BLOCKING MISBEHAVING USERS IN CROSS DOMAIN NETWORK

[1]Shapna.E,[2]K.Kavitha.

[1]Research Scholar,Department of Computer Science, Hindusthan College Of Engineering And Technology,Coimbatore
[2]Assistant Professor, Department of Computer Science, Hindusthan College Of Engineering And Technology,Coimbatore

Abstract: Network reachability is a necessary attribute for accepting end-to-end network behavior and helps in detect violation of security policies across the network. While quantify network reach ability within one organizational domain is a difficult problem in itself performing the same computation across a network spanning multiple organizational domains presents a novel challenge. The problem of quantifying network reach ability across multiple organizational domains is more difficult because the privacy of security policies of individual domains is a serious concern and needs to be protected through this process. Here proposed the first cross-domain privacy-preserving protocol for quantifying network reach ability. In this protocol constructs equivalent representations of the Access Control List (ACL) rules and determines network reach ability while preserving the privacy of the individual ACLs. This protocol can accurately determine the network reach ability along a network path through different administrative domains. Have implemented and evaluated our protocol on both real and synthetic ACLs. The experimental results show that the online processing time of an ACL containing thousands of rules is less than 25 s. Given two ACLs each containing thousands of rules the comparison time is less than 6 s and the total communication cost is less than 2100 kB.

1. INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication.

To our best knowledge, no prior work has addressed the problem of privacy-preserving network reach ability quantification. Keeping the reach ability restriction information private is important for two reasons. First, such information is often misconfigured and has security holes that can be exploited by attackers if it is disclosed. In reality, most firewall policies have security holes. Disclosing ACLs allows attackers to analyze and utilize the vulnerabilities of subnets along a given path.

The disadvantages are current practice of determining network reach ability through probing has two major drawbacks. First, probing is expensive because it needs to generate and send a significant amount of probe packets. Second, probing is inaccurate, e.g., it cannot probe the open ports with no server listening on them.

Proposed the first privacy-preserving protocol for quantifying network reach ability for a given network path across multiple domains. Our protocol consists of three phases: ACL preprocessing, ACL encoding and encryption and ACL comparison.

In the first phase transform all the ACLs into an equivalent representation, firewall decision diagram (FDD) and then extract the non-overlapping rules with accept decisions.

In the second phase, to perform privacy-preserving comparison, we reduce the problem to that of computing privacy-preserving intersection of two numerical ranges. Accordingly first transform the rules, which are represented as ranges into a sequence of prefix numbers and then encrypt these numbers with secret keys of different parties. This phase enables different parties to compute the intersection of non-overlapping rules in their ACLs without revealing these rules.

In the third phase the destination ACL computes the intersection of its non-overlapping rules with the rules from its adjacent ACL, and then the adjacent ACL further repeats this computation with its adjacent ACL

until the source ACL is reached. Finally all the ACLs collaboratively decrypt the encrypted intersection of the non-overlapping rules but only the first party (with the source ACL) obtains the result. To reduce the computation and communication cost, we use the divide-and-conquer strategy to divide the problem of computing reach ability of ACLs to the problem of computing reach ability of three ACLs. The initial intersection is performed among the rules of three adjacent ACLs that are located in a sequence along the network path. Subsequent comparisons are grouped in a similar manner, i.e., the intersection of three ACLs can be treated as a new ACL, and the process is repeated among three new ACLs. This optimization technique reduces the number of ACL encryptions and the number of messages in our protocol from $O(n^2)$to O(n).
There are four key challenges in the privacy-preserving quantification of network reach ability.

It is computationally expensive. An ACL may consist of many rules, and each rule consists of multiple fields. Therefore, comparing multiple ACLs with a large number of rules can be quite expensive, even if only a few ACLs are involved in the process. Furthermore, the complexity of comparison can be expensive due to overlapping rules resulting in many comparisons.
Protecting the privacy of the ACL rules is crucial. Since a rule has to be sent to other parties to enable comparison, it is necessary to propose a protocol that will not reveal the rule but still allows the different ACLs to calculate the intersection.

Communication cost is high as even calculating the intersection of a small number of ACLs is a tedious process and requires a number of messages to be exchanged among different parties.

Computing the reach ability information when ACLs are updated is an important performance-related issue. It is necessary to explore optimization approaches in such scenarios without sacrificing the privacy of individual ACLs.

2. **RELATED WORK**

A Quantitative study of firewall configuration errors Computer used Once a company acquires a firewall a systems administrator must configure and manage it according to security policy that meets the company's needs.

Configuration is a crucial task probably the most important factor in the security a firewall provides. The Algorithmic Security is used a network security company that he cofounded. The limitations are Plug flow reactors have a high volumetric unit conversion, run for long periods of time without maintenance and the heat transfer rate can be optimized by using more thinner tubes or fewer, thicker tubes in parallel. The Advantages are CSTRs (Continuous Stirred Tank Reactor) and PFRs have fundamentally different equations, so the kinetics of the reaction being undertaken will to some extent determine which system should be used.
Efficient private matching and set present protocols based on the use of ho- mom orphic encryption and balanced hashing, for both semi-honest and malicious environments. For lists of length k, obtain O(k) communication overhead and O(k ln ln k) computation. The protocol for the semi honest environment is secure in the standard model, while the protocol for the malicious environment is secure in the random oracle model. The computing exponentiations algorithm is used. The limitations are immaturity, Reliance on third-party illuminators, Complexity of deployment. The Advantages are Lower procurement cost, Lower costs of operation and maintenance, due to the lack of transmitter and moving parts , Covert operation, including no need for frequency allocations.
Firewall design: Consistency, completeness and compactness A rewall is often placed at the entrance of each private network in the Internet. The function of a rewall is to examine each packet that passes through the entrance and decide whether to accept the packet and allow it to proceed or to discard the packet. Are wall is usually designed as a sequence of rules. FDD algorithm is used. The limitations are All logics are for representing proofs, including propositional logic. The higher the order of the
logic, the more powerful it is in the sense of its language being more expressive and its deduction being more general. The Advantages are Less powerful logic is that it is easier to reason about, and that it is tends to

be easier to write algorithms for, in the sense that (depending on what the algorithm is intended to do) these algorithms will tend to be more complete and/or efficient and/or to terminate (e.g. algorithms for proving statements in the logic). The advantage of a more powerful logic is that it is more expressive and thus capable of representing and/or proving more of mathematics. SANE: A protection architecture for enterprise networks Connectivity in today's enterprise networks is regulated by a combination of complex routing and bridging policies, along with various interdiction mechanisms such as ACLs, packet filters and other middle boxes that attempt to retrofit access control onto an otherwise permissive network architecture. This leads to enterprise network that are inflexible, fragile, and difficult to manage. The MST algorithm has the property that no switch learns the network topology nor is the topology reproducible from packet traces Advantages Flash drives use little power, have no fragile moving parts, and for most capacities are small and light. Data stored on flash drives is impervious to mechanical shock, magnetic fields, scratches and dust. The Limitations are Like all flash memory devices, flash drives can sustain only a limited number of write and erase cycles before the drive fails.

Structured firewall designs It addresses the completeness problem because the syntactic requirements of a firewall decision diagram force the designer to consider all types of traffic. It also addresses the compactness problem because in the second step we use two algorithms (namely FDD reduction and FDD marking) to combine rules together, and one algorithm (namely firewall compaction)to remove redundant rules. Moreover, the techniques and algorithms presented in this paper are extensible to other rule-based systems such as IP sec rules. Distance vector algorithm is used. The advantage of such representation will become evident when combining several IDDs. The main problem with fuzzing to find program faults is that it generally only finds very sim.

Collaborative enforcement of firewall policies in virtual private networks On real-life firewall policies, for processing packets our experimental results show that Vguard is 552 times faster than CDCF on one party and 5035 times faster than CDCF on the other party. The algorithm for converting a firewall to an FDD. The Advantages are Exchange large volumes of data using Electronic Data Interchange (EDI), Share product catalogs exclusively with trade partners. The Limitations are Extranets can be expensive to implement and maintain within an organization (e.g., hardware, software, employee training costs), if hosted internally rather than by an Application Service Provider. Security of extranets can be a concern when hosting valuable or proprietary information. Unraveling the complexity of network management Its develop a suite of complexity models that describe the routing design and configuration of a network in a succinct fashion, abstracting away details of the underlying configuration languages. Our models, and the complexity metrics arising from them, capture the difficulty of configuring control and data plane behaviors on routers. Our algorithms automatically identify roles by finding routers that share similar configurations. The Advantages are Management of distributed data with different levels of transparency like network transparency, fragmentation transparency, replication transparency, etc. Increase reliability and availability. The limitation is Analysis of distributed data.

Efficient and secure protocols for privacy-preserving set operations The Fast one secure against the active adversary. Our constructions of NIZK have independent interest in that, though also mentioned as building blocks, the previous work did not illustrate how to construct them. We construct these NIZK with an additional non-malleable property, the same complexity as claimed in the previous work, and also an improvement on the communication complexity. The Algorithms are Probabilistic Polynomial-Time is algorithm is used. One advantage of is that we no longer need the two extra initial messages. The Limitations are Migration addresses the possible obsolescence of the data carrier, but does not address the fact that certain technologies which run the data may be abandoned altogether, leaving migration useless.

Privacy- preserving cross- domain network reachability quantification have implemented and evaluated our protocol on both real and synthetic ACLs. The experimental results show that the online processing time of an ACL with thousands of rules is less than 25 seconds, the comparison time of two ACLs is less than 6 seconds and the communication cost between two ACLs with thousands of rules is less than 2100 KB. The Pohlig-Hellman algorithm. this algorithm is used. The Advantages are Streamlines the supply chain from point of origin to point of sale. Reduces labor costs through less inventory handling. The Limitations are Potential partners may not have the necessary storage capacities. An adequate transport fleet is needed to operate.

SplitX: High-performance private analytics Presents SplitX, a high- performance analytics system for making differentially private queries over distributed user data. SplitX is typically two to three orders of magnitude more efficient in band-width, and from three to five orders of magnitude more efficient in computation than previous comparable systems, while operating under a similar trust model. Similarly requires an algorithm to determine which data would be safe to contribute a priori. Which translates into an availability benefit, than a standalone encryption scheme? On the other hand encryption is considered more resilient to brute force attacks. The Limitations are An IDA system by design is more resilient to device failure and data loss. With encryption if either the keys or the cipher text is lost the data will be unrecoverable.

Cross-domain privacy-preserving cooperative firewall optimization this paper explores inters firewall optimization across administrative domains for the first time. The key technical challenge is that firewall policies cannot be shared across domains because a firewall policy contains confidential information and even potential security holes, which can be exploited by attackers. In this paper, we propose the first cross-domain privacy-preserving cooperative firewall policy optimization protocol. Specifically, for any two adjacent firewalls belonging to two different administrative domains, our protocol can identify in each firewall the rules that can be removed because of the other firewall. The Pohlig-Hellman algorithm is used. The Advantages are Malicious activity may be identified by the other party using anomaly detection Approaches. It avoids encrypting and sending the duplicate prefixes for each field and, hence, significantly reduces the computation and communication costs. The Disadvantages are No corrupted employees are trying to reveal the private firewall policies of other parties. Condition holds for all the predicates computed from rule r and then rule r is redundant.

3. SYSTEM MODEL

PRIVACY-PRESERVING PROTOCOLS

Similarity join consists of grouping pairs of records whose similarity is greater than a threshold, T. Privacy preserving protocols for similarity join are used to protect the data of two sources from being totally disclosed during the similarity join process. Protocol to perform similarity join using phonetic encodings, which proposed a privacy preserving record matching protocol on both data and schema levels, which concentrated on the e health applications and its intrinsic private nature, Frequency Inverse Document Frequency (TF.IDF) based comparison

function and a secure blocking schema. Other methods concentrated on using encryption to preserve privacy. To our knowledge, the existing privacy preserving protocols for similarity join, concentrated only on the syntax representation of the values, and did not consider the semantic relationships among them. Besides, in our previous work, we showed that the similarity join performance would be improved significantly when using long attributes as join attributes, instead of short attributes. However, the existing secure protocols are used mainly with short attributes.

The term short attribute refers to any attribute of short string data type, whereas the term short string refers to the data type representing any string value of limited length, such as person name, paper title, and address. On the other hand, the term long attribute refers to any attribute of long string data type, whereas the term long string refers to the data type representing any string value with unlimited length, such as paper abstract, movie summary, and user comment.

In addition to the desired effect of improving the similarity join performance by using long attributes, long string attributes contain much more information than short string attributes, and most databases include such attributes. Furthermore, using long attributes can provide some level of privacy. The information to be shared can be written or merged as long strings without the need to include the secure data. In the following, we provide two applications illustrating the motivation to use long attributes in secure similarity join methods.

4. MODULE DESCRIPTION

- **ACL preprocessing**
- **ACL encoding and encryption**
- **ACL comparison**
- **Optimization**

• ACL preprocessing

In the first phase, we transform all the ACLs into an equivalent representation, firewall decision diagram (FDD), and then extract the non-overlapping rules with accept decisions.

• ACL encoding and encryption

In the second phase, to perform privacy-preserving comparison, we reduce the problem to that of computing privacy-preserving intersection of two numerical ranges.

Accordingly first transform the rules, which are represented as ranges, into a sequence of prefix numbers, and then encrypt these numbers with secret keys of different parties. This phase enables different parties to compute the Intersection of non-overlapping rules in their ACLs without revealing these rules.

.

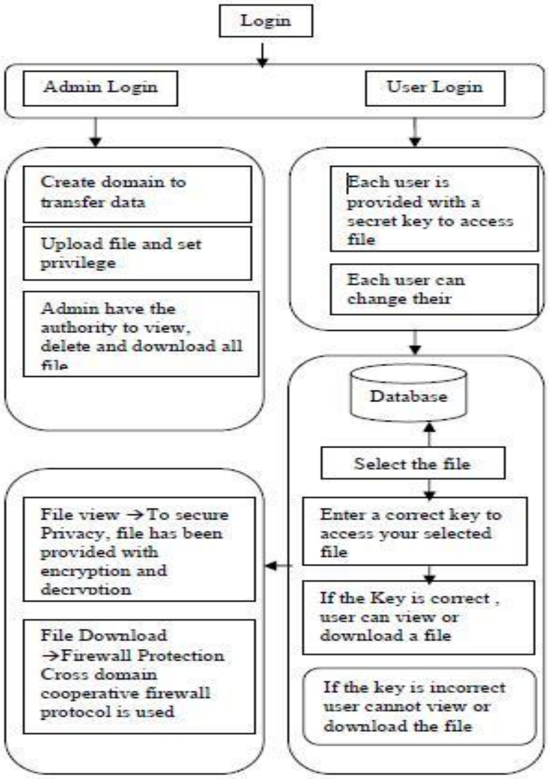
• ACL comparison

In the third phase, the destination ACL computes the intersection of its non-overlapping rules with the rules from its adjacent ACL, and then the adjacent ACL further repeats this computation with its adjacent ACL until the source ACL is reached.

• Optimization

Finally, all the ACLs collaboratively decrypt the encrypted intersection of the non-overlapping rules, but only the first party (with the source ACL) obtains the result. To reduce the computation and communication cost, we use the divide-and-conquer strategy to divide the problem of computing reach ability of ACLs to the problem of computing reach ability of three ACLs. The initial intersection is performed among the rules of three adjacent ACLs that are located in a sequence along the network path. Subsequent comparisons are grouped in a similar manner, i.e., the intersection of three ACLs can be treated as a new ACL, and the process is repeated among three new ACLs. This optimization technique reduces the number of ACL encryptions and the number of messages in our protocol from O(n^2)to O(n).

4.1 DATA FLOW DIAGRAM:


Login
Admin Login
User Login
Create domain to transfer data
Upload file and set privilege
Admin have the authority to view, delete and download all file
Each user is provided with a secret key to access file
Each user can change their
Database
Select the file
Enter a correct key to access your selected file
If the Key is correct , user can view or download a file
If the key is incorrect user cannot view or download the file
File view →To secure Privacy, file has been provided with encryption and decryption
File Download →Firewall Protection Cross domain cooperative firewall protocol is used

5. CONCLUSION

Firewalls are designed to provide access control. We proposed the method Cross Domain cooperative firewall across different administrative domains by using key management, in order to enable a privacy preserving and security. By using this method the security will be increased and controlled and also we can able to provide privacy and security. Need to check Privacy-Preserving Range Comparison. If the rule exists we propose a cross domain cooperative firewall protocol to optimize the network. If the rule does not exist, the network performance collapse and discards due to the entry of third party. Thereby privacy and security fails. To overcome this bug we underwent a study of cross domain cooperative firewall protocol. We implemented our protocol in java and conducted extensive evaluation. The results on real firewall policies show that our protocol can avoid 98% of rules in a firewall.

6. FUTURE WORK

Future work is in order to increase the system accuracy by extending the current protocol. To find out the maximum speed of the packet to be reached. Extending the process used for proxy server. Using V-Guard framework for sending and receiving the packets is very faster.

REFERENCES

[1] 1.A. Wool, “A quantitative study of firewall configuration errors,” Computer, vol. 37, no. 6, pp. 62–67, Jun. 2004.

[2] M. Freedman, K. Nissim, and B. Pinkas, Efficient private matching and set intersection,” in Proc. EUROCRYPT, 2004, pp. 1–19.

[3] M. G. Gouda and A. X. Liu, “Firewall design: Consistency, completeness and compactness,” in Proc. ICDCS, 2004, pp. 320–327.

[4] G. G. Xie et al., “On static reachability analysis of IP networks,” in Proc. IEEE INFOCOM, 2005, pp. 2170–2183

[5] M. Casado et al., “Sane: A protection architecture for enterprise networks,” in Proc. USENIX Security Symp., 2006, pp. 137–151

[6] M. G. Gouda and A. X. Liu, “Structured firewall design,” Comput. Netw. J., vol. 51, no. 4, pp. 1106–1120, 2007.

[7] P. Matousek, J. Rab, O. Rysavy, and M. Sveda, “A formal model for network-wide security analysis,” in Proc. IEEE Int. Conf. Workshop Eng. Comput. Based Syst., 2008, pp. 171–181.

[8] B. Zhang, T. S. E. Ng, and G.Wang, “Reachability monitoring and verification in enterprise networks,” presented at the SIGCOMM, 2008,(poster).

[9] X. Liu and F. Chen, “Collaborative enforcement of firewall policies in virtual private networks,” in Proc. PODC, 2008, pp. 95–104.

[10] T. Benson, A. Akella, and D. Maltz, “Unraveling the complexity of network management,” in Proc. NSDI, 2009, pp. 335– 348.