Global Journal of Computer Science and Technology
Volume 11 Issue 4 Version 1.0 March 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Spectrum of Effective Security Trust Architecture to Manage the Interception of Packet Transmission in Value Added Networks

By S. N. Panda, Gaurav Kumar
Manav Bharti University

Abstract- World is growing with the emerging technologies. The computer networks and packet transmission systems are also growing in parallel, hence to manage and provide security to packet, a secured system is required. Networks seize or simply intercept is one of the challenges in the fast growing world of Cyber Crime. The network establishments are facing various types of threats on routine basis. To efficiently transmit information across a network, there is need of an improved and reliable architecture. An intrusion or intercept refers to an active sequence of events that deliberately try to cause harm, such as rendering system unusable, accessing unauthorized information, or manipulating such information. Security professionals may want to have Intercept Detection Systems record information about both successful and unsuccessful attempts so that security professionals will have a more comprehensive understanding of the events on their networks. The intercept detection systems should be developed with utmost care to avoid any natural or intentional attempts. Moreover, the packet encryption algorithm should be developed in such a way so that cracker is not able to change even a single bit in the confidential data.

Keywords- Trust Architecture, Packet Encryption, Cyber Security, Simulation, Secured Applications, Intercept Detection Systems

Classification: GJCST Classification: D.4.6, H.2.7

Strictly as per the compliance and regulations of:

Spectrum of Effective Security Trust Architecture to Manage the Interception of Packet Transmission in Value Added Networks

S. N. Panda[1], Gaurav Kumar[2]

Abstract-World is growing with the emerging technologies. The computer networks and packet transmission systems are also growing in parallel, hence to manage and provide security to packet, a secured system is required. Networks seize or simply intercept is one of the challenges in the fast growing world of Cyber Crime. The network establishments are facing various types of threats on routine basis. To efficiently transmit information across a network, there is need of an improved and reliable architecture. An intrusion or intercept refers to an active sequence of events that deliberately try to cause harm, such as rendering system unusable, accessing unauthorized information, or manipulating such information. Security professionals may want to have Intercept Detection Systems record information about both successful and unsuccessful attempts so that security professionals will have a more comprehensive understanding of the events on their networks. The intercept detection systems should be developed with utmost care to avoid any natural or intentional attempts. Moreover, the packet encryption algorithm should be developed in such a way so that cracker is not able to change even a single bit in the confidential data.

Keywords: Trust Architecture, Packet Encryption, Cyber Security, Simulation, Secured Applications, Intercept Detection Systems

I. Introduction

With the advent of Globalization, the Business as well as Defense Applications needs highly secured and consistent architecture so that packets can be transmitted in the network without any risk. Trust is the groundwork of the relationship which is established by a business organization with their customers, vendors, and employees. The speed at which computer network communications is taking place is increasing. It is therefore important to make the routines that send and receive network communication packets as efficient as possible such that information can be transmitted as fast as possible.

In order to achieve security and privacy in Wireless Sensor Networks, it is necessary to implement and deploy a certain number of mechanisms.

About[1]- Professor Regional Institute of Management and Technology Mandi Gobindgarh, Punjab, India
E-mail: panda.india@gmail.com
About[2]- Research Scholar Manav Bharti University Solan, Himachal Pradesh, India
E-mail: kumargaurav.in@gmail.com

According to the ITU-T X.509, Section 3.3.54, trust is defined as: "Generally an entity can be said to 'trust' a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects."

Trust is the establishment of confidence that something will or will not occur in a predictable or promised manner. The enabling of confidence is supported by identification, authentication, accountability, authorization, and availability.

To develop the trust between multiple parties, a set of principles or rules is to be offered so that the security of the entire model can be improved.

A study by McAfee has estimated that cyber crime losses may have passed $1 trillion in 2008, and, if a solution is not identified and implemented soon, that number is projected to grow with the slumping economy. Network Intercept provides solutions for Individuals and businesses looking to detect and avoid malicious intent on the internet, improve productivity, and protect their online privacy.

II. Intercept Detection Systems and Related Threats

An intrusion-detection system (IDS) refers to the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. The intrusion detection part of the name is a bit of a misnomer, as an IDS does not actually detect intrusions—it detects activity in traffic that may or may not be an intrusion. Intrusion detection is typically one part of an overall protection system that is installed around a system or device—it is not a stand-alone protection measure.

It is also important to note that IDSs and IPSs are just two of many methods that should be employed in a strong security program. Using a layered approach, or defense in depth, based on careful risk analysis is critical in any information protection program because a network is only as secure as its weakest link. This means that a network should have multiple layers of security, each with its own function, to complement the overall security strategy of the organization.

Intercept Detection and Prevention Systems are vital for many organizations, from small offices to large multinational corporations with many benefits:

- Greater proficiency in detecting intrusions than by doing it manually
- In-depth knowledge bases to draw from
- Ability to deal with large volumes of data
- Near real-time alerting capabilities that help reduce potential damages
- Automated responses, such as logging off a user, disabling a user account, or launching automated scripts
- Strong deterrent value
- Built-in forensic capabilities
- Built-in reporting capabilities

The most common types of threats fall into categories such as:

- Actual or attempted unauthorized probing of any system or data
- Actual or attempted unauthorized access
- Introduction of viruses or malicious code
- Unauthorized modification, deletion, or disclosure of data
- Denial of service attacks

These are all very good reasons to implement these technologies, but there are three main reasons that justify the need more than the others:

Legal and regulatory issues In 1998, the U.S. Presidential Decision Directive 63 (PDD 63) established steps to increase the use of intrusion detection and prevention to protect the national infrastructure. British Standard 7799 was first published in February 1995 and identified a comprehensive set of controls defining "best practices" for information security. Regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Gramm-Leach-Bliley Act of 1999 (GLBA) require audit controls to record and examine suspicious data-access activities. The preceding regulations may or may not be necessary, depending on the nature and location of your organization. In addition, implementation of an IDS/IPS program is not a requirement for complying with any of these, but will help to meet the requirements.

Quantification of attacks IDS and IPS allow a systems administrator the opportunity to quantify attacks against the organization's network for management. IDSs and IPSs both are able to build a profile of the types of attacks that are being tried against a network. This allows a stronger business case to be made for appropriate security measures, which can often be hard to justify. IPSs and IDSs can also provide evidence against attackers if litigation is desired.

Establishment of an overall defense-in-depth strategy IDSs and IPSs have become a critical part of a strong defense-in-depth security program, and their use shows due diligence on the part of the organization because the organization is being proactive in the expectation of and reaction to intrusions. Both technologies will help provide protection for network and application layer vulnerabilities, as well as help to correlate and validate information from other devices, such as antivirus programs, firewalls, and routers.

The advantages of intercept detection include the following:

- Can detect external hackers as well as internal network-based attacks
- Scales easily to provide protection for the entire network
- Offers centralized management for correlation of distributed attacks
- Provides defense in depth
- Gives system administrators the ability to quantify attacks
- Provides an additional layer of protection

III. Types of Intercept Detection Systems

IDSs fall into one of three categories: host-based intrusion-detection system (HIDS), network-based intrusion-detection system (NIDS), and hybrids of the two.

A HIDS system will require some software that resides on the system and can scan all host resources for activity; some just scan syslog and event logs for activity. It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base.

A NIDS system is usually inline on the network, and it analyzes network packets looking for attacks. A NIDS receives all packets on a particular network segment, including switched networks (where this is not the default behavior) via one of several methods, such as taps or port mirroring. It carefully reconstructs the streams of traffic to analyze them for patterns of malicious behavior. Most NIDSs are equipped with facilities to log their activities and report or alarm on questionable events. In addition, many high-performance routers offer NID capabilities.

A hybrid IDS combines a HIDS, which monitors events occurring on the host system, with a NIDS, which monitors network traffic. The basic process for an IDS is that a NIDS or HIDS passively collects data and preprocesses and classifies them. Statistical analysis can be done to determine whether the information falls outside normal activity, and if so, it is then matched

against a knowledge base. If a match is found, an alert is sent.

IV. Intrusion-Prevention System (IPS)

IPS systems are similar in setup to IDS systems—an IPS can be a host-based IPS (HIPS), which work best at protecting applications, or a network-based IPS (NIPS). User actions should correspond to actions in a predefined knowledge base; if an action isn't on the accepted list, the IPS will prevent the action. Unlike an IDS, the logic in an IPS is typically applied before the action is executed in memory. Other IPS methods compare file checksums to a list of known good checksums before allowing a file to execute, and to work by intercepting system calls.

An IPS will typically consist of four main components:

- Traffic Normalizer
- Service Scanner
- Detection Engine
- Traffic Shaper

The traffic normalizer will interpret the network traffic and do packet analysis and packet reassembly, as well as performing basic blocking functions. The traffic is then fed into the detection engine and the service scanner. The service scanner builds a reference table that classifies the information and helps the traffic shaper manage the flow of the information. The detection engine does pattern matching against the reference table, and the appropriate response is determined.

V. Cryptography and Cryptographic Algorithms

Cryptography is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptographic algorithms are sequences of processes, or rules, used to encipher and decipher messages in a cryptographic system. In simple terms, they're processes that protect data by making sure that unwanted people can't access it. These algorithms have a wide variety of uses, including ensuring secure and authenticated financial transactions.

Most cryptography algorithms involve the use of encryption, which allows two parties to communicate while preventing unauthorized third parties from understanding those communications. Encryption transforms human readable plaintext into something unreadable, also known as ciphertext. The encrypted data is then decrypted to restore it, making it understandable to the intended party. Both encryption and decryption operate based on algorithms.

There are many different types of cryptographic algorithms, though most of them fit into one of two classifications — symmetric and asymmetric. Some systems, however, use a hybrid of both classifications. Symmetric algorithms, also known as symmetric-key or shared-key algorithms, work by the use of a key known only to the two authorized parties. While these can be implemented in the form of block ciphers or stream ciphers, the same key is used for both encrypting and decrypting the message. The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are the most popular examples of symmetric cryptography algorithms.

Asymmetric cryptography algorithms rely on a pair of keys — a public key and a private key. The public key can be revealed, but, to protect the data, the private key must be concealed. Additionally, encryption and decryption of the data must be done by the associated private and public keys. For example, data encrypted by the private key must be decrypted by the public key, and vice versa. RSA is one of the most common examples of this algorithm.

Symmetric algorithms are usually much faster than asymmetric algorithms. This is largely related to the fact that only one key is required. The disadvantage of shared-key systems, however, is that both parties know the secret key. Additionally, since the algorithm used is the public domain, it is actually the key that controls access to the data. For these reasons, the keys must be safe-guarded and changed relatively frequently to ensure security.

While cryptographic algorithms are used to provide security, they are not 100% fool-proof. Suboptimal system can be infiltrated and sensitive information can be compromised as a result. Rigorous testing of the algorithms, therefore, especially against established standards and identified weaknesses is vital to assuring the utmost security.

VI. Symmetric-key Cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976. One round (out of 8.5) of the patented IDEA cipher, used in some versions of PGP for high-speed encryption of, for instance, e-mail.

VII. Public-key Cryptography

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating

parties must, ideally, share a different key, and perhaps each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret. The difficulty of securely establishing a secret key between two communicating parties, when a secure channel does not already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world.

The goal of cryptanalysis is to find some weakness or insecurity in a cryptographic scheme, thus permitting its subversion or evasion.

It is a common misconception that every encryption method can be broken. In connection with his WWII work at Bell Labs, Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key material is truly random, never reused, kept secret from all possible attackers, and of equal or greater length than the message. Most ciphers, apart from the one-time pad, can be broken with enough computational effort by brute force attack, but the amount of effort needed may be exponentially dependent on the key size, as compared to the effort needed to use the cipher. In such cases, effective security could be achieved if it is proven that the effort required (i.e., "work factor", in Shannon's terms) is beyond the ability of any adversary. This means it must be shown that no efficient method (as opposed to the time-consuming brute force method) can be found to break the cipher. Since no such showing can be made currently, as of today, the one-time-pad remains the only theoretically unbreakable cipher.

There are a wide variety of cryptanalytic attacks, and they can be classified in any of several ways. A common distinction turns on what an attacker knows and what capabilities are available. In a ciphertext-only attack, the cryptanalyst has access only to the ciphertext (good modern cryptosystems are usually effectively immune to ciphertext-only attacks). In a known-plaintext attack, the cryptanalyst has access to a ciphertext and its corresponding plaintext (or to many such pairs). In a chosen-plaintext attack, the cryptanalyst may choose a plaintext and learn its corresponding ciphertext (perhaps many times); an example is gardening, used by the British during WWII. Finally, in a chosen-ciphertext attack, the cryptanalyst may be able to choose ciphertexts and learn their corresponding plaintexts. Also important, often overwhelmingly so, are mistakes (generally in the design or use of one of the protocols involved; see Cryptanalysis of the Enigma for some historical examples of this).

VIII. Cryptosystems

One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or cryptosystem. Cryptosystems (e.g. El-Gamal encryption) are designed to provide particular functionality (e.g. public key encryption) while guaranteeing certain security properties (e.g. CPA security in the random oracle model). Cryptosystems use the properties of the underlying cryptographic primitives to support the system's security properties. Of course, as the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem can be derived from a combination of several more primitive cryptosystems. In many cases, the cryptosystem's structure involves back and forth communication among two or more parties in space (e.g., between the sender of a secure message and its receiver) or across time (e.g., cryptographically protected backup data). Such cryptosystems are sometimes called cryptographic protocols.

Some widely known cryptosystems include RSA encryption, Schnorr signature, El-Gamal encryption, PGP, etc. More complex cryptosystems include electronic cash systems, signcryption systems, etc. Some more 'theoretical' cryptosystems include interactive proof systems, (like zero-knowledge proofs,), systems for secret sharing, etc.

IX. Objectives of the Study

The main objectives of this research are to focus on Multiple Trust Architectures and heir features. Moreover the emphasis is given to explore various kinds of cryptographic algorithms used and Trust Architectures. The paper proposes a Trust Architecture for Value Added Networks and the need of an effective cryptography algorithm for Proposed Trust Architecture. An implementation of the proposed Trust Architecture and Cryptography Algorithm can be performed using Simulation.

X. Conclusion and Scope of Future Work

All Trust Architectures and Intercept detection technology are not effective. These neither provided security to packet formation nor giving any security during transmission. All Trust Architecture developed till now doesn't provide absolute security and significant features. The VAN sometimes paralyzed and giving a great scope to the intruders/interceptors and other cyber criminals either to damage or alter or misuse the packets during transmission. Most of the fund transfer systems, EDI systems, business applications are using emerging technologies and exposed to vulnerability increases tremendously. Moreover, the cryptographic algorithms used during packet formation and

transmission are sometimes responsible for vulnerabilities.

References Références Referencias

1. Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent Issued on August 18, 1998
2. Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia
3. Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security Practice, Sun BluePrints™ OnLine - December 2002, Trust Modeling for Security Architecture Development
4. Security, Encryption, Acceleration, http://www.networkintercept.com
5. Youlu Zheng, Shakil Akhtar, Networks for Computer Scientists and Engineers, Oxford University Press, 2009
6. Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004
7. "IDATA – An Effective Intercept Detection Algoritm for Packet Transmission in Trust Architecture" accepted for publication in an International Journal IEEE Potential in incoming issue (Paper id is POT-2010-0006).
8. Gaurav Kumar, Dr. S. N. Panda, "An Effective Algorithm for Development and Analysis of Forensic Database in Security Trust Architecture", POT-2010-0040.R1selected for publication in IEEE Potentials ISSN: 0278-6648.
9. Dr. S. N. Panda, Gaurav Kumar, "An Implementation of IDATA: Intercept Detection Algorithm for Packet Transmission in Trust Architecture", Global Journal of Computer Science and Technology, GJCST Volume 10 Issue 11 Version 1.0 October 2010, Hayward, CA, USA Online ISSN: 0975-4172, Print ISSN: 0975-4350