International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 59 - 61

"Efficient Techniques for Privacy-Preserving Sharing of Sensitive Information for larger data"

Asma Khanam
Department of Computer Science & Engg.
Nuva College of Engineering & Technology
Nagpur, India
asma.persona@gmail.com

Prof. Shyam P. Dubey
Department of Computer Science & Engg.
Nuva College of Engineering & Technology
Nagpur, India

Abstract:-The need of privacy preserving sharing of sensitive information occurs in many different and realistic scenarios every day, ranging from national security to social networking. A typical setting involves two parties; one is for seeking information from the other without revealing the interest while the second is either willing or compelled, to share only the requested information. This poses two challenges; one how to enable sharing such that parties learn no information beyond what they are entitled to, and the second is how to do so efficiently, in real-world practical terms. This explores the notion of Privacy-Preserving Sharing of Sensitive Information (PPSSI), and provides a concrete and efficient incarnation, modeled in the context of simple database querying. Proposed approach functions like a privacy shield to protect parties to disclose more than the required minimum of their respective sensitive information. PPSSI deployment induces several challenges, which are addressed in this paper. Comprehensive experimental results attest to the practicality of attained privacy features and show that our approach incurs quite low overhead.

Keywords: *Privacy-Preserving Sharing of Sensitive Information, privacy shield.*

*****

I. Introduction

In today's growing digital world, there is often a tension between safeguarding privacy and sharing information. Although, in general, sensitive data clearly needs to be kept intimate, data owners are often motivated, or forced, to share sensitive information Privacy-Preserving Sharing of Sensitive Information (PPSSI), and propose one efficient and secure instantiation that functions like a privacy shield to protect parties to disclose more than the required minimum of sensitive information. We model PPSSI in the context of uncomplicated database-querying applications with two parties: a server that has a database, and a client, that performs simple disjunctive equality queries.

In terms of the airline safety example above, the airline (server) has a database of passenger information, while DHS (client) poses queries corresponding to its TWL. Intended Contributions. We explore the idea of Privacy-Preserving Sharing of Sensitive Information (PPSSI). Our main focuses are Private Set Intersection (PSI) techniques. As a part of PPSSI design, we address several challenges stemming from adapting PSI to realistic database settings. In particular, we propose a novel encryption method to handle challenges of 'multi-sets' and 'data pointers'. And present a new architecture with an Isolated Box to deal with "bandwidth" and "liability" challenges. Our experimental evaluation demonstrates that our approach incurs very low overhead: about 10% slower than standard (not privacy-preserving) MySQL. All source code is publicly available.

II. Problem Definition

- Focused on alternative attack detection methods (statistical /behavioral).
- Machine learning techniques have been successfully used.
- In certain domains despite the extensive academic research efforts.
- Such systems have had limited success I field of intrusion detection.

III. Objective

- The implementation stage of the project is when the theoretical design is turned out into a working system. Thus it can be considered as the most critical stage for achieving a successful new system and giving the user, confidence that the new system will work and be effective.
- The implementation stage involves planning, analysis of the existing system and it's restraints on implementation, designing methods to achieve changeover and evaluation of changeover methods.

IV. Proposed System

We propose to establish a defense-in-depth intrusion detection framework. For better attack detection, big data incorporates attack graph analytical processes into the intrusion detection processes. We must note that the design of does not intend for improving any of the existing intrusion detection algorithms; indeed, employs a re-configurable virtual networking approach for detecting and countering the attempts to compromise VMs, thus preventing zombie VMs.

Flow Diagram

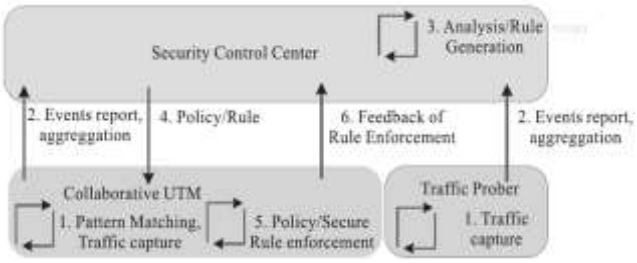

Figure1. Data Flow System

Main Modules:-

1. User Module

In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2. Countermeasure Selection:

Countermeasure Selection to illustrate how big data works, let us consider for example, an alert is generated for node 16 (*vAlert* = 16) when the system detects LICQ Buffer overflow. After the alert is generated, the cumulative probability of node 16 becomes 1 because that attacker has already compromised that node. This triggers a change in cumulative possibilities of child nodes of node 16. Now the next step is to select the countermeasures from the pool of countermeasures *CM*.

3. Attack Analyzer:

The major functions of big data system are performed by attack analyzer, which includes procedures such as attack graph construction and update, alert correlation and selection of countermeasure. The process of constructing and utilizing the Scenario Attack Graph (SAG) has of three phases: information gathering, attack graph construction, and potential exploit path analysis. With this information, attack scan be modeled using SAG. Each node in the attack graph exploited by the attacker. Each path from an initial node to a goal node represents a successful attack, attack where the vulnerability is discovered by the attacker but is not detected by vulnerability scanner. In such case, the real alert will be consider as false, given that there does not exist corresponding node in SAG. Thus, current research is difficult to address how to reduce the false negative rate. It is important to note that vulnerability scanner should be able to notice most recent vulnerabilities and sync with the latest vulnerability database to reduce the chance of Zero-day attacks. Snort: An open source network intrusion (encroachment) prevention and detection system. It uses a rule-based language combining signature, protocol and anomaly inspection methods.

Snort: the most widely establish intrusion detection and prevention technology and it has become the de facto standard technology worldwide in the industry. Snort does not evaluate the rules in the order that they appear in the Snort rules file. In default, the order is:

1. Alert rules
2. Pass rules
3. Log rules

Straightforward fulfillment of data-leak detection requires the plain text sensitive data. However, this requirement is undesirable, due to it may threaten the confidentiality of the sensitive information. If a detection system is compromised, then it may expose the plain text sensitive data (in memory). In addition, the data owner may need to outsource the data-leak detection to providers, but it may be unwilling to reveal the plain text sensitive data to them. Therefore, one needs new solutions of data-leak detection that allow the providers to scan content for leaks without learning the sensitive information. The proposed method has several advantages.

1. To avoid the attacker.
2. Secrecy of the data should be maintained.
3. Key management is not an issue since there are no secret keys involved as encryption is carried out based on the distribution of values amongst various shares.
4. The scheme is robust to withstand brute force attacks.

We categorize causes for sensitive data to appear on the outbound traffic of an organization, including the legitimate data use by the employees into three categories. Case I Inadvertent data leak: The sensitive data is accidentally leaked in the outbound traffic by a legal user. This paper focuses on detecting this type of accidental data leaks over supervised network channels. Inadvertent data leak takes place may be due to human errors such as forgetting to use encryption, incautious forwarding of an internal email and attachments to outsiders.

V. Conclusions

In this paper, we proposed a novel architecture for Privacy-Preserving Sharing of Sensitive Information (PPSSI), based on efficient PSI techniques. It enables a client and a server to exchange information without leaking more than the required minimum. Privacy guarantees are formally defined and achieved with provable security. Experimental results show that our approach is sufficiently efficient for real-world applications.

References

[1] Asonov, D., Freytag, J.-C.: Almost optimal private information retrieval. In: PETS (2003)
[2] Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506–522. Springer, Heidelberg (2004)
[3] Caslon Analytics. Consumer Data Losses, http://www.caslon.com.au/datalossnote.htm
[4] Chor, B., Gilboa, N., Naor, M.: Private information retrieval by keywords. Manuscript (1998)
[5] Chor, B., Kushilevitz, E., Goldreich, O., Sudan, M.: rivate information retrieval. Journal of the ACM 45(6), 965–981 (1998)
[6] Davidoff, S.: What Does DHS Know About You?, http://tinyurl.com/what-dhs-knows
[7] De Cristofaro, E., Jarecki, S., Kim, J., Tsudik, G.: Privacy-preserving policy-based information transfer. In: Goldberg, I., Atallah, and M.J. (eds.) PETS 2009. LNCS,
[8] vol. 5672, pp. 164–184. Springer, Heidelberg (2009)
[9] De Cristofaro, E., Lu, Y., Tsudik, G.: Efficient techniques for privacy-preserving sharing of sensitive information. Cryptology ePrint Archive, http://eprint.iacr. org/2011/113
[10] De Cristofaro, E., Tsudik, G.: Practical private set intersection protocols with linear complexity. In: Sion, R. (ed.) FC 2010. LNCS, vol. 6052, pp. 143–159. Springer, Heidelberg (2010)

[11] Feige, U., Killian, J., Naor, M.: A minimal model for secure computation (extended abstract). In: STOC (1994)
[12] Fischlin, M., Pinkas, B., Sadeghi, A.-R., Schneider, T., Visconti, I.: Secure set intersection with untrusted hardware tokens. In: CT-RSA (2011)
[13] Freedman, M.J., Nissim, K., Pinkas, B.: Efficient private matching and set intersection.
[14] In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 1–19. Springer, Heidelberg (2004)
[15] Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T.: Protecting data privacy in private information retrieval schemes. In: STOC (1998)