International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359

Research Article | December 2012

Intelligent Network Practices and Innovative Networking Solution for Enterprises

Dr. Piyush Gupta
Asst. Prof., Dept. of Computer Science & Engineering
Birla Institute of Technology, Jaipur

Kashinath Chandelkar
Research Scholar, Dept. of Computer Science & Engineering
Birla Institute of Technology, Jaipur

Abstract:

Security is becoming a critical part of organizational information systems. The detection of attacks against computer networks is becoming a harder problem to solve in the field of Network security. Intrusion Detection is an essential mechanism to protect computer systems from many attacks. The success of an intrusion detection system depends on the selection of the appropriate features in detecting the intrusion activity.

The objective of the paper is to search, identify and block an unauthorized access into the organizational networks by any means. Ethernet, WiFi and Thin Client System is considered with probable genetic solutions. A new architecture is proposed to control data packets at different levels to ensure the network security. Devices are placed based on the scale of security and accessibilities supporting multicore network. Being the network is hidden it is difficult to trace any node for attack. Packet Filtering Bridge (PFB) followed by firewall and tool like MRTG (Multi Route Traffics Grapher) enables to trace and block unauthorized data packets, without affecting the Local Area Network (LAN)/Wide Area Network (WAN) architecture.

Keywords: **Multi Route Traffic Grapher, LAN, WAN, PFB.**

I. Introduction

Network Security is the ability to protect a computer system and its resources with respect to confidentiality, integrity, and availability. Various protocols, firewalls are in existence to protect these systems from computer threats. Intrusion is a type of cyber attack that attempts to bypass the security mechanism of a computer system. Such an attacker can be an outsider who attempts to access the system, or an insider who attempts to gain and misuse non-authorized privileges. Intelligent network management is a contribution of both System Administrator and End Terminal Users, which goes as continuous project. Assuming a LAN or WAN with 500 plus terminals and different LANs which include wired connection, wireless connection (WiFi), or any other hot spot system is included in the network.

As a network manager, it is a prime necessity to understand the network configuration thoroughly. Each networking device including Gateway, Router, Switches, LAN cable and Network Interface Card (NIC), plays a vital role in the layered network management. The next job shall be deploying policies as per the designed groups which include students, staff, manager, system administrator, faculties and so on. Client terminals do not be neglected at the same time, as they are the subways through which attack into the network is possible. They basically require application software's installed on the stable operating system, a regular updates for antivirus definition and continuous system maintenance is a must. With a multi core architectural support and assigned security policies at operating system, application software(s), system authentication, data encryption, and routing through NIC card help to trace the unidentified node within the network in a short span of time.

II. Major Network Categories (Ethernet, WiFi & Thin Client Support)

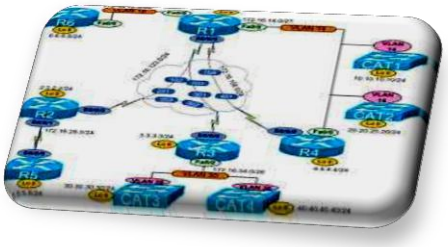


Fig-(Types of Local Area Networks) Source: CISCO Networks

B. Wireless LAN (WiFi)

It works basically with radio waves and with wavelength in electromagnetic spectrum (300 GHZ- 3KHZ and wavelength 1mm
– 100km) that travels with the speed of light. As per the above fig-1, category 2 can be extended for wifi connectivity with proper configuration and security levels in the network. The major issue faced by the administrator is hacking into the network and that can overcome by selecting, enabling, configuring and updating a firewall to its latest. Once done, the router/terminal needs to send the updates to the control system instantly. On the second layer, Media Access Control (MAC) filtering should be enabled on the control system with unique Service Set Identifier (SSID). It is a responsibility of the administrator to setup the WiFi component with enabled Wireless Protected Access (WPA) / WPA2 for better security.

C. Thin Client System

No organization likes to make an old terminal redundant on purchase of new slot, rather they may be utilized to design a thin client (Category 3 in fig-1). The LAN comprises of smart/ dumb terminals connected to the server/control system, which has concerned setup. The user terminal is allowed to boot through LAN, gains a dynamic IP address and an option to select operating system. As an authorized user, the server shares resources with end user for the gained session. Universal Serial Bus (USB) ports and CD-ROM are the targeted loopholes to enter into the network that can be disabled by the administrator by default and data sharing shall be allowed on the control node.

III. Problems faced by Network administrator

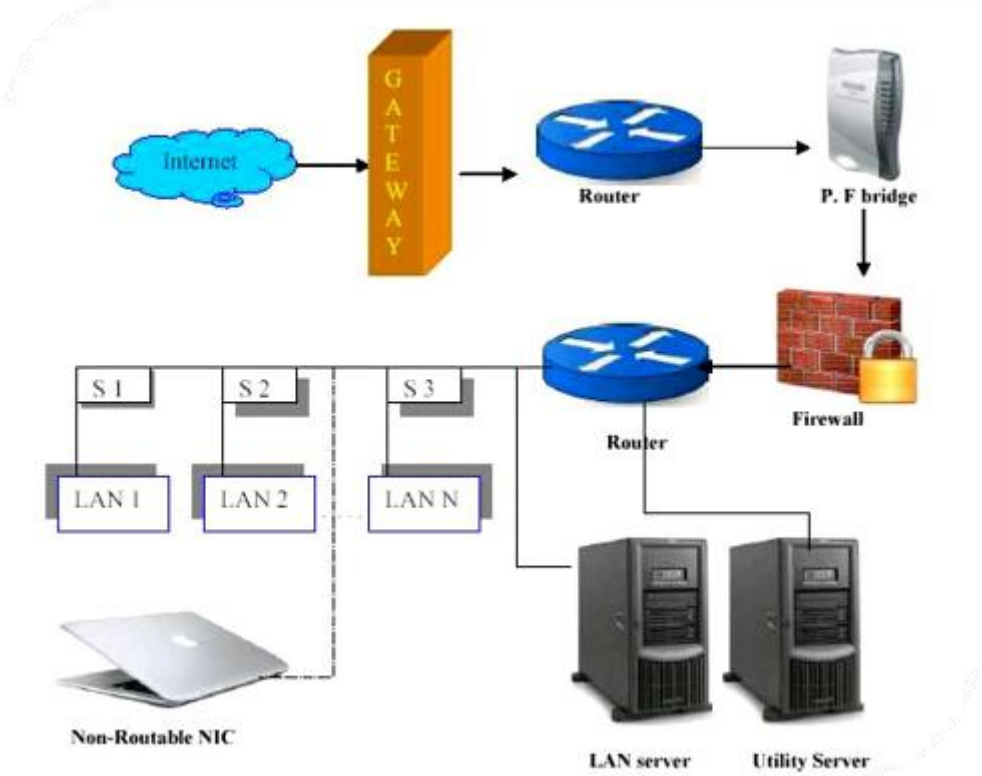
Network administrator is a responsible person to grant and restrict the control of all the possible connected devices within the organizational network and related issues of the broadband security from the gateway onwards. The challenges and threats faced include unauthorized access either from internal terminals, outside intruders and /or viruses through the gateway. Detection of all the threats and denying access on the prompt is the key objective of this paper. Following algorithms/methods are analyzed for node detection and denying the services for unauthorized accesses.

Table –I: Methods/ Algorithms compared for better solution to Network Security

Sr. No	Name of the Method/ Algorithm	Key features	Drawbacks
1	Least Square Method	• Used for identification of open loop system. • Used for structural identification (device used) • Used for parameter identification (tools used)	Noisy data makes the solution unreliable.
2	A Simple Genetic Algorithm for Local Tuning: efficient global optimization technique	• Works on the concept of Natural Evolution. • Uses guided search • Relies on Mutational Changes	Natural Selection and Mutation is time consuming hence will be out of time bound.
3	Gauss Markov Theorem for system identification	• Works with non singular covariance operator	Can be used in finite dimensions only
4	Bellmen Ford Algorithm	• Used in RIP (Routing Information Protocol) • Calculates distance between itself and sends update to each terminal • Calculates shortest path	Changes in network topology is not reflected quickly as updates are spread over the nodes
5	Binary Search Algorithm	• Is faster then linear search algorithm • Mid=(first +last) / 2	Can be only used if the array is sorted.

IV. Conclusion

The proposed solution shall be represented graphically as under:



(Fig-2) Proposed Network Security Solution

The architecture shown in Fig-2 is designed to overcome the drawbacks of the algorithms applied on the network. In the proposed solution, the network is kept hidden. The devices are positioned according to the scale of activities and accessibility. The data packets have to pass through packet filtering bridge followed by firewall. The utility server holds updated antivirus, tool to control network graph like multi route traffic Grapher and sniffing software. LAN server is dedicated for client requirements. A non-routable NIC is available to keep an eye on both the servers and routers, which are difficult to trace. This architecture performs without loss of bandwidth and high-level multicore security with possible needs fulfilled in better way.

REFERENCES

Journal/ Articles

[1] Big Dummy's Guide to the Internet (C) 1993, 1994 by the Electronic Frontier Foundation [EFF]

[2] Jean Armour, Polly Manager of Network Development and User Training NYSERNet, Inc. 111 College Place Syracuse, NY 13244-4100 315/443-4120 FAX: 315/425-7518 jpolly@nysernet.org

[3] Cyber security tips, Texas department of information resources, March 2009, volume 3, issue-2. [4] An intelligent network, the international engineering consortium, at www.iec.org, pages –32.

[5] Design Space and Analysis of Worm Defense Strategies, David Brumley LiHao, Liu Pongsin Poosankam, Dawn Song Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, Pennsylvania dbrumley, lhliu, ppoosank, awnsongg@cmu.edu

[6] A genetic algorithm approach to optimal, topological design of all terminal networks berna dengiz, and fulya altiparmak Department of Industrial Engineering Gazi University, Ankara, TURKEY 06570 Alice e. smith1, Department of Industrial Engineering University of Pittsburgh, Pittsburgh, PA 15261.

[7] Automatically Identifying Trigger-based Behavior in Malware, David Brumley, Cody Hartwig, Zhenkai Liang, James Newsome, Dawn Song, Heng Yin Carnegie Mellon University ,dbrumley, chartwig, zliang, jnewsome, dawnsong, hyin Carnegie Mellon University, 5000 Forbes Avenue Pittsburgh,

[8] Building a More Secure Network, George Rosamond, March 8, 2004 GSEC Practical Requirements (v.1.4b) [9] The changing role of network administrator, By Jim Metzler Ashton, Metzler & associates,
[10] CISCO cloud intelligent network, © 2012 Cisco and/or its affiliates. All rights reserved. (1110R) C45-693143-01 02/12. [11] White paper on networking by Cisco, Next-Generation Networks: Business Value for Today and Tomorrow
[12] A crash course in managing security by Rik Ferrow, the magazine of use nix & sage November 2001 • Volume 26 • Number 7
[13] Emerging cyber threats (report 2009), Georgia tech information security center.
[14] Optimal Traffic Engineering Via Newton's Method, Dahai Xu ,dahaixu@research.att.com , AT&T Labs - Research, New Jersey, USA
[15] Hardware-Assisted Intelligent Network Monitoring and Measurement at 10 Gigabit/s and Beyond, National Aeronautics and Space Administration, Computing Technology (NASA).
[16] Rich, automatically protecting against integer-based vulnerabilities, David Brumley, Tzi-cker Chiueh, Robert Johnson dbrumley@cs.cmu.edu, chiueh@cs.sunysb.edu, rtjohnso@cs.sunysb.edu Huijia Lin, Dawn Song huijia@cs.cornell.edu, dawnsong@ece.cmu.edu.
[17] An Intelligent Search Technique for Solving, Train Scheduling Problems: Simulated Annealing and Constraint Satisfaction M.T. Isaai1, Scientia Iranica, Vol. 14, No. 5, pp 442{449, Sharif University of Technology, October 2007.
[18] Remote Timing Attacks are Practical, David Brumley, Dan Boneh, Carnegie Mellon University Stanford University dbrumley+@cs.cmu.edu dabo@cs.stanford.edu
[19] Vulnerability-Specific Execution Filtering for Exploit Prevention on Commodity Software James Newsome Carnegie Mellon University jnewsome@ece.cmu.edu David Brumley Carnegie Mellon University, dbrumley@cs.cmu.edu Dawn Song Carnegie Mellon University dawnsong@cmu.edu.
[20] Towards Automatic Generation of Vulnerability-Based Signatures, David Brumley, James Newsome, and Dawn Song Carnegie Mellon University Pittsburgh, PA, USA {dbrumley, jnewsome, dawnsong}@cmu.edu Hao Wang and Somesh Jha University of Wisconsin-Madison Madison, WI, USA, hbwang, jha@cs.wisc.edu
[21] Defending against an Internet based Attack on the Physical World, Simon Byers AT&T Labs – Research, New Jersey byers@research.att.com, Aviel D. Rubin, Johns Hopkins University Information Security Institute Baltimore, Maryland rubin@jhu.edu, David Kormann AT&T Labs – Research , New Jersey davek@research.att.com
[22] Sweeper, A Lightweight End-to-End System for Defending Against Fast Worms Joseph Tucek, Shan Lu, Chengdu Huang, Spiros Xanthos Yuanyuan Zhou University of Illinois at Urbana Champaign tucek, shanlu, James Newsome David, Brumley Dawn Song, Carnegie Mellon University.
[23] Virtual Appliances for Deploying and Maintaining Software ,Constantine Sapuntzakis, David Brumley, Ramesh Chandra Nickolai, Zeldovich Jim Chow, Monica S. Lam, Mendel Rosenblum ,Computer Systems Laboratory Stanford University
[24] Applying Genetic Algorithms to Efficiently Locate Mobile Terminals in Personal Communication Networks- Proceeding ICNC '07 Proceedings of the Third International Conference on Natural Computation - Volume 04 Pages 302-306

Books/Chapters

[1] Hackers Beware Eric Cole, Publisher: New Riders Publishing, First Edition August, 13.
[2] E-book on web technologies, pages-169, bookchumps.com
[3] Research methodology, methods and techniques (second edition), new age international publications by C.R. Kothari
[4] Google Hacking for Penetration Testers Using Google as a Security Testing Tool ,Johnny Long, pages-170.
[5] Least square method for system identification.ppt, by Dr. Djamel Bouchaffra, CSE 513, soft computing, 18 slides. [6] The Google Hacker's Guide johnny@ihackstuff.com http://johnny.ihackstuff.com, pages- 32
[7] Dr. Thomas Magedanz IKV++ GmbH , Intelligent Network Evolution - Impact of Internet, CORBA, TINA and Mobile Agent Technologies

Online sources

[1] http://m.zdnet.com/blog/india/how-do-indians-spend-time-on-the-intern.
[2] Hacking and network defense, www. Infowar.com
[3] *Emerging Cyber-threats Predicted for 2011, R. Colin Johnson*, http://www.smartertechnology.com - Smarter Technology Ziff Davis Enterprise Holdings Inc Generated: 31 August, 2012, 06:38. [4] *Network and*

server security, soft layer technologies, soft layer.com
[5] *Cisco Cloud Intelligent Network*: Connect the World of Many Clouds, 2011 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.
[6] http://msisac.cisecurity.org/newsletters/documents/2012-01Template-MSISAC.pdf
[7] http://www.tandfonline.com/doi/pdf/10.1080/00207727008920223 [8] http://www.filehungry.com/
[9] http://en.wikipedia.org/wiki/Brute_force_attack
[10] http://anss.org.au/nss2013/index.htm
[11] http://www.inderscience.com/dev/search/index.php?action=record&rec_id=27299 [12] http://www.threatremove.com/
[13] http://www.smartertechnology.com/c/s/Security/
[14] http://deepblue.lib.umich.edu/bitstream/2027.42/3575/5/bab1192.0001.001.pdf. [15] http://en.wikipedia.org/wiki/Intelligent_network
[16] http://www.interhack.net/pubs/network-security.pdf
[17] http://www.ehow.com/search.html?s=Network+Scan&skin=tech&t=all&rs=1 [18] http://en.wikipedia.org/wiki/Bellman%E2%80%93Ford_algorithm.