastrophic — productivity in a NetWare environment plummets if the network isn't available for even an hour. The PC itself was originally intended for private use but now is increasingly being networked. In many cases little or no procedures are put in place, so much so that a common requirement for network management is simple inventory control. Generally there is little or no understanding of exactly what equipment is present, how it is connected and who it belongs to.

One of the factors that is little understood and the main feature that allows LANs to be so simple is also its biggest security flaw. The broadcast nature of LANs means that traffic transmitted on the network must pass by all stations that are connected to the same physical LAN so that the sender has to have no knowledge of the location of the receiver. This is a benefit in that it is precisely for this reason that LAN's have been so easy to install and use but the consequences are great.

The paper analogy would be to have an internal mail system where all letters are passed to every employee unopened but expect them not to read it. This fact may not have been too much of a problem if it weren't for the fact that one of the requirements for this greater connectivity has resulted in all LAN adapters ability to become promiscuous, that is, actually listen and receive all the traffic that passes by. To compound the problem, you don't even know whether an adapter is listening promiscuously or not.

Promiscuously listening to traffic is fine for administrators using network analyzers but they're public domain packages available that turn a standard 386 into a network analyzer, quite capable of capturing full rate LAN traffic. Your system may be protected by passwords, but many network operating systems pass the password in clear text and even if they aren't, the data that is then accessed generally is not.

With the growth of the PC and network industry, computer literacy has also grown instep. Interviews with virus writers generally site boredom, intrigue and fame as motivations for their endeavours. With the exception of well publicized events such the Internet Worm, these talents have not been turned towards the LAN in just the same way as they reek havoc on the PC itself, but the knowledge and facilities are available.

To compound the problem, now that LANs are nearly commonplace, there is a move for greater connectivity over the WAN so the reach of your networks is even wider. One of the largest growing areas in the industry are Remote Access servers that mimic local network connectivity over a fast serial modem link. With this new technology it isn't even possible to rely on physical containment of your PCs.

Today's network environments

A typical network environment will have:

- Hub-based wiring system, probably twisted pair running probably Ethernet or Token Ring.
- A central server or servers that everyone may connect to.
- Modem access for home working or maintenance purposes.
- There may be unknown equipment on the LAN, for which you know nothing.

The server will be protected by passwords, but will be transmitted to all hosts, not just the server, whether encrypted or not. This still probably isn't safe because in many cases you could capture the packet on the LAN and then replay it back, or you can simply guess the password. Humans are frail, studies show that apparently an algorithm to guess just nine passwords will gain access to the majority of all accounts: your user identification itself, spouses name, child's name etc. Anything much more complicated just detracts from its use, indeed the biggest problem to all security measures are that if they are too complicated, they will fall into disuse.

Threats

You can summarize the threats posed by LANs by categorizing them broadly into three areas:

- Integrity — making sure data is available, without modification.
- Privacy — don't let anyone see data they're not supposed to.
- Masquerade — don't allow anyone to pretend they are someone else.

The obvious and traditional solution to provide confidentiality is to add encryption to all LAN hosts. Although possible it cannot be implemented without cost and penalties in terms of ease of use and administration. However, with the advent of structured wiring environments there are now possibilities to remove the security loophole of broadcast LANs whilst maintaining the ease of use by making the repeaters themselves more secure. In structured wiring environments it is common to have repeaters in the form of hubs, generally in a central wiring closet. Typically this is locked to provide physical security, preventing any unauthorized tampering of the network.

Other features which enhance security are also possible within the hub. By studying the state of the link pulse on twisted pair and fibre networks ensure that a good reliable connection is present. Loss of link pulse could mean either a faulty cable or someone (unauthorized) has tapped into the link. Integrity can also be improved by incorporating standard redundancy features for key components such as power supplies and removing central points of failure with redundant paths between hubs.

Because only a few end stations are connected to the hub in a star wired confidentiality it is also possible by only selectively sending data to end stations whilst maintaining the normal repeater criteria or implementing a bridge or switch in the hub. Switches also allow higher performance for the network as a whole and also provides error containment but not without a cost penalty over a repeater.

The hub can track movement and changes in addresses throughout the network by monitoring addresses of the packets as they are received by the hub. In structured wiring environments this provides a great deal of inventory control and also can assist in the administration of moves adds and changes.

The benefits of implementing security features within the hub or switch are that they are easy to administer — the system works autonomously, only requiring to know who is on which port and doesn't require any onerous tasks such as password key distribution. Also the system is totally non-intrusive, the user is totally unaware that the system is in place but prevents then seeing data they are not meant to, seeing who is talking to whom and prevents an end user capturing packets for replay.

Network management

For your network to be really secure, there must be a corresponding network management procedure that is equally secure. There's little point in having any device that incorporates even the most sophisticated security system if you can switch everything off in a simple telnet session with just a simple password.

The de facto method for the management of network equipment today is the Simple Network Management Protocol (SNMP) proposed by the Internet Engineering Task Force (IETF) in their Request For Comments (RFC) documents. Security was understood to be non-trivial to implement so was treated separately in the original design of the SNMP-management protocol, as it was in the original work of the IEEE in 802.1.

The original security work for the security for SNMP is now a proposed standard and fully documented. Unfortunately, from a security point of view, at the same time as the RFCs for the Secure SNMP were launched a new protocol was proposed that not only addressed the security aspects of SNMP but also some of its other problems, such as its inefficient use of bandwidth for table retrieval. This protocol is known as SNMPv2 and is nearing completion in the IETF working groups.

SNMPv2 uses four techniques to provide secure network management:

- Authenticate — to prove who you are
- Data Integrity — to ensure the data hasn't been changed
- Timestamp all packets — to prevent replay
- Encrypt — to stop sensitive data being seen by anyone

The techniques proposed in both Secure SNMP and SNMPv2 rely on encryption and authentication to achieve their aims. Encryption provides confidentiality so that vital information such as routing information or passwords cannot be seen. Presently the only algorithm proposed is DES although because of export restrictions it has been de-emphasized and the working group has concentrated on administration models that do not require encryption at all. Authentication ensures that not only is the data from who it says it is from, but also that it hasn't been altered in any way and the information is time-stamped to prevent replay.

Conclusion

Local Area Networks have grown in an uncontrollable fashion because of they are so easy to use due to the design of the technology. This growth has produced a security nightmare that is only now being recognized and solutions put in place. The best solutions are undoubtedly ones that are easy to use and administer and are unobtrusive to the user.

Traditional solutions have been based on implementing security solutions in the network operating systems themselves. However, the network devices themselves can add valuable security features that do not degrade network performance, are unobtrusive to the users yet do not prevent the flexibility that have allowed the widespread adoption of LANs. Any security solution must be manageable and this itself leads to security issues that also must be addressed. It is only recently that enhancements to the popular SNMP protocol are now, for the first time addressing the security issue with a new protocol: SNMPv2.

This paper was presented at Compsec '95 International the 12th World Conference on Computer Security, Audit and Control, Queen Elizabeth II Conference Centre, Westminster, London, UK, 25-27 October 1995.