International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 3 Issue 6 November 2013
International Manuscript ID : 2249054XV3I6112013-06

AN EMPIRICAL IMPLEMENTATION OF CRYPTOGRAPHY ALGORITHM

Jamal kh madhloom [1], Bilal Riyadh Imran [2], Sandeep Goel [3]

1. M.Tech.(CSE) Scholar, M. M. University, Mullana, Haryana, India
2. M.Tech.(CSE) Scholar, M. M. University, Mullana, Haryana, India
3. Head of Department, CSE, M. M. University, Mullana, Haryana, India

Abstract

In today's scenario, the networks are facing challenges from increasing interceptions and cracking attempts through various sources. There is need to secure the data packets roaming around the network from multiple interceptions using efficient cryptographic algorithms. To avoid the problem of in between cracking attempts, we have developed a new algorithm for cryptography that works in multiple phases. In the first phase, the Java based software accepts input as a stream of characters. Then two numbers n1 and n2 are accepted. The swapping is performed in the multiples of n1 in the way that first n1th character is replaced by last n1th character. In the final stage, if direction LEFT is selected, it means that n2 characters from right will be moved to the leftmost position.

Using this method, encryption and decryption can be performed effectively with unique cryptographic technique without any complexity. Moreover, the forensic database will keep record of every invalid or unacceptable decrypted packet. Using records in this database, we can analyze the behavior of intercepts to avoid these in future. 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 networks 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 this manuscript, we have developed and implemented a new algorithmic approach for cryptography that is relatively secure and rapid.

Keywords - Network Security, Cryptography, Encryption

INTRODUCTION

In order to achieve security and privacy in Wireless Sensor Networks, it is necessary to implement and deploy a certain number of mechanisms. [1, 2]

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.” [3]

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. [4]

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 [5, 6].

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 [6]:

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.

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.

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.

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-andegg 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.

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.

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.

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. This research work proposes and implements the efficient algorithms for Packet Encryption as well as the standard to detect any kind of intercept attempt.

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.

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.

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

OBJECTIVES OF THE STUDY

The main objectives of this research are –

1. Focus on Multiple Trust Architectures and their features
2. Explore various kinds of cryptographic algorithms used and Trust Architectures
3. Propose Trust Architecture for Value Added Networks
4. Propose Cryptography Algorithm for Proposed Trust Architecture
5. Implementation of proposed Trust Architecture and Cryptography Algorithm by using Simulation

CONCLUSION

Networks are facing challenges from increasing interceptions and cracking attempts through various sources. There is need to secure the data packets roaming around the network from multiple interceptions using efficient cryptographic algorithms. The packet encryption algorithm explained is an efficient algorithm based on multiple layer operation which is a unique method. Using this method, encryption and decryption can be performed effectively with unique cryptographic technique without any complexity. Moreover, the forensic database will keep record of every invalid or unacceptable decrypted packet. Using records in this database, we can analyze the behavior of intercepts to avoid these in future.

REFERENCES

[1] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent 5797039 Issued on August 18, 1998

[2] D. M. Kyriazanos, N. R. Prasad, and C. Z. Patrikakis, "A security, privacy and trust architecture for wireless sensor networks," in Proc. 50th Int. Symp. ELMAR-2008, Zadar, Croatia, Sept. 10–12, 2008, pp. 523-529

[3] D. Andert, R. Wakefield, and J. Weise. (2002, Dec.). Professional Services Security Practice. Sun Blue- Prints. Trust modeling for security architecture development [Online]. Available: http://www.sun.com/blueprints/ 1202/817-0775.pdf

[4] Network Intercept. (2009). Security, Encryption, Acceleration [Online]. Available: 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] http://www.thenetworkencyclopedia.com/d2.asp?ref=1495

[8] Analysis of Snake Movement Forms for Realization of Snake-like Robots, Shugen MA, JAPAN, Proceedings of the 1999 IEEE International Conference on Robotics & Automation Detroit, Michigan May 1999

[9] A Simulator to Analyze Creeping Locomotion of a Snake-like Robot, Proceedings of the 2001 IEEE International Conference on Robotics & Automation, Seoul, Korea. Shugen Wen J, Yuechao WANG, Hitachi-Shi Ibaraki-Ken

[10] Control of a Creeping Snake-like Robot, Igor Grabec, University of Ljubljana, Faculty of Mechanical Engineering, ASkerEeva

[11] Design and Control of a Snake Robot according to Snake Anatomy, Ahmadreza Rezaei, Yasser Shekofteh, Mohammad Kamrani, Ali Fallah, Farshad Barazandeh, Amirkabir University, Tehran, Iran

[12] Tracking Multiple Objects Using Moving Snakes, Jonas De Vylder, Daniel Ochoa, Wilfried Philips, Laury Chaerle, Dominique Van Der Straeten, Department of Telecommunications and Information Processing, IEEE

[13] Motion Planning of a Snake-like Robot Based on, Artificial Potential Method, Changlong Ye, Deli Hu, Shugen Ma, Huaiyong Li, Proceedings of the 2010 IEEE, International Conference on Robotics and Biomimetics, December 14-18, 2010, Tianjin, China

[14] Improving Concavity Performance of Snake Algorithms A. Roubies, A. Hajdu, I. Pitas Dept. of Informatics, Aristotle University of Thessaloniki, Box 451, GR-54124 Thessaloniki, Greec