ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

Proven Algorithmic Strategies for Information Protection

Ms.Gurpreet Kaur

Assistant Professor, Chandigarh University, Gharuan, Punjab, India

Abstract: Information technology professionals, holding the responsibility of determining appropriate solutions for the security of confidential information, examine cryptographic approaches through algorithmic properties. Implementation of the symmetric-key and public-key strategies remain the most frequently applicable policies for professionals requiring the distribution of private information. The number of parties possessing access to secure information and the viability of prospective adversaries impact the decision-making process for a technical solution. After determining the nature of the communication stream, including the necessary technical properties, information technology professionals can identify specific algorithms for securing information. When communication streams require simple transactions of encryption and decryption by all parties, the symmetric-key strategy provides a convenient method for the protection and retrieval of information. For more complex networks of communication, the public-key strategy provides additional algorithmic structures to protect information from access by prospective adversaries. Applying both strategies simultaneously can assure maximum protection of the storage and distribution of confidential information.

Index Terms: adversaries, algorithms, cryptography, public-key, symmetric-key.

I. INTRODUCTION

INTERCEPTION of communication by adversaries disrupts the protection and distribution of secure communication. Two technology users, seeking to distribute confidential information securely through an internet connection, discover the challenges of protecting data from breach by third parties. Deriving and implementing protocols for preventing disturbances in communication is the primary objective for information security professionals. Cryptography examines solutions for delivering information securely between parties without the presence of outside networks. While computer programmers and software engineers often engage in the process of protecting data by establishing algorithms, cryptography extracts symmetric-key and public-key as the two primary solutions for distributing secure information.

II. OBJECTIVES

Cryptographic algorithms implement a mathematical computation presenting challenges to adversarial interruption. When technology users possess a confidential password for application which is not sent through public networks, reversing or interrupting functions may become exponentially more difficult. After applying a padlock to a locker, for example, the user can only reverse its function by using a special password unknown to outside parties. While modern cryptography may require parties to distribute numerical identifiers publically, users extract additional confidential digits outside of an internet connection in order to ensure information security [1].

Sound cryptographic solutions force adversaries to engage in trail and error queries where a seemingly infinite number of prospective answers are present. Since no adversary has an infinite amount of time to guess the correct password, these algorithms provide a computationally secure strategy for protecting information.

Even though information security professionals could presumably develop an infinite number of algorithms for protecting data, applying proven computational theories remains the most frequent solution for delivering cryptographic services. While symmetric-key and public-key provide efficient paradigms for technological security, information technology professionals should consider additional protocols for assuring the protection of communication. By identifying the properties and application strategies of both principles while considering additional areas in which private data can provide extra protections, the professional can implement the appropriate security solution for any given technical scenario.

III. RESEARCH METHODOLOGY

Through an evidence-based examination of the principles and strategies of symmetric-key and public-key, information technology professionals determine the appropriate solution for application and identify other potential algorithmic innovations. Symmetric-key, typically a speedy and simple solution, contains fundamental principles for keeping data secure. Public-key, a more complex algorithmic solution, ensures greater protection from adversaries. The prospect of using both technologies simultaneously presents opportunities for providing the greatest protection for confidential information.

Even though the symmetric-key requires less algorithmic data in order to provide a security solution, information technology professionals frequently implement the strategy as a matter of convenience and simplicity. When transferring information, two or more respective parties have access to one key. Any party can use it for the encryption or decryption of any file on particular networks. Since the sender and receive information holds the same key, the solution provides simple retrieval of

confidential information to all parties.

While symmetric-key remains a frequent solution for information technology professionals, many implement a public-key strategy for additional protective measures. Public-key commands two separate keys for encryption and decryption processes. The strategy essentially creates a "public" and "private" key in which the former is available for all parties through a communication stream and the later can only be seen when the individual user extracts additional digits from the public key [2]. Even though the process is slower and more complex than symmetric-key, it becomes far more challenging for potential adversaries to intercept confidential information.

While many information technology professionals take an "either-or" approach when determining the appropriate for information security, both strategies possess the ability to work concurrently. In order to provide the most protection against adversaries, the professional should implement the public-key strategy as the foundational security plan. By adding the convenience of symmetric-key for the retrieval of the various public keys for accessing information, the professional can make it more efficient for users to access information while making it more challenging for adversaries.

IV. IMPLICATIONS

Online communication streams with multiple parties require a technical solution with the widest possible range of protection against security breaches. When two or more partiers communicate through a network, the prospect of adversarial interruption increases significantly. Therefore, implementing the public-key strategy as a foundational security policy provides the necessary protections for confidential information. However, using the symmetric-key strategy to provide additional protections for the retrieval of public keys establishes a comprehensive approach to securing confidential information. Using both strategies collaboratively creates multiple algorithmic structures providing security and nearly eliminates any chances of security breach by adversaries.

REFERENCES

[1] B. Hemenway, "Overview of Secure Multiparty Computation" in Achieving Higher-Fidelity Conjunction Analysis Using Cryptography to Improve Information Sharing, 1st ed., vol. 1, Santa Monica: RAND Corporation, 2014, pp. 5-20.

[2] N. Koblitz, (2004, Dec.) A Survey of Public-key Cryptosystems. SIAM Review. [Online]. 46(4), pp. 599-634. Available: http://www.jstor.org/stable/20453567