International Journal For Technological Research In Engineering
Volume 5, Issue 12, August-2018 *ISSN (Online): 2347 - 4718*

SECURITY REQUIREMENTS ENGINEERING: A FRAMEWORK FOR REPRESENTATION AND ANALYSIS

Aarshvi Patel[1]
[1]Student, L.J. Institute of Engineering and Technology,Ahmedabad,Gujarat,India

ABSTRACT: This paper presents a framework for security requirements elicitation and analysis, based upon the construction of a context for the system, representation of security requirements as constraints, and satisfaction arguments for the requirements in the system context. The system context is described using a problem-centered notation, then is validated against the security requirements through construction of a satisfaction argument. The satisfaction argument is in two parts: a formal argument that the system can meet its security requirements, and a structured informal argument supporting the assumptions expressed in the formal argument. The construction of the satisfaction argument may fail, revealing either that the security requirement cannot be satisfied in the context, or that the context does not contain sufficient information to develop the argument. In this case, designers and architects are asked to provide additional design information to resolve the problems. We evaluate the framework by applying it to a security requirements analysis within an air traffic control technology evaluation project.

I. INTRODUCTION

Over the last few years, reports of software security failures have become commonplace. Statistics from the Software Engineering Institute's CERT Coordination Center, a center of internet security expertise, show that the number of reported application vulnerabilities rose from 171 in 1995 to 5,990 in 2005 (CERT, 2006). The sources of problems are diverse. One source is programming errors; in 2003, one internet worm named Blaster, exploiting a flaw in Microsoft's Windows operating system, reportedly infected approximately 500,000 computers (Gallagher, 2003). "Estimates are that it [Blaster] cost approximately $1.3 billion to correct and in lost productivity" (Ibid). Another source is not looking at security requirements of the complete system. For example, CardSystems Solutions exposed details of some 40 million credit cards by storing unneeded transaction history data where hackers could get to it (Dash, 2005); this visible storage was part of their system but not part of their security planning. The resulting loss has not been disclosed, but is known to be in excess of several millions of dollars (Federal Trade Commission, 2006). These two examples strongly suggest that improving software-based system security would have a significant financial impact. This thesis addresses the second source of security problems: the failure to consider security requirements of the complete system, or said another way, the failure to obtain adequate security requirements for a system. By adequate security requirements, we mean requirements that if respected, lead to a system's security goals being satisfied. Adequate general requirements have been shown to have a very positive impact on the success of projects: for examples see the Standish Group's Chaos reports (Standish Group, 1995, 1999, 2001), and the introduction to Mead et al. (Mead, Hough, & Stehney, 2005). Although the empirical evidence is not yet unequivocal, there is evidence that adequate security requirements will have as positive an impact on system security as adequate general requirements have on system success

II. EXISTING SYSTEM

Sensor data aggregation assumes a trusted aggregator, and hence cannot protect user privacy against an untrusted aggregator in mobile sensing applications. Several recent works consider the aggregation of time-series data in the presence of an untrusted aggregator. To protect user privacy, they design encryption schemes in which the aggregator can only decrypt the sum of all users' data but nothing else.

Use threshold Paillier cryptosystem to build such an encryption scheme. To decrypt the sum, their scheme needs an extra round of interaction between the aggregator and all users in every aggregation period, which means high communication cost and long delay. Moreover, it requires all users to be online until decryption is completed, which may not be practical in many mobile sensing scenarios due to user mobility and the heterogeneity of user connectivity.

DISADVANTAGES OF EXISTING SYSTEM

- Cannot protect user privacy against untrusted aggregators.
- Existing works do not consider the Min of time-series data.

PROPOSED SYSTEM

We propose a new privacy-preserving protocol to obtain the Sum aggregate of time-series data.

The protocol utilizes additive homomorphic encryption and a novel, HMAC- based key management technique to perform extremely efficient aggregation.

ADVANTAGES

- Our scheme has much lower communication overhead than existing work.
- Utilizes the redundancy in security to reduce the communication cost for each join and leave.

MODULE DESCRIPTION:

- System Model Module
- Encryption Scheme Module

- Key Generation Module
- Aggregation Protocol Module

System Model Module

In this module first we develop our system model, with mobile users.

An aggregator wishes to get the aggregate statistics of n mobile users periodically, for example, in every hour.

The time periods are numbered as 1, 2, 3, and so on.

In every time period, each user i encrypts her data xi with key ki and sends the derived ciphertext to the aggregator. From the ciphertexts, the aggregator decrypts the needed aggregate statistics using her aggregator capability k0.

In each time period, a mobile user sends her encrypted data to the aggregator via WiFi, 3G or other available access networks. No peer-to-peer communication is required among mobile users, since such communication is nontrivial in mobile sensing scenarios due to the high mobility of users and users may not be aware of each other for privacy reasons.

We consider an untrusted aggregator that is curious about each individual user's data. The aggregator may eavesdrop all the messages sent from/to every user. A number of users may collude with the aggregator, and reveal their data to the aggregator. A number of users may also collude to obtain the aggregate.

Encryption Scheme Module

One building block of our solution is the additive homomorphic encryption scheme.Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext. To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used. The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, there is no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key. It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks.

Key Generation Module

Suppose there are nc random numbers. The aggregator has access to all the numbers, and it computes the sum of these numbers as the decryption key k0. These numbers are divided into n random disjoint subsets, each of size c. These n subsets are assigned to the n users, where each user has access to one subset of numbers. User i computes the sum of the numbers assigned to it as the encryption key ki. The aggregator cannot know any user's encryption key because it does not know the mapping between the random numbers and the users. When c is large enough, it is infeasible for the aggregator to guess the numbers assigned to a particular user with a brute-force method. The aggregator's decryption key cannot be revealed by any user because no user knows all the numbers.

Aggregation Protocol Module

The Min aggregate is defined as the minimum value of the users' data. This module presents a protocol that employs the Sum aggregate to get Min.

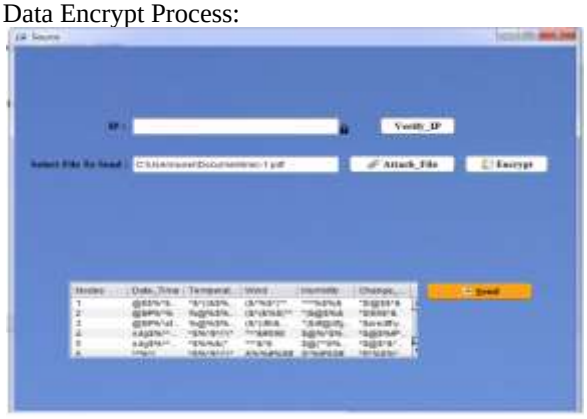
Each user uses just one set of secrets for all instances of the sum aggregation protocol.

When the plaintext space is large, the cost of the basic scheme is high. In some application scenarios, it may not be necessary to get the exact Min, but an approximate answer is good enough. For such scenarios, the basic scheme can be extended to get an approximate Min with much smaller cost.

SCREENSHOTS

SRE Event Pages:

Data Encrypt Process:



SRE Nodes Diagram:

Framework For Representation And Analysis Nodes Connection:

III. CONCLUSION

To facilitate the collection of useful aggregate statistics in mobile sensing without leaking mobile users' privacy, we proposed a new privacy-preserving protocol to obtain the Sum aggregate of time-series data. The protocol utilizes additive homomorphic encryption and a novel, HMACbased key management technique to perform extremely efficient aggregation. Implementation-based measurements show that operations at user and aggregator in our protocol are orders of magnitude faster than existing work. Thus, our protocol can be applied to a wide range of mobile sensing systems with various scales, plaintext spaces, aggregation loads, and resource constraints. Based on the Sum aggregation protocol, we also proposed two schemes to derive the Min aggregate of time-series data. One scheme can obtain the accurate Min, while the other one can obtain an approximate Min with provable error guarantee at much lower cost. To deal with dynamic joins and leaves, we proposed a scheme that utilizes the redundancy in security to reduce the communication cost for each join and leave. Simulation results show that our scheme has much lower communication overhead than existing work.

REFERENCES

[1] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin, M. Hansen, E. Howard, R. West, and P. Boda, "Peir, the Personal Environmental Impact Report, As a Platform for Participatory Sensing Systems Research," Proc. ACM/USENIX Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '09), pp. 55-68, 2009.

[2] A. Thiagarajan, L. Ravindranath, K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, and J. Eriksson, "VTrack: Accurate, Energy-Aware Road Traffic Delay Estimation Using Mobile Phones," Proc. ACM Seventh Conf. Embedded Networked Sensor Systems (SenSys '09), pp. 85-98, 2009.

[3] S. Consolvo, D.W. McDonald, T. Toscos, M.Y. Chen, J. Froehlich, B. Harrison, P. Klasnja, A. LaMarca, L. LeGrand, R. Libby, I. Smith, and J.A. Landay, "Activity Sensing in the Wild: A Field Trial of Ubifit Garden," Proc. SIGCHI Conf. Human Factors in Computing Systems (CHI '08), pp. 1797-1806, 2008.

[4] J. Hicks, N. Ramanathan, D. Kim, M. Monibi, J. Selsky, M. Hansen, and D. Estrin, "AndWellness: An Open Mobile System for Activity and Experience Sampling," Proc. Wireless Health, pp. 34- 43, 2010.

[5] N.D. Lane, M. Mohammod, M. Lin, X. Yang, H. Lu, S. Ali, A. Doryab, E. Berke, T. Choudhury, and A. Campbell, "Bewell: A Smartphone Application to Monitor, Model and Promote Wellbeing," Proc. Fifth Int'l ICST Conf. Pervasive Computing Technologies for Healthcare, 2011.

[6] V. Rastogi and S. Nath, "Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption," Proc. ACM SIGMOD Int'l Conf. Management of Data, 2010.

[7] E. Shi, T.-H.H. Chan, E. Rieffel, R. Chow, and D. Song, "Privacy- Preserving Aggregation of Time-Series Data," Proc. Network and Distributed System Security Symp. (NDSS '11), 2011.

[8] T.-H.H. Chan, E. Shi, and D. Song, "Privacy-Preserving Stream Aggregation with Fault Tolerance," Proc. Sixth Int'l Conf. Financial Cryptography and Data Security (FC '12), 2012.

[9] E.G. Rieffel, J. Biehl, W. van Melle, and A.J. Lee, "Secured Histories: Computing Group Statistics on Encrypted Data While Preserving Individual Privacy," http://arxiv.org/abs/1012.2152, 2010.

[10] P.-A. Fouque, G. Poupard, and J. Stern, "Sharing Decryption in the Context of Voting or Lotteries," Proc. Fourth Int'l Conf. Financial Cryptography (FC '00), pp. 90-104, 2000.

[11] MNDOLI, "Mnosha Permissible Exposure Limits," http:// www.dli.mn.gov/OSHA/PDF/pels.pdf, 2013.

[12] S.B. Eisenman, E. Miluzzo, N.D. Lane, R.A. Peterson, G.-S.Ahn, and A.T. Campbell, "The Bikenet Mobile Sensing System for Cyclist Experience Mapping," Proc. ACM Fifth Int'l Conf. Embedded Networked Sensor Systems (SenSys '07), pp. 87-101, 2007.

