International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com
UGC Approved Journal No: 45483
Volume 8, Issue3 Pages 31-33

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

EFFICIENT AUTHENTICATION FOR MOBILE AND PERVASIVE COMPUTING

[1]Dr.Muntha Raju,[2]Mr. Mohd Mohammed Ali, [3]Ms. Gazala Begum
[1]Professor, [2]Associate Professor, [3]Assist professor
[1,2,3] Dept of CSE, Shadan College of Engg & Tech

ABSTRACT- An application in which messages that need to be exchanged are short and both their privacy and integrity need to be preserved, rely on the existence of small devices that can exchange information and form communication networks. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. In this, two narrative techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more efficient than any message authentication code in the literature. The key idea behind the proposed techniques is to utilize the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using standalone authentication primitives.

Keywords: Pervasive, Primitives

1. INTRODUCTION

Preserving the integrity of messages exchanged over public channels is one of the classic goals in cryptography and the literature is rich with message authentication code (MAC) algorithms that are designed for the sole purpose of preserving message integrity. Based on their security, MACs can be either unconditionally or computationally secure. Unconditionally secure MACs provide message integrity against forgers with unlimited computational power. On the other hand, computationally secure MACs are only secure when forgers have limited computational power. We utilize the fact that the message to be authenticated is also encrypted, with any secure encryption algorithm, to append a short random string to be used in the authentication process. Since the random strings used for different operations are independent, the authentication algorithm can benefit from the simplicity of unconditional secure authentication to allow for faster and more efficient authentication, without the difficulty to manage one-time keys.

2. LITERATURE REVIEW

The Auto-ID Center is developing low-cost radio frequency identification (RFID) based systems with the initial application as next generation bar-codes. We describe RFID technology, summarize our approach and our research, and most importantly, describe the research opportunities in RFID for experts in cryptography and information security. The common theme in low-cost RFID systems is that computation resources are very limited, and all aspects of the RFID system are connected to each other. Understanding these connections and the resulting design trade-offs is an important prerequisite to effectively answering the challenges of security and privacy in low-cost RFID systems.
In cryptography, secure channels enable the confidential and authenticated message exchange between authorized users. A generic approach of constructing such channels is by combining an encryption primitive with an authentication primitive (MAC). In this work, we introduce the design of a new cryptographic primitive to be used in the construction of secure channels. Instead of using general purpose MACs, we propose the employment of special purpose MACs, named \E-MACs". The main motive behind this work is the observation that, since the message must be both encrypted and authenticated, there can be a redundancy in the computations performed by the two primitives.

International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395
Research Paper
Available online at: www.jrrset.com
UGC Approved Journal No: 45483

If this turned out to be the case, removing such redundancy will improve the efficiency of the overall construction. In addition, computations performed by the encryption algorithm can be further utilized to improve the security of the authentication algorithm. In this work, we show how E-MACs can be designed to reduce the amount of computations required by standard MACs based on universal hash functions, and show how E-MACs can be secured against key-recovery attacks.

Message authentication codes (MACs) based on universal hash-function families are becoming increasingly popular due to their fast implementation. In this paper, we investigate a family of universal hash functions that has been appeared repeatedly in the literature and provide a detailed algebraic analysis for the security of authentication codes based on this universal hash family. In particular, the universal hash family under analysis, as appeared in the literature, uses operation in the finite field. No previous work has studied the extension of such universal hash family when computations are performed modulo a non-prime integer n. In this work, we provide the first such analysis. We investigate the security of authentication when computations are performed over arbitrary finite integer rings Zn and derive an explicit relation between the prime factorization of n and the bound on the probability of successful forgery. More specifically, we show that the probability of successful forgery against authentication codes based on such a universal hash-function family is bounded by the reciprocal of the smallest prime factor of the modulus n. This thesis report seeks to study and analyze in-depth regarding various medium access control (MAC) layer algorithms and protocols that have been implemented and proposed

for wireless networks. Theory begins with a short overview of basic MAC algorithms used in wired networks as well as some problems appear when these algorithms used for wireless medium access control layer. This Recommendation specifies a message authentication code (MAC) algorithm that is based on a symmetric key block cipher. This cipher-based MAC is abbreviated CMAC, analogous to the abbreviation for the hash function-based MAC, HMAC, that is standardized in FIPS Pub.198. CMAC may be appropriate for information systems in which an approved block cipher is more readily available than an approved hash function.

3. EXISTING SYSTEM

If the authenticated message must also be encrypted, existing MACs are not designed to utilize the functionality that can be provided by the underlying encryption algorithm. MACs are designed for the general computer communication systems, independently of the properties that messages can possess.

4. PROPOSED SYSTEM

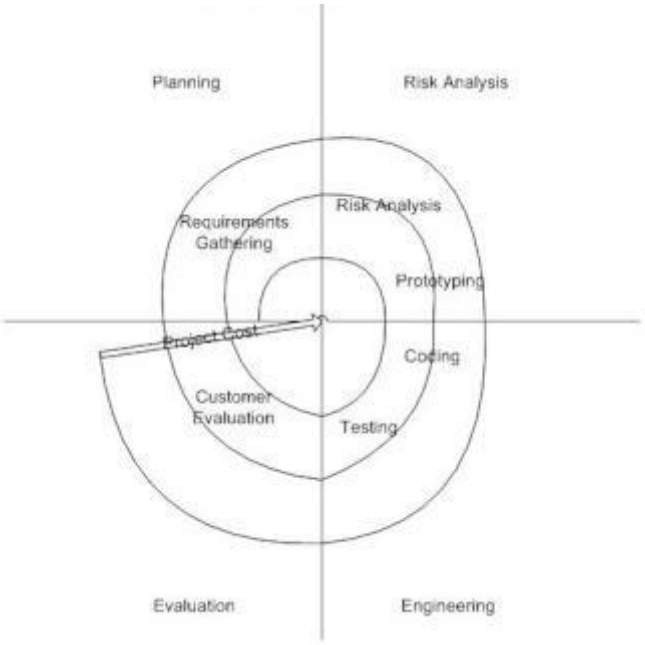
The Novelty of the proposed scheme is to utilize the encryption algorithm to deliver a random string and use it to reach the simplicity and efficiency of one-time pad authentication without the need to manage impractically long keys. Messages are relatively short, addition and modular multiplication can be performed faster than existing computationally secure MACs. This methodology is more simplicity and efficiency than regular MACs. The spiral model is similar to the incremental model, with more emphasis placed on risk analysis. The spiral model has four phases: Planning, Risk Analysis, Engineering and Evaluation. A software project repeatedly passes through these phases in iterations (called Spirals in this model). The baseline spiral, starting in the planning phase, requirements are gathered and risk is assessed. Each subsequent spirals builds on the baseline spiral.

- **Planning Phase:** Requirements are gathered during the planning phase. Requirements like ‘BRS’ that is ‘Bussiness Requirement Specifications’ and ‘SRS’ that is ‘System Requirement specifications’.
- **Risk Analysis:** In the risk analysis phase, a process is undertaken to identify risk and alternate solutions. A prototype is produced at the end of the risk analysis phase. If any risk is found during the risk analysis then alternate solutions are suggested and implemented.

International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395
Research Paper
Available online at: www.jrrset.com
UGC Approved Journal No: 45483

- **Engineering Phase:** In this phase software is developed, along with testing at the end of the phase. Hence in this phase the development and testing is done.
- **Evaluation phase:** This phase allows the customer to evaluate the output of the project to date before the project continues to the next spiral.

Diagram of Spiral model:



3. CONCLUSION

The fact that the message to be authenticated must also be encrypted is used to deliver a random nonce to the intended receiver via the cipher text. This allowed the design of an authentication code that benefit from the simplicity of unconditionally secure authentication without the need to manage one-time keys.

REFERENCES

1. L. Carter and M. Wegman, "Universal Hash Functions," J. Computer and System Sciences, vol. 18, no. 2, pp. 143-154, 1979.
2. T. Helleseth and T. Johansson, "Universal Hash Functions from Exponential Sums over Finite Fields and Galois Rings," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96), pp. 31-44, 1996.
3. V. Shoup, "On Fast and Provably Secure Message Authentication Based on Universal Hashing," Proc. 16th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '96), pp. 313-328, 1996.S
4. B. Alomair, A. Clark, and R. Poovendran, "The Power of Primes: Security of Authentication Based on a Universal Hash-Function Family," J. Math. Cryptology, vol. 4, no. 2, 2010.
5. B. Alomair and R. Poovendran, "E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels," IEEE Trans. Computers, 2012.
6. Federal Information Processing Standards (FIPS) Publication 113, Computer Data Authentication, FIPS, 1985.
7. ISO/IEC 9797-1:1999 Standard, Information Technology – Security Techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms Using a Block Cipher, ISO/IEC, 1999.
8. M. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," 2005.
9. T. Iwata and K. Kurosawa, "OMAC: One-Key CBC MAC," Proc. Int'l Conf. Fast Software Encryption (FSE '03), pp. 129-153, 2003.
10. M. Bellare, R. Guerin, and P. Rogaway, "XOR MACs: New Methods for Message Authentication Using Finite Pseudorandom Functions," Proc. 15th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '95), pp. 15-28, 1995.