INTRUSION DETECTION SOLUTION USING ANOMALY DETECTION SCHEME

Ms. Shivani Sharma[1], Mr.Amit Asthana[2], Mr. Manik Chandra Pandey[3]

[1]PG Student, Deptt. Of CSE, Swami Vivekanand Subharti University, (India)
[2,3]Asst. Prof., Deptt. Of CSE, Swami Vivekanand Subharti University, (India)

ABSTRACT

Intrusion detection system (IDS) is a security layer that is used to discover ongoing intrusive attacks and anomaly activities in information systems and is usually working in a dynamically changing environment. Although increasing IDSs are developed in the literature, network security administrators are faced with the task of analyzing enormous alerts produced from the analysis of different event streams. In this paper we present three types of intrusion detection based on the source of detection – host based, network based and hybrid intrusion detection and also focuses on intrusion detection techniques i.e. misuse detection and anomaly detection techniques, supervised and unsupervised based learning based on the different approaches.

Keywords: Intrusion, Attacks, Misuse Detection, Anomaly Detection, Pattern Matching, Neural Network, Data Mining.

I INTRODUCTION

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

The goals of the IDS provide the requirements for the IDS policy. Potential goals include:

- Attack Detection
- Attack Prevention
- Detection of policy violations
- Enforcement of use policies
- Enforcement of connection policies
- Collection of evidence

II TO IDENTIFY THE INTRUSION THE FOLLOWING OPERATION PERFORMS BY IDS PERFORMS

Manual log examination

- Automated log examination
- Host-based intrusion detection software

- Network-based intrusion detection software
- Audit of system structure and fault
- Audit tracing management of operating system and recognition of users behavior against security policy of an organization
- Statistics analysis of abnormal activities
- Monitoring and analyzing user and system activities
- Recognition activity model for identification of known attacks and generating the alarm as an indication of attack
- Measuring the confidentiality and integrity of the system and data files.

2.1 Following are the factors for the measurement of IDS [2].

- **Alarm:** A signal that suggests that a system has been or is being attacked.
- **True Positive:** A legitimate attack which triggers IDS to produce an alarm.
- **False Positive:** An event signaling IDS to produce an alarm when no attack has taken place.
- **False Negative:** A failure of IDS to detect an actual attack.
- **True Negative:** When no attack has taken place on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack
- **Alarm filtering:** The process of categorizing attack alerts produced from an IDS in order to distinguish false positives from actual attacks

III ARCHITECTURAL MODEL

A generic architectural model of a typical intrusion detection system is shown in figure 1 [3]. Typically, IDS uses information existing in audit storage, system configuration decal and system knowledge of previous attacks. IDS may be located in a target system or in a system external to it. In later case, IDS will not be compromised even if the target system is invaded. IDS may use active information for reduction of detection time. Active information includes intermediate system behavior that leads to detecting intrusions. On detecting anomaly, IDS sends alarm to Site Security Officer (SSO). By scheming baseline of normal activities it is feasible to identify any deviations. But this approach mainly depends on correctness of fixing the baseline of user behavior without proper baseline; IDS may generate numerous false alarms. A user activities is termed as normal, provided its current behavior is similar to its earlier behavior that is found safe. A IDS may be manually provided with user's profiles for reference. When an unknown user interacts with the system, the process models the users legal behavior and also updates the model as and when new features in the users activities are identified. This model is included in reference data. When a user's behavior differs with its model, the system puts the user in suspect list.

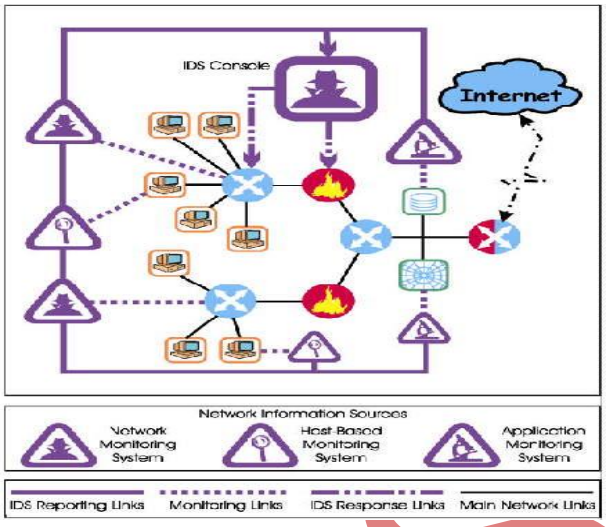


Fig.1

IV TYPES OF INTRUSION DETECTION

4.1 Network Based (Network IDS)

Network based intrusion detection attempts to recognize unauthorized, illegal, and jarring behavior based exclusively on network traffic. A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network. Using the captured data, the IDS system processes and flags any suspicious traffic. Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only assemble, identifying, logging and alerting.

4.2 Host Based (HIDS)

Generally referred to as HIDS, host based intrusion detection attempts to identify unlawful, dishonest, and abnormal behavior on a specific device. HIDS generally involves an agent installed on each system, monitoring and alerting on local OS and application activity. The installed agent uses a combination of signatures, rules, and heuristics to identify unauthorized activity. The role of a host IDS is inactive, only gathering, identifying, sorting, and alerting.

4.3 Physical (Physical IDS)

Physical intrusion detection is the act of identifying threats to physical systems. Physical intrusion detection is most often seen as physical controls put in place to ensure CIA. In many cases physical intrusion detection systems act as avoidance systems as well. Examples of Physical intrusion detections are:

- Security Guards
- Security Cameras
- Access Control Systems (Card, Biometric)
- Firewalls

- Man Traps
- Movement Sensors

V INTRUSION DETECTION TECHNIQUES

5.1 Misuse/Signature-Based Detection

This type of detection engine detects intrusions that follow well-known patterns of attacks (or signatures) that use known software International Journal of Network Security & Its Applications The main restraint to this approach is that it only looks intended for the known weaknesses and may not care about detecting unidentified future intrusions [26]. Misuse Detection Techniques includes genetic algorithm, expert system, pattern matching, state transition study and keystroke monitoring based approaches for the detection of attacks.

- **Genetic Algorithm Based Detection**

There are many researchers who used GAs in IDS to detect malicious intrusion from normal use. The Genetic Algorithm provides the necessary population breeding, randomizing, and statistics gathering functions.

- **Expert System Based Detection**

Expert System is a system of software or combined software and hardware capable of adeptly executing a specific duty usually performed by a human expert. Expert systems are highly specialized computer systems capable of simulating a human specialist's knowledge and reasoning into Knowledge-base and are characterized by a set of facts and heuristic rules. Heuristic rules are rules of thumb accumulated by a human expert through intensive problem solving in the domain of a particular task.

- **State transition based:**

In this approach IDSs try to indentify intrusion by using a finite state machine that deduced from network. IDS states correspond to different states of the network and an event make transit in this finite state machine. An activity identifies intrusion if state transitions in the finite state machine of network reflect to sequel state. The main problem in this technique is to find out known signatures that include all the possible variations of pertinent attack, and which do not match non intrusive activity.

5.2 Anomaly/Statistical Detection

An anomaly based detection engine will search for something rare or unusual [26]. They analyses system event streams, using statistical techniques to find patterns of activity that appear to be abnormal. The primary disadvantages of this system are that they are highly expensive and they can recognize an intrusive behavior as normal behavior because of insufficient data. Anomaly Detection Techniques includes Statistical, Neural Network, Immune System, file checking and Data Mining based approaches for the detection of attacks.

- **Statistical based methods**
  Statistical methods monitor the user/network behavior by measuring certain variables statistics over time [7].

- **Distance based methods**
  These methods try to overcome limitations of statistical outlier detection approach when the data are difficult to estimate in the multidimensional distributions [8].

- **Profile based methods**
  This method is similar to rule based method but in this type profile of normal behavior is built for different types of network traffics, users, and all devices and deviance from these profiles means intrusion.

- **Signature based**
  Matching available signatures in its database with collected data from activities for identifying intrusions.

- **Neural Network Based**
  This Neural Network model solved normal attack patterns and the type of the attack. When given data was presented to the model.

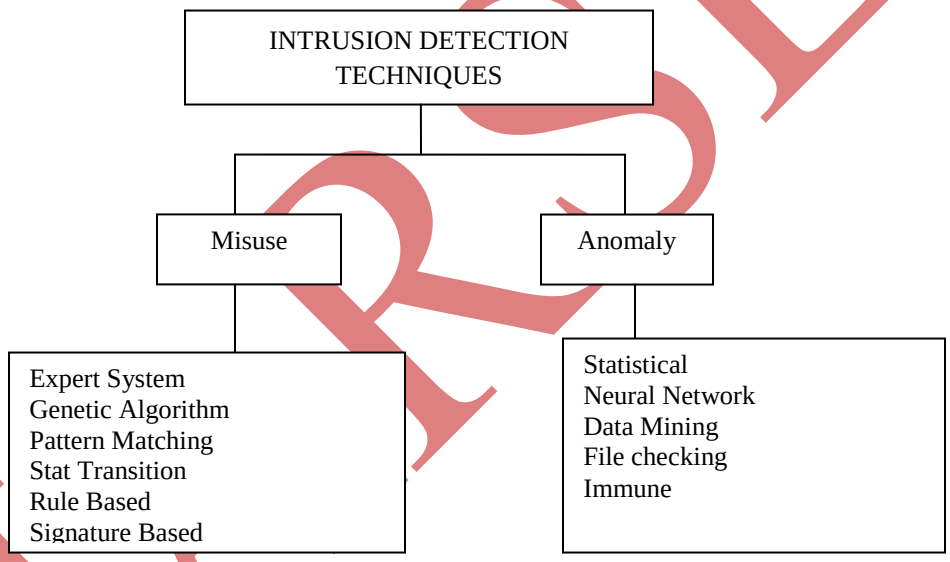


Fig.2

VI COMPARISON OF IDS TECHNIQUES

	Advantages	**Disadvantages**
Misuse Detection	Accurately and generate much fewer false alarm	Cannot detect novel or unknown attacks
Anomaly Detection	Is able to detect unknown attacks based on audit	High false-alarm and limited by training data.

6.1 Vulnerabilities of Manets

6.1.1 Vulnerabilities accentuated by manet context

Access Control

- Lack of physical boundary/packet boundary

- Shared, open broadcast medium
- E.g. IP masquerading, passive eavesdropping, DoS

6.1.2 Vulnerabilities specific to manets

Trust

- Lack of trust in the underlying infrastructure
- Collaborative participation of networks is mandatory for routing and auto-configuration
- E.g. Refusal of Service (RoS), Emission of false information, Sleep-deprivation torture, DoS on MAC, DAD

6.2 Intrusion Detection Systems

i. Attempts to detect intrusions on autonomous systems e.g: *computer networks*

ii. Based on Deployment
- Host Based (HIDS) (e.g. ZoneAlarm)
  - Uses hosts' audit logs & visible traffic for intrusion detection
- Network Based (NIDS) (e.g. NFR)
  - Uses substantial network traffic for intrusion detection

iii. Based on Techniques
- Anomaly Detection (e.g. use of normal profile)
- Misuse Detection (e.g. use of attack signatures)
- Specification Based (e.g. monitor invariants for violations)

iv. Policy Based (e.g. monitor policy violations)

6.3 Requirements of an IDS on Manets

i. Not introduce a new weakness
- Anomaly detection system itself should not make the node weaker than it already is (e.g. listening in promiscuous mode)

ii. Need little system resources
- In general nodes on manets have stringent requirements on resources (e.g. may not be able to run complex detection algorithms)

iii. Have proper response for detections
- An IDS should not only detect but also should response to the detected intrusions, preferably without human intervention (e.g. modify firewall to avoid attacking hosts etc.)

iv. Be reliable
- Fewer false positives, as there is no extensive crisis control infrastructure to handle alarms

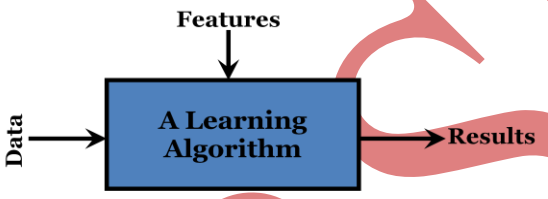
v. Interoperable with other IDS
- Be able to collaborate with other nodes for detection or response (e.g. use standards)

6.4 Problems of Current Techniques

- **Lack of traffic convergence points:** Prohibits the use of NIDS, Firewalls, Policies etc.
- **Lack of available data at hosts:** ID algorithms have to work with "partial and localized information" in and around the radio range of hosts
- **Lack of communication among nodes:** Disconnected operations & Location dependent computing
- **Lack of standards** :Lack of protocol standards

$$|signatures| = |protocols| * |vulnerabilities| * |topologies|$$

6.5 Anomaly Detection In General



- Pick a learning algorithm
- Pick some features
- Train the algorithm
- Test the algorithm
- Tune the algorithm, features
- Go to 3

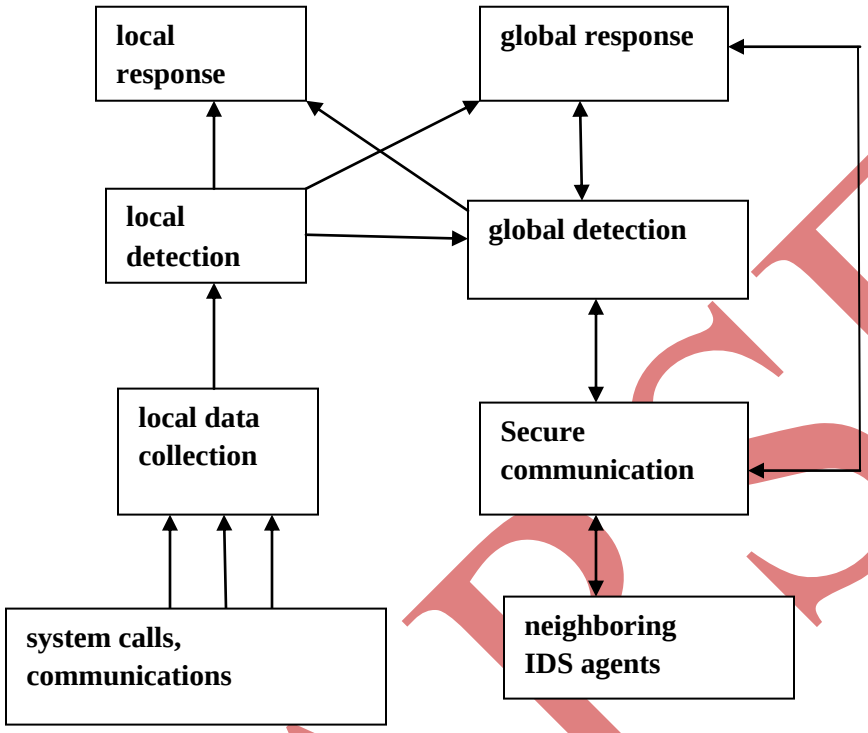
6.5.1 Anomaly Detection on Manets

i. Arguments for Anomaly Detection on Manets
   - One too many signatures to maintain for a misuse detection systems
   - Keeping the signatures up to date is a bigger problem
   - Lack of centralized management and monitoring points makes policy based systems difficult and also policies among communities may be incompatible
   - Specification based systems may work but no one tried it, AFAIK

ii. Arguments Against Anomaly Detection on Manets
   - There may not be a clear separation between normalcy and anomaly (e.g. emission of false routing information)
   - There may not be enough data for anomaly detection systems (e.g. disconnected operations, lack of communication in general)
   - Processing, memory requirements for anomaly detection are relatively high and nodes may not be able to cope up with the requirements

- Hasn't proven itself useful in fixed networks (IMHO)

6.6 Proposed System Architecture



6.6.1 Proposed Process

- PCR= Percentage of Changed Routes
- PCH= Percentage of Changes of sum of Hops of all routes
- Training process simulate diversity of normal situations and trace data is gathered
- A detection model trained on this data can work on any node
- Computing the normal profile
  - Denote PCR the class
  - Also, denote distance, direction, velocity, and PCH the features
  - Use n classes to represent the PCR ranges
  - Apply a classification algorithm to learn a classifier for PCR
  - Repeat the process to learn a classifier for PCH

6.6.2 Process of Anomaly Detection

i. Training & Testing

- Feed the trace data to classification algorithm

- Compute confidence for all classification rules
- Compute PCR, PCH deviation scores PCRD, PCHD
- Assign classes {*normal*, *abnormal*} for (PCHD, PCRD)
- Use a classification/clustering algorithm on (PCHD, PCRD, Class) to compute a classifier
- Refine the models

ii. Deviation (PCRD, PCHD) is measured by the confidence value of violated classification rule

iii. Combination of classification algorithms (2,5) is used on hosts for anomaly detection

- Pick a learning algorithm (lots of tools)
- And the 3T's (train, test, tune)
- Just don't over fit or over tune

VII CONCLUSION

In this survey paper, we describe the generic architectural model of a IDS with their types, in which they are employed in the network and how those types can be used to enhance the security of an organization. Specifically we also focus on two important techniques of intrusion detection system: Misuse and Anomaly based detection based on number of different approaches with their strengths and weakness.Researchers proposed several intrusion detection approaches and each detection approach is suitable only for detecting a particular type of attack. Because of limited attack coverage of each approach, there is an urgent need to arrive of a generic detection approach that handles almost all types of attacks. For that it is required to understand and analyze the techniques that are already investigated by several researchers.We hope this study will be useful for researchers to carry forward research on system security for designs of a IDS that not only will have identified strengths but also overcome the drawbacks.

REFERENCES

[1] Anonymous, 2001. Maximum Security, Third editionSams publications, Indianapolis, Indiana, USA

[2] Yuebin Bai, Hidetsune Kobayashi, 2003. IntrusionDetection System: Technology &DevelopmentProceedings of the17th International Conference onAdvanced formation Networking and Applications(AINA'03).

[3] A Murali M Rao,2005. A Survey on Intrusion DetectionApproaches, IEEE.

[4] Eric Maiwad, 2001. Network Security A Beginners Guide, Chief Technology Officer, TMH publications.

[5] S. Kumar, Classification and Detection of ComputerIntrusions, Ph.D. Thesis, Purdue University.

[6] S. Axelsson,2000. Intrusion Detection Systems: ASurvey and Taxonomy, Technical Report 99 15Department of Computer Engineering, ChalmersUniversity

[7] White paper, Intrusion Detection: A Survey,ch.2, DAAD19-01,NSF, 2002

[8] K. Scarfone, P. Mell, Feb. 2007. Guide to IntrusionDetection and Prevention Systems (IDPS), NISTSpecial Publication, 800-94.

[9] Aleksandar L., Vipin K., and Jaideep S.,2005. Massive Computing Managing Cyber Threats, Issues, Approaches, and Challenges. Chapter 2. IntrusionDetection: A Survey. Computers/GeneralInformation. Springer.

[10] D. J. Brown, B. Suckow, and T. Wang,2002. Surveyof Intrusion Detection Systems.

[11] Prof.A.K.Gulve, D.G.Vyawahare, April / May 2011. Survey OnIntrusion Detection System, in InternationalJournal Of Computer Science And ApplicationsVol. 4, No. 1

[12] A. H. M. Rezaul Karim,R, M. A. P.Rajatheva,Kazi M.Ahmed,2006. An EfficientCollaborative Intrusion Detection System forMANET Using Bayesian Approach, pp.187-190.

[13] Latifur Khan R Mamoun Awad R BhavaniThuraisingham,2007 A New Intrusion Detection SystemUsing Support Vector MachinesAnd HierarchicalClustering, The VLDB Journal 16,pp.507 –521.

[14] Tsong Song Hwang, Tsung-Ju Lee,Yuh-Jye Lee,2007.A Threetier IDS via Data Mining Approach, *MineNet'07.*

[15] Weiming Hu, Steve Maybank,April 2008. AdaBoost- BasedAlgorithm for Network Intrusion Detection, IEEETRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: YBERNETICS,VOL. 38, O.2,PP.577-583

[16] Hu Zhengbing, Li Zhitang,Wu Junq, January 21-23,2008. A NovelNetwork Intrusion Detection System(NIDS)Based on Signatures Search of Data Mining, e- Forensics, ICST 978-963- 9799-19-6.

[17] Amit Kumar Choudhary, Akhilesh Swarup,Neural Network Approach for IntrusionDetection, ICIS 2009November 24- 26,2009Seoul, Korea ACM 978-1-60558-710-3.

[18] Stefano Zanero,Sergio M.Savaresi, Unsupervised learningtechniques for anintrusion detection system, SAC'04 March1417, Nicosia, Cyprus, ACM 1581138121/03/04.

[19] Liberios VOKOROKOS, Anton BALÁŽ, MartinCHOVANEC, Intrusion Detection System UsingSelf Organising Map,Acta Electrotechnica etInformatica No. 1,Vol. 6, 2006 ,pp.1-6.

[20] H. Günes Kayacık, A. Nur Zincir-Heywood,2006,Using Self- Organizing Maps to Build an AttackMap for Forensic Analysis, PST, Oct 30-Nov 1, Markham, Ontario,Canada, ACM 1-59593-604-1/06/00010

[21] Zhenwei Yu, Jeffrey J. P. Tsai, An AutomaticallyTuning Intrusion Detection System, IEEETRANSACTIONS ON SYSTEMS, MAN,ANDCYBERNETICS—PART B: CYBERNETICS, VOL37, NO. 2,APRIL 2007,pp. 373-384

[22] Stefano Zanero, ULISSE, a Network IntrusionDetectionSystem, CSIIRW '08 May 12-14, OakRidge, Tennessee,USA ACM 978-1-60558-098-2

[23] V. K. Pachghare, Parag Kulkarn, Deven M.Nikam, IntrusionDetection System Using SelfOrganizing Maps, 978-1-4244- /09/2009 IEEE

[24] Mansour M. Alsulaiman, Aasem N. Alyahya,RaedA.Alkharboush, Nasser S. Alghafis, 2009. IntrusionDetection System using Self- Organizing Maps,Third International Conference on Networkand System Security, 978-0-7695-3838-9/09DOI0.1109/NSS.2009.62

[25] Stefan Axelsson, Combining a Bayesian Classifierwith Visualisation:Understanding the IDS,VizSEC/DMSEC'04,October 29, 2004, Washington DC, USA., ACM1581139748/04/0010.

[26] Iftikhar Ahmad, Sami Ullah Swati, Sajjad Mohsin, IntrusionDetection Mechanism by Resilient BackPropagation (RPROP) EUROPEAN JOURNALOF SCIENTIFICRESEARCH, Volume 17, No. 4August 2007,pp 523-530.

[27] Antonis Papadogiannakis, Michalis PolychronakisEvangelos P. Markatos, Improving the Accuracy of Network Intrusion Detection Systems Under LoadUsing Selective Packet Discarding, EUROSEC'10,Paris, France ,2010 ACM 978-1-4503-0059-9/10/04.

[28] Z. Bankovic, D. Stepanovic, S. Bojanic, O.Nieto-Taladriz, AGAbased Solution for IntrusionDetection, Journal of Information Assurance andSecurity 4 (2009) 192-199.

[29] W. Spears, and V. Anand, A Study of CrossoverOperators inGenetic Programming, InProceedings of the Sixth InternationalSymposiumon Methodologies for Intelligent Systems,Charlotte,NC.1991, pp. 409-418

[30] A. Chittur, Model Generation for an IntrusionDetectio SystemUsing Genetic Algorithms,Ossining High School, Ossining NY,2001.

[31] A. Abraham, Evolutionary Computation inIntelligent NetworkManagement , in EvolutionaryComputing in Data Mining,Springer,pp. 189-210,2004

[32] W. Li, Using Genetic Algorithm for NetworkIntrusion Detection,Proceedings of the UnitedStates Department of Energy Cyber SecurityGroup, 2004

[33] ANDERSON, D., FRIVOLD, T., AND VALDES,A. 1995. Nextgeneration intrusion detection expertsystem (NIDES): A summary. SRI-CSL-95-07

[34] Sebring, M.M., E. Shellhouse, M. Hanna and RWhitehurst. Expert Systems in IntrusionDetection: A Case Study.

[35] U. Lindqvist, P.A. Porras. Detecting Computer andNetwork Misuse Through the Production-BasedExpert System Toolset (PBEST).In Proceedings ofthe 1999 IEEE Symposium on Security andPrivacy. pp. 146 -161