THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-10-November-2019

Data Security

[1]Dr.S.Vetrivel, Assistant Professorand [2]Ms.L.Sugirtha
[1] Assistant Professor, St.Joseph Arts & Science College
[2]Research Scholar, St.Joseph Arts & Science College
sugi1087@gmail.com

Abstract:

Past research in the field of cryptography has not given much consideration to arithmetic coding as a feasible encryption technique, with studies proving compression-specific arithmetic coding to be largely unsuitable for encryption. Nevertheless, adaptive modeling, which offers a huge model, variable in structure, and as completely as possible a function of the entire text that has been transmitted since the time the model was initialized, is a suitable candidate for a possible encryption-compression combine. The focus of the work presented in this paper has been to incorporate recent results of chaos theory, proven to be cryptographically secure, into arithmetic coding, to devise a convenient method to make the structure of the model unpredictable and variable in nature, and yet to retain, as far as is possible, statistical harmony, so that compression is possible. A chaos-based adaptive arithmetic coding-encryption technique has been designed, developed and tested and its implementation has been discussed. For typical text files, the proposed encoder gives compression between 67.5% and 70.5%, the zeroth-order compression suffering by about 6% due to encryption, and is not susceptible to previously carried out attacks on arithmetic coding algorithms.

Introduction

The IDEA of combining data compression with encryption of data is a useful one since, in addition to an optimization of storage space required and transmission times needed, compression leads to a decrease in the redundancy in the plaintext, which makes the data more resistant to statistical methods of cryptanalysis. Nevertheless, incorporating cryptographic features in a compression algorithm is a difficult exercise and often leads to a compromise between the amount of compression achieved and the amount of security incorporated. Also, computational resources today allow the cryptanalyst to carry out organized attacks with much success, and the time required to carry out brute force attacks, too, has been greatly reduced. From a strong cryptographicpoint of view, the security of data should be based on an

algorithm where brute force attack has a minimum of 2128 choices in the search space. Robust algorithms, promising sufficient data security, are, therefore, an ever-recurring need.

Continuous Threat Management

1. Adaptive defense, predictive defense, prevention technology to be ready for timely incident response.We call this continuous threat management. Visibility into how the hacker got in, how they moved, and attack replay so you can build a predictive defense. Even then hackers will get through. How can we use automation and information sharing to prevent future attacks? Engagement-based solutions do not miss what the attacker is doing.
2. Open source product that reverse-engineers and unpacks firmware images so you can see the vulnerabilities.

Some commercial tools that audit source code give a false sense of security because nothing is being checked after compilation. There are techniques for sanitizing malicious inputs. Use known libraries to create a secure environment.

3. Use tools that provide virtual patching while the developing is fixing the problem. The least effective technique is blacklisting since there are too many hacks to list and keep track of.
4. Data-driven approach with centralized data collection with monitoring and triggered alerts.

ISSN:0971-1260

Vol-22-Issue-10-November-2019

5. Unified threat management, firewalls, and analyze data in real time. We get a vast amount of data from our own enterprise in a central repository. Run advanced analytics before the incident becomes problematic. Process and analyze data in real time. According to Cyber security Ventures, the cost of cybercrime will be $6 trillion by 2021.
6. Multi-layer, rapid detection and response for prevention.

   Some people think firewall or network security for prevention is equivalent to a flu shot; however, you can still get the flu. You must be equally prepared for when the attack is successful to prevent breaches from having a material impact on the business. Some breaches will spend 100 to 150 days accessing different areas of your network. We're able to reduce this by 85%-95% by identifying and tracking the intruder and stopping them before they can have a material impact. It takes the attacker time to move laterally to imprint and find the ideal time for the exfiltration of data. Most attacks don't exfiltrate for 30 to 60 days. We're able to see the behavior and address it.
7. Real-time ingestion and visualization: to track the intruder as they move in and around the network.
8. Leverage the same building blocks or micro services and containers to enable more scalable, automated, and secure apps.

   Detection moves from signature to scalable analytics. Move from rule-based and adapt to changes in the environment. More flexible adapting to a variety of workloads without concerns with threat vectors up front.

THE ENCRYPTION PROCESS

1) Transform the file into binary sequences and divide the sequence containing 'n' bits in each block. The value of 'n'is a Secret Key.
2) Generate the first pseudorandom sequence of numbers and modulate the sequence by 3 to select any of the three crossover operations, from that sequence we can select:
0. Single point
1. Uniformed
2. Two point
The crossover operation will be applied on each block of binary digits.
3) Generate another pseudorandom sequence of numbers and modulate the sequence with a secret key (range from16-255)
We denote the sequence as:
Z1, Z2, Z3….Zn
Find out the decimal value of each crossover blocks i.e.:
C1, C2, C3….Cn
Now do the following operation,
Xi=ZiZi<< (n/2)
Ei=Ci Xi, i=i+1 (i = 1, 2, 3, 4…n)
4) Repeat step 3 until end of the data.
5) Now between E1, E2, E3….En block select a block for mutation. Perform mutation operation on the mentioned block, the number will be then saved into the key file,
Ei = (255-Ei)
i.e. the encrypted block looks like:
E1, E2,(255-E3),….En.
6) By printing the E1, E2, E3…., En values into a file (any file format) we can get our cipher text.

THE DECRYPTION PROCESS

The steps for decryption are just reversal of the encryption process.
1) Read the key file and read the values form reverse direction. Read the encrypted text file to get the encrypted text and divide it into 'n' bit per sequence mentioned in the key.

2) (Mutation) Do Mutation of the mentioned block number in the key:Ei =255-(255-Ei)

3) Generate a pseudo random sequence and modulate the sequence with the secret key,
We denote the sequence as:
Z1, Z2, Z3….Zn
Find out the decimal value of each crossover blocks i.e.:
E1, E2, E3…. En
Now do the following operation,
Xi=ZiZi<< (n/2)
Ci=Ei Xi, i=i+1 (i = 1, 2, 3, 4…n)

EXPERIMENTAL RESULTS

In our experiment over the algorithm for the pseudorandom sequence we are here using Blum

ISSN:0971-1260

Vol-22-Issue-10-November-2019

BlumShub PRNG which provides a strong security proof.

Encryption:

Consider a simple text file – **Narula**
1) Binary equivalent of this text is-
01001110011000010111001001110101011011000110000
Length is: 48
2) Now, we divide the binary string into 6 blocks with
8byte/ block.
• *8 is the 1st key value.*
B1=01001110 B2=01100001
B3=01110010 B4=01110101
B5=01101100 B6=01100001
3) Now by generating a pseudorandom sequence and modulate the value to 3 we get the sequence:
0 2 2 2 1
So, for the crossover between B1 & B2, 0th operation *single point crossover* being selected,
B1=0100 1110 B2=0110 0001
C1=0100 0001 B2=0110 1110
C1 will store as crossover string.
B2= 01 101 110 B3=01 110 010
C2= 01 110 110 B3=01 101 010
C2 will store as crossover string.
After the crossover process is being finished, the crossover string will look like:
C1= 01000001 C2= 01110110
C3 = 01110010 C4= 01101101
C5 = 01101101 C6= 01100000
4) Generate the next pseudorandom sequence by using the prime values.
By using secret key value modulation of the sequence will become:
Z1=78 Z2=60 Z3=114
Z4=159 Z5=108 Z6=144
By finding decimal value of each block we get ,
C1=65 C2=118 C3=114
C4=109 C5=109 C6= 96
Now perform the following operation,
X1=78 78<<4
E1= 65 X1
Z2=60 60<<4
E2= 118 X2
After finishing the operation, We get,
E1=1263 E2=906 E3=1824
E4=2306 E5=1729 E6=2544
5) Perform mutation operation on the 4th block which is a secret key,
E4 = (255-2306) = -2051
After finishing the operation we get,
E1=1263 E2=906 E3=1824
E4=-2051 E5=1729 E6=2544
6) Finally transforming E1, E2, E3, E4, E5, and E6 into character & putting it into a file we get:
Encrypted String: **ïŠýÁð**

STANDARDS FOR SECURE NETWORKING

To ensure a consistent set of requirements, lower training costs and speed the introduction of new security capabilities, IT managers should use these 10 security techniques across their networks.

1. Use a layered defense. Employ multiple complementary approaches to security enforcement at various points in the network, therefore removing single points of security failure.

2. Incorporate people and processes in network security planning.

Employing effective processes, such as security policies, security awareness training and policy enforcement, makes your program stronger. Having the people who use the network (employees, partners and even customers) understand and adhere to these security policies is critical.

3. Clearly define security zones and user roles. Use firewall, filter and access control capabilities to enforce network access policies between these zones using the least privileged concept. Require strong passwords to prevent guessing and/or machine cracking attacks, as well as other strong forms of authentication.

4. Maintain the integrity of your network, servers and clients. The operating system of every network device and element management system should be hardened against attack by disabling unused services. Patches should be applied as soon as they become available, and system software should be regularly tested for viruses, worms and spyware.

ISSN:0971-1260

Vol-22-Issue-10-November-2019

5. Control device network admission through endpoint compliance. Account for all user device types -- wired and wireless. Don't forget devices such as smart phones and handhelds, which can store significant intellectual property and are easier for employees to misplace or have stolen.

6. Protect the network management information. Ensure that virtual LANs (VLAN) and other security mechanisms (IPSec, SNMPv3, SSH, TLS) are used to protect network devices and element management systems so only authorized personnel have access. Establish a backup process for device configurations, and implement a change management process for tracking.

7. Protect user information. WLAN/Wi-Fi or Wireless Mesh communications should use VPNs or 802.11i with Temporal Key Integrity Protocol for security purposes. VLANs should separate traffic between departments within the same network and separate regular users from guests.

8. Gain awareness. Network traffic, threats and vulnerabilities for each security zone, presuming both internal and external threats. Use antispoofing, bogon blocking and denial-of-service prevention capabilities at security zone perimeters to block invalid traffic.

9. Use security tools to protect from threats. Guarantee performance of critical applications. Ensure firewalls support new multimedia applications and protocols, including SIP and H.323.

10. Log, correlate and manage security and audit event information. Aggregate and standardize security event information to provide a high-level consolidated view of security events on your network. This allows correlation of distributed attacks and a network widevcv awareness of security status and threat activity.

STRATEGY

- A strategy is more important than tools and techniques. Every tool has its own limitations and it needs multiple tools. Design, check model, code analysis, dynamic testing, compliance testing. We automate with Jenkins and send issues to JIRA. Auditing is key.
- Security by design. Companies are worried about how much money they can raise from V.C.'s, building the best game, collecting and selling consumer analytics. The C-level needs to be thinking about security first and understand that the lack of consumer privacy will backfire. Google acquired AdMob which reallocates consumers without their permission. There will be a backlash regarding creep ware. Face book was calling the GPS function every second. Apple asked them to stop because it was wearing down iPhone batteries.

- Provide security professionals with continuous integration tools like Jenkins to automate security tasks. Use DevOps tools to allow security professionals to get more done in less time. The pitfall is when looking to solve problems it don't look at how it fits with the overall strategy. Look at how the tool fits into the entire practice. If the tool requires a person to run it, it cannot be automated. We need the tool to be a process enable rather than the other way around.

SYMMETRIC KEY

Symmetric proteins are ideal objects to investigate protein evolution and folding. It is generally accepted that symmetric proteins have been arisen from gene duplications and fusion. However, these repetitive or symmetric signals were almost lost in their sequences during evolution but remain in their structures. Investigating how these proteins keep their symmetric structures by "asymmetric" sequences is a way to understand protein evolution and folding. On the other hand, understanding the building principle of symmetric proteins is also necessary for designing de novo proteins, because symmetric structures are relatively simple to be built from basic units. One solution to the problem above is that protein sequences may contain hidden symmetric signals that

ISSN:0971-1260

Vol-22-Issue-10-November-2019

determine their symmetric structures. Recently, the hidden symmetric signals might be contributed by a small number (about 30%) of identical or key residues.

Conclusion and Scope for future development:

The International Telecommunication Union and Alliance for Telecommunications Industry Solutions provide standards that enterprises can use in their vendor selection process. However, no single set of technologies is appropriate for all organizations. Regardless of the size of the organization or the depth of the capabilities required, secure networking must be an inherent capability, designed into the DNA of every product. By following the steps described above, companies will have the right approach for securing their increasingly mobile, converged networks. In fact an efficient encryption and decryption process to provide more and apposite security for a message. The intruder or a hacker may find lots of difficulties to fine the original message even if he intrudes into the communication process. Apart from Fibonacci, prime and factorial number series the sender can use any other number series like sine, cosine, tan etc to decode and encode the information in a communication channel.

References:

[1]. William Stallings, “Cryptography and Network Security – Principles and Practices”, Pearson Education, Third Edition, 2005.
[2]. Andrew S. Tenenbaum, “Computer Networks”, Prentice Hall, Fourth Edition, 2003.
[3]. Behrouz A. Forouzan, “Cryptogarphy and Network Security” Tata Mcgraw Hill, Fourth Editon, 2005.
[4]. Douglas Robert Stinson,” Cryptography and Network Security – Theory and Practice”, CRC Press, Third Edition, 2006.
[5]. Stuart McClure, Joel Scambray, George Kurtz,” Hacking Exposed: Network Security Secrets and Solutions” McGraw Hill, Fourth Edition, 2003.
[6]. GerdE.Keiser,” Local Area Networks” Tata McGraw Hill, 2001.
[7]. Ferguson, NeilsSchneier and Bruce,” Practical Cryptography” Wiley Publisher, Mrach 2003 Edition.
[8]. Burnett, Steve Paine and Stephen,” RSA Security’s Official Guide to Cryptography”, Tata McGraw Hill, March 2001 Edition.
Journals and Websites:
[9]. M. Bellare, T. Kohno and V. Shoup,” Stateful Public-Key Cryptosystems: How to Encrypt with One 160-bit Exponentiation”, Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), ACM, 2006.
[10]. M. Bellare and T. Kohno,” Hash function balance and its impact on birthday attacks”, Advances in Cryptology - Eurocrypt 2004 Proceedings, Lecture Notesin Computer Science Vol. 3027, C. Cachin and J. Camenischeds, Springer-Verlag, 2004.
[11]. M. Blaze, J. Ioannidis and A. Keromytis. "DSA and RSA Key and Signature Encoding for the KeyNote Trust Management System." RFC-2792. IETF, March 2000.
[12]. A. Biryukov and A. Shamir,” Real Time Cryptanalysis of the Alleged A5/1 on a PC”, Preliminary Draft, December 09, 1999.