IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IV (Sep – Oct. 2014), PP 43-46
www.iosrjournals.org

Limitations of Network Security for Enabling Application Access

Rajesh Kumar

I. Introduction

As described above, network security was developed to protect the physical network and - as with network-layer Virtual Private Network (VPN) solutions - to extend the network. Protecting the network means identifying which packets have access to the protected network and which do not. Extending the network means identifying which remote devices or networks have access to the protected network and which do not. Applications, which use the network for a communications infrastructure, require far more granular control than network security can provide. For example, while literally thousands of applications utilize the UDP protocol, most network security simply prevents the UDP protocol - not individual applications - from traversing the network border. By operating at the network layer, network security has four major limitations when used as the sole enabler of secure application access:

Limited Application Connectivity

The use of network security severely limits connectivity for trusted applications as it prevents unwanted access. This connectivity is limited primarily by firewalls, which are further complicated by their use of NAT and non-routable private IP addresses. Firewalls are also often configured to block DNS traffic, which creates additional problems as application traffic is routed. These techniques, while critical for protecting the network, undermine an enterprise's ability to utilize the applications its business requires.

Limited Application Support

By limiting the ability of applications to connect, the number and types of applications that are securely enabled by network security is limited, too. Each application that the network administrator chooses to support requires new policies to define and manage,which further exposes the network. Consequently, supported applications are kept to a minimum. Network security addresses this with application proxies and VPNs. Application proxies, however, support individual applications; many of these solutions, while functional, are unacceptably slow. VPNs represent an alternative for fully trusted users,but the number of users that qualify to be a network node is small in relation to the total number of users requiring access. Even with a patchwork of point solutions and voluminous firewall access rules,enterprise network security has very limited application support.

Limited Application Security

Network security,by definition, provides network-layer security, which is often insufficient for deploying mission critical applications. Network security protects network devices. It authenticates and authorizes the device, which implies that once authorized to attach to the network any user or application can use this connection to access the network - a huge security risk. Additionally, network security can provide network layer encryption, which is often not flexible enough to adapt to the varying application- specific encryption requirements. Network security also can provide very little security within an application through protocol filtering, as only standard applications such as telnet and FTP are supported.

Limited Application Traffic Management

Enabling and managing reliable application traffic is challenging for network security. Network security products divide physically connected networks into many logically disconnected networks. They force all the network traffic to pass through a single access point (i.e.,the network perimeter or DMZ). When the perimeter is compromised or experiencing a physical failure, no applications, including those that are allowed to cross the perimeter, will be accessible. In most network architectures, redirecting applications to a different perimeter is a labor intensive task. Additionally, managing reliable access proves challenging when routing rules are broken. Since network security is based on the isolation principle, routing rules must be set manually.Any changes or updates that are required can be time consuming and prone to error.

II. The Challenge

hen network security is used to deploy applications, the network security itself presents the biggest obstacle to unfettered access to applications. Network security is critical. Firewalls are critical. NAT is critical. Private IP addresses are critical. How, then, can applications be securely extended without compromising the

network security? How can applications be securely extended to users independent of the network layer infrastructure and security? How can applications be securely extended to users who are on another private network behind third party network security and infrastructure? In short, can organizations separate protecting and securely extending the physical network from protecting and securely extending applications?

Introducing Application Security

As described above, network security is designed to protect and extend the network. It operates at layers two and three of the OSI network layer stack and is therefore not ideal for protecting and extending applications that operate at higher layers.

Application security represents the solution for securing applications and extending applications. As in any layered security model, application security complements and operates independent of the underlying security layers. Application security is an enabling technology that allows applications to be securely extended - akin to network security allowing networks to be securely extended to remote users or branch offices. Since applications are required everywhere, application security should not be constrained by physical network security, but at the same time it should not compromise it. Application security offers a more logical, virtual network - called the Application Network - that allows applications to be securely extended to any user anywhere in the world.

III. Defining the Application Network

The Application Network delivers the capabilities that allow organizations to now benefit both from unfettered access to the applications their businesses need and from enhanced application and network security. No longer required to make trade-offs between the productivity benefits of, for example, deploying real-time business applications and the consequential security risks of implementing and managing complex policies or point solutions.

Enterprises can now simply deploy the applications their businesses and the marketplace demands. The Application Network is not a physical network, but a conceptual one that is implemented to overcome the limitations of deploying applications using network security. Complementary to the physical IP network, the Application Network utilizes the underlying IP network to enable connectivity between trusted users and applications irrespective of their location and network security infrastructure. Working with network security, the Application Network enhances overall protection by securing the physical and logical network devices. It also provides security services to the individual users who use these network devices, such as laptops and application servers. Finally, it provides security services to the individual applications that run on the network devices.

When deployed, the Application Network represents a logical network that is layered over the physical networks while also serving as a logical network layered under the applications that require the physical network for communications and connectivity. The Application Network has the following four characteristics:

Cyber Murder

- Xenon Software is a leading software development company which has executed several branded software products for the Financial and Healthcare industry. Aplomb Hospitals, Singapore is one of the customers of the Company to whom a total Hospital Management software has been supplied.
- One day, Xenon receives a notice by fax stating inter-alia that there have been a chain of deaths in the hospital due to a faulty functioning of the software and claims damages to the extent of US $ 30 Million.
- Mr Ranganathan the CEO of Xenon rushes to Singapore to sort out the issue only to be arrested by Singapore Police immediately on landing and charged with “Causing Death Due to Negligence”.

Case Of A New Employee

- Chand IT Services is a BPO company based in Bangalore and engaged mainly in the processing of Financial Information for its US based principal who also do similar business with Chennai FinServe.
- Raghu the HR Manager recently recruited Sudha from Chennai FinServe at twice the salary she was drawing since she was part of an experienced software development team which had developed FinPro9, a Financial Information Processing Tools which enabled faster transaction processing. The tool was a proprietory software developed by Chennai FinServe and was responsible for making the company a preferred outsourcing partner in the Financial Information Processing.
- One fine day Police call on Chand IT Services for enquiry. They check systems in Sudha’s department and find a copy of FinPro9 installed in the network.They arrest M/s Raghu, Sudha, the network administrator and the CEO of the Company charging them of a conspiracy leading to theft of proprietory software from Chennai FinServe.

Hacking Of A Cnc Machine

- Mr Pramod is in charge of the systems that control the production.
- Bizone Chemicals is a company engaged in the manufacture of high value chemicals through batch processing. The process parameters are controlled through a sophisticated automated system configured through a computer console.
- It is found one day that an entire batch of chemicals worth several crores of rupees are qualitatively rendered inferior because the parameters of processing set for the batch was faulty.
- The access is controlled through a log-in ID and password system and several persons in the Company are authorized to access the Computer with different functional responsibilities.
- All passwords are allocated by the system administrator. The CEO of the Company maintains a list of all passwords allocated to authorized persons which is written down on paper and held in his personal safe custody.
- A complaint is filed by the CEO at the local Police Station alleging employee mischief.
- Police pick up Mr Pramod for enquiry. He insists that he had set the parameters correctly and it has been altered by some body in the Company without his authority.

Employee Jealousy

- Mr Vishwas and Ms Radha work in a Software Company as Programmers. Mr Vishwas is junior to Ms Radha, but is selected by the management for a prestigious project in USA. Ms Radha protests and demands that Mr Vishwas should withdraw and let her take his place. Mr Vishwas refuses and in the argument ridicules Ms Radha in open office that he was found to be a better person for the job and hence was selected.
- After some time, a large software development assignment is awarded to the Company and after a rigorous selection process and interviewing, the customer selects Mr Vishwas as project leader and names him as the key project resource. He is specially briefed and trained to take up the assignment.
- The customer has paid a large advance and the project is ready for commencement under a critical implementation schedule.
- Ms Radha's father in the meantime files a complaint with Police in India stating that he is in receipt of an obscene e-mail from his daughter's e-mail address and it has been sent by Mr Vishwas by hacking into her e-mail account. He also states that Mr Vishwas had unauthorisedly used Ms Radha's Credit Card while both were in USA and she had complained to the Company and that was the reason for his attempt to defame her.
- Police arrest Mr Vishwas and rendered unable to travel.
- The starting of the project is delayed and the Customer in USA has issued a notice of withdrawing the order and claiming damages for the delay..

Domain Name

- M/s Maser Info Ltd is a 15 year old, software company engaged in production of Banking Software and markets several products for the Banking industry under the brand "Maser Info".
- The Company has signed its first US Contract for a software project worth Rs 25 crores and has recruited several top notch professionals exclusively to service the project.
- The Company receives a notice from a Court in US, based on a complaint from a software Company that action is being initiated for "Infringement of a Trade Mark". The complaint alleges that the trade mark "Maser Info" is registered in USA for software products and using the mark as part of the Company's name and product and canvassing business in USA is an abuse of their rights. They demand payment of a large compensation and immediate stop to the activities of Maser Info all over the world.

TERRORIST MESSAGE

- Green Bird Textiles is a major Textile Manufacturer Exporter of repute and maintains a website. The website contains many pictures of its facilities, products, Directors etc.
- The Chairman of the Company is on a visit to USA and is arrested under a charge of continued active support to terrorism. Simultaneously other Directors and top executives are also under fear of being arrested.
- It is alleged that several photographs on the website of the Company were used to hide steganographic messages containing instructions for various terrorist activities across the globe.

SPAM

- Mantra BankSol is a Company which has developed and delivered a Core Banking Software product to a Canadian Customer. One of the features included in the product is that whenever a new product is

introduced, an e-mail information is sent to all the existing customers advising them about the features of the new product.

- An NGO in Canada has started legal proceedings against the Canadian Customer of Mantra BankSol for sending "Spam" mails.
- The customer claims a back to back indemnity from Mantra BankSol since the contract specifications envisages that the product would be "Cyber Law Compliant" and it was expected of Mantra BankSol to have brought to the attention of the customer any "Cyber Law Related Risks" arising due to the software structure.

IV. Carious Liability

- The webmaster of Company Hindustan Consumers Products receives an e-mail from a person Thomas stating that he is in receipt of a mail in the name of the CEO of the company offering dealership for the company's products in Chile in from one Mr Xavier and wants some additional information.
- The mail is passed on to the GM Marketing who is on tour and sees the mail only after 15 days.
- He has no plans for marketing in South Korea and ignores the mail
- After 6 months, a series of notices are received by the Company that the dealership agreements are not honoured and threatening legal action.
- Complainants state having paid huge amounts for the dealership to Mr Xavier who posed himself as the agent of the company.

V. Role Of Security Consultants

- Assist an Organization with E-Business Risk
- Protect the work force from the consequences of Cyber Crimes
- Improve the longevity of the Cyber Worker's career
- Assisting the HR Manager
- Mitigation of the Risk through appropriate security measures
- Assisting the IT Security Manager
- Protect the Information Assets of the organization from
- Being destroyed
- Being Manipulated
- Being Stolen
- Being spied upon being lost
- Protecting Information Assets

References

[1]. J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom98), 1998.

[2]. D. Camara and A.F. Loureiro. Gps/ant-like routing in ad hoc networks. Telecommunication Systems, 18(1–3):85–100, 2001.

[3]. H.S. Chang, W. Gutjahr, J. Yang, and S. Park. An Ant System approach to Markov Decision Processes. Technical Report 2003-10, Department of Statistics and Decision Support Systems, University of Vienna, Vienna, Austria, September 2003.

[4]. C. Cheng, R. Riley, S.P. Kumar, and J.J. Garcia-Luna-Aceves. A loop-free extended bellman-ford routing protocol without bouncing effect. ACM Computer Communication Review (SIGCOMM '89), 18 (4):224–236, 1989.

[5]. L. Chrisman. Reinforcement learning with perceptual aliasing: The perceptual distinctions approach. In Proceedings of the Tenth National Conference on Artificial Intelligence, pages 183–188, 1992.

[6]. I. Cidon, R. Rom, and Y. Shavitt. Multi-path routing combined with resource reservation. In IEEE INFOCOM'97, pages 92–100, 1997.

[7]. I. Cidon, R. Rom, and Y. Shavitt. Analysis of multi-path routing. IEEE/ACM Transactions on Network- ing, 7(6):885–896, 1999.

[8]. A. Colorni, M. Dorigo, V. Maniezzo, and M. Trubian. Ant system for job-shop scheduling. Belgian Journal of Operations Research, Statistics and Computer Science (JORBEL), 34:39–53, 1994.

[9]. M. Cottarelli and A. Gobbi. Estensioni dell'algoritmo formiche per il problema del commesso via ggiatore. Master 's thesis, Dipartimento di Elettronica e Informazione, Politecnico di Milano, Italy, 1997.

[10]. J.-L. Deneubourg, S. Aron, S. Goss, and J.-M. Pasteels. The self-organizing exploratory pattern of the argentine ant. Journal of Insect Behavior, 3:159–168, 1990.