Use of Mathematics in Network Security

Abstract

Security is a vital aspect of any networked system, as the dependency on network infrastructures has grown over the past few decades. With the advent of the internet, security becomes a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur.

The inventor of the internet, when renewed can minimize the probable attacks that can be sent via network. Operating systems, with antivirus and other means. We get so caught up in our media streaming, online shopping, and social networking that we forget that nothing happens on a computer without numbers. Every time we post a kitten video, tweet our political views, and tell the world what we had for breakfast, it all boils down to binary code, the numbers '0' and '1'. Maybe one day they'll figure out how to encrypt email using icons and emails, but for now, we have to surrender to mathematics.

G.K.Patil
Head,
Dept of Mathematics,
A.C.S College, Shankarnagar,
Biloli, Nanded,
Maharashtra, India

Keywords: Internet Security, Personal Computer, Internet Technology, Mathmatical tools And Communication Channel.

Introduction

A computer network is an interconnected collection of devices that facilitate you to store retrieve, and share information the most common of such devices are personal computers (PCs) mini computers, mainframe computers, terminals, workstations, thin clients, printers. Fax machines, papers, and various data storage devices. In modern age some more network connectable devices have come into market. There are interactive Televisions, Videophones, handheld devices, navigational and environmental control systems. Ultimately these devices provide a two way access to big number of things on the global computer network. In this world of internet network is a web of several accessible devices. The business world it gathers analysis, organise and disseminate the information for the purpose of profit. The business network is based upon internet technology many people are still worried about the safety of online transactions.

1. Are internet financial transactions safe?
2. Can email that sent via the internet be monitored by third parties, causing concern about what one puts into emails?
3. Can anything be done about worms, viruses and other "malware" that seem, unfortunately to be as much a part of modern life as catching a cold or the flu?

Mathematics is helping for the become of online transactions. In the previous times mathematical tools were supposed to be inapplicable for security purposes but now these tools are making it all possible. New techniques have emerged in the market for manufacturing faster and sizable have increased it has become just line a cat and mouse game.

What is Networking?

Networking is the use of many computing devices together in order to share resources. Such resources are printers CD'S files or even electronic communications such as e-mails and instant messages. These networks can be prepared using several different methods, such as cabbies telephones lines, satellites radio waves, and infrared becomes.

Network Security

Systems and network technology is a basic technology for variety of application security is very important to network and applications.

Although, network security is a critical requirement in emergency network, there is remarkable lack of security methods that can be implemented. There seen a gap of communication between the developers of security developed process which is based upon the open system interface (OSI) the OSI model has many benefits in designing networks. It offers modularity flexibility ease of use and standardisation on of protocol. Protocol of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustment, allowing flexibility in development. When it comes of network security, it must be maintained that the whole network is secure. The network security not only concerns about security in the computers at each end of the communication chain. But it should plan for communication channel. A possible hacker may target the communication channel, obtain data, decrypt it and re-insert a fails massage. Security the network is just as important as securing and encrypting the massage.

An effective network security plan is developed with understanding of security issues, potential attackers, needed level of security and factors that make a network vulnerable to attack[1]. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavour. To minimise the vulnerability of the computer of the network we can use many product as tools. These tools are network operating system, encryption, authentication mechanisms, security management and firewalls. In business world combination of some of these tools is used. “Internets” are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself.

Benefits of Computer Networking

Cost-Effective Resource Sharing

With the help of net working in business computers we can minimise the expenditure on hardware by sharing components and peripherals. We can also save time with this system.

Streamlined Business Processes

There are several benefits of computer networking within the company between companies and customers. The internal business process can be streamlined with the help of with the help of with the company networks. The day to day tasks such as employee collaboration on projects, Provisioning, and holding meeting can take less time and it is less expenditure.

Powerful, Flexible Collaboration between Companies

When one or more companies are connect with a selected network portion, they can streamline business process that normally occupy inordinate amounts of time and effort.

Improved Customer Relations

Customer relations can be improved by providing good services. The electronic stone front can search of and order products and services over the internet. With this the customers can get and access of shopping at home. This process is time and energy consuming which is very beneficial.

Secure Management of Sensitive Information

This computer networking system has a big benefit of protection network access to resources & fuses with this sensitive data, equipment and other resource can be secured. This control can be exercised over both the employees and people outside your company who access your system over the internet.

Use of Mathematics in Network Security

Boolean Values

In some computers a branch of mathematics called Boolean Algebra is applied. To craft decision and response many languages are used. Python is a favourite Language among the hackers and cyber security systems.

Cryptography

Cryptography is the mostly used mathematical method in network security. Cryptography is just like puzzles where you are supposed to write a given sentence in numbers instead of words. Each number here stands

d for alphabet. Just by eliminating the uses of ‘and’ the ‘ing’ and so on, you can ultimately decipher the whole sentence customers get satisfaction by this method. Hackers and information system analysis use equation that are far more sophisticated and mathematical sentence to encrypt information.

Conclusion

That, it is a truth one must know that network security is in caressingly gaining attention as the internet expands. The security dangers and internet protocol were analysed to enhance the necessary security technology. This security technology is mostly software based but many times common hardware devices are also used.

Security on a network is not something to be taken lightly. In today’s interconnected world, it is essential that you steps to protect your valuable data from all points of attack, both external and internal. Originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used.

Many Network security software's offers many features to help secure the server and the network.

References

Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously, "Computer, vol.31, no.9.

Kak Young, Basic Concepts of computer Networks http://www.slideshare.net/makyong1/basic-concepts-of-networks?related=2

Beutelspacher, A., Cryptology, Mathematical Association of America, Washington, 1994.

Bidgoli, H. (ed.), The Internet Encyclopaedia, John Wiley, Hoboken, 2004

Bidgoli, H. (ed.), The Handbook of Information Security, John Wiley, Hoboken, 2006

Bidgoli, H. (ed.), The Handbook of Computer Networks (to appear).

Cheswick, W. And S. Bellovin, A. Rubin, Firewalls and Internet Security: Repelling the Wily Hacker, 2nd edition. Addison-Wesley, 2003.

Coutinho, S., The Mathematics of Ciphers, A. K. Peters, Natick, 1999.

Davies, D. And W. Price, Security for Computer Networks, John Wiley, Chichester, 1984.

Diffie, W. And M. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, p. 644-654.

Elgamal, T., A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. On Info. Theory, vol. IT-31(1985) 469-472.

Galbraith, S., Elliptic curve public key cryptography, Mathematics Today, 35 (1999) 76-79.

Garfinkel, S. And G. Spafford, Practical Unix and Internet Security. O'Reilly and Associates, Inc.,1996.

Golomb, S., Shift Register Sequences, Holden-Day, San Francisco, 1967.

Hellman, M., An Overview of Public Key Cryptography, IEEE Communications magazine, May 2002, p. 42-49.

Koblitz, N., A Course in Number Theory and Cryptography, Springer-Verlag, New York, 1987.

Koblitz, N., Elliptic curve cryptosystems, Math. Of Comp. 48 (1987) 203-209.

Koblitz, N and A. Menezes, A survey of public-key cryptosystems, 2004 (available on the web.)