2012 32nd International Conference on Distributed Computing Systems Workshops

Authentication and Access Control in the Internet of Things

Jing Liu and Yang Xiao,
Department of Computer Science
The University of Alabama
101 Houser Hall, Box 870290
Tuscaloosa, AL 35487-0290 USA

C. L. Philip Chen
Faculty of Science of Tech.,
University of Macau
Macau, Macau

[*]*Abstract*—**Due to the inherent vulnerabilities of the Internet, security and privacy issues should be considered and addressed before the Internet of Things is widely deployed. This paper mainly analyzes existing authentication and access control methods, and then, it designs a feasible one for the Internet of Things.**

Keywords- Authentication, Access Control, Internet of Things

I. INTRODUCTION

The smart devices, like smart phones and sensing nodes, are now forming an emerging global and Internet-based information service platform called the Internet of Things (IoT) [1]. Generally, the IoT architecture is based on some existing data communication tools, which could range from RFID (Radio Frequency IDentification) -tagged products to complex computational items. The latter originally targeted productivity, mobile applications, and entertainment, but now they are placed into new contexts, realize a better user interface, or package functionality aspects in a new, cheaper, or more robust way [1, 2].

The most challenging topics in such an interconnected system of miniaturized "things" are security and privacy aspects [3-7]. Before the IoT existence, corrupted digital systems were mostly unable to act in the physical world. This will change dramatically and dangerously now that corrupted digital systems can operate in and influence the physical world [3, 6, 7].

Authentication and access control technologies [8-50] are known as the central elements to address the security and privacy problems in computer networks. They can prevent unauthorized users from gaining access to resources, prevent legitimate users from accessing resources in an unauthorized manner, and enable legitimate users to access resources in an authorized manner.

The rest of this paper is organized as follows: Section II proposes our design on authentication and access control for the IoT, and security analysis; Section III is the conclusion of this paper.

II. OUR DESIGN

Authentication is a communication protocol processing procedure. In the IoT, secure communication should be constructed between one "thing" and another by such a procedure. The identity that the second "thing" or object claims should be consistent with what the first one claims. Claimed identity information becomes a single message. Based on this message, we verify the identity of the "things".

The purpose for both communication partners to implement authentication protocol is to have solid communication in the high layer (e.g., application layer). In order to do that, usually the authentication protocol has several sub-tasks such as identification key establishment, or key switching and consultation. In an authentication process, identity of the claimer can be acquired through message identification. In authenticated key establishment protocol, key establishment materials are also important protocol messages, which is part of entity authentication.

In this paper, we focus on simple and efficient secure key establishment based on ECC (Elliptic Curve Cryptosystem). For the access control policy, we adopt RBAC-based (Role-Based Access Control) authorization method using the thing's particular role(s) and application(s) in the associated IoT network.

A. Architecture

Based on what we have learned from current literatures of Internet of Things, we may reasonably draw an abstract architecture for it (as shown in Fig. 1). "Things" or objects become end nodes in the Internet environment. They have unique global addresses (e.g., IPv6 address) and are capable of communicating with each other over the Internet. In order to organize and manage massive resources, every object will pre-register on a nearby trustworthy access point or gateway (denoted as Registration Authority, or RA). This assumption has another advantage that the RA can expend computing and storage capacity of the "things" or objects for authentication purpose. Meanwhile, RA is also able to maintain a history record of all access requests for auditing

[*] Prof. Yang Xiao is the corresponding author. E-mail: yangxiao@ieee.org

1545-0678/12 $26.00 © 2012 IEEE
DOI 10.1109/ICDCSW.2012.23

purpose.

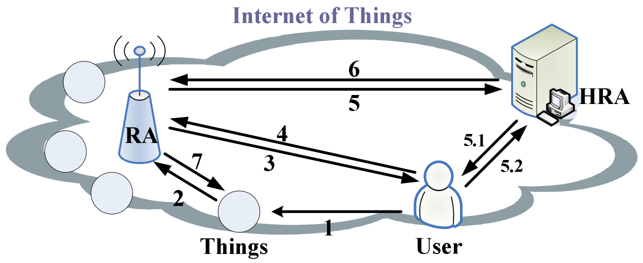

Fig. 1. An example of IoT architecture.

B. Authentication Protocol

To better describe our protocol, we first introduce some relevant terms here.

F_p: a finite field,

E: an elliptic curve defined on F_p with a large order,

P: a point on E,

G: the group of elliptic curve points on E,

$h()$: a public one-way hash function,

s: the RA's private key,

ID_u: the identity of the user,

ID_t: the identity of the "thing".

As we known, key establishments and distribution are the fundamental tasks for entity authentication. We can use either SKC or PKC for their implementations, but we have to know the pros and the cons of each algorithm. SKC-based schemes suffer the following problems: they require a large memory to store key materials, provide low scalability due to distribution of the keys, add and revoke keys, and require complicated key pre-distribution. On the other hand, PKC-based schemes suffer from high energy consumption and considerable time delay. PKC provides a more flexible and simple interface compared to SKC, which does not require key pre-distribution, pair-wise key sharing, or complicated one-way key chain schemes. For our situation, it is a wise choice if we adopt a PKC-based solution and at the meantime, we also address the aforementioned constraint problems. Based on current research achievements, we believe ECC-based solution is a solid one to be considered.

To establish a session key for two entities, taking a user and an object as an example, only three steps are required as follows.

- Firstly, the RA who is responsible for the object will produce a random $P\in G$ and compute $P_s = sP$ in F_p. Note that, the s is a secret key that is assumed to be assigned before the RA has joined the IoT. For each user with ID_u, RA will generate $P_u = h(ID_u)$ and the private key of the thing $S_u = s\ P_u$.
- Secondly, the user generate an ephemeral private key a and compute $Q_u = a\ S_u$ and $Q_u' = a\ P$. Then the user will send an authentication message $\{ID_u, Q_u, h(ID_u||ID_t||Q_u||\ Q_u')\}$ to the RA. Once receive the message, RA will compute $Q_u'' = s^{-1}Q_u$ and check whether $h(ID_u||ID_t\ \ ||Q_u||\ \ Q_u'')$ equal to $h(ID_u||ID_t||Q_u||Q_u')$ or not. If not, authentication fails. Otherwise go to step 3.
- The third step is session key establishment. Similarly, the RA will choose a random ephemeral key b and compute $Q_t = bP$ for the desired "thing". The session key will be $h(abP)$ based on ECC algorithm.

The next question is how to authenticate a legitimate user in the IoT. "Things" and users are in different domains. They could locate in different hierarchy level of the network. Central authentication method is only valid if a wide accepted KDC (key distribution center) is available. In industry, OpenID technology solves this problem. OpenID enables users to have a single account that allows them to log on to many different sites by authenticating a single identity provider [8]. One approach to identity management is federated identity management, in which participating sites form a circle of trust. Therefore, if the user is authenticated to one site, the other sites will automatically log the user in if the user visits them [8]. This lightweight idea should be adopted into our design. As such, user authentication is performed in the user domain or registered OpenID service provider. We denote it as home registration authority (HRA). Note that, peer-to-peer authentication method is another solution that can be utilized for further research. However, without solving the mutual-trust problem between two entities, this approach cannot be success.

As shown in Figure 2, a complete request procedure for accessing a "Thing" involves seven steps.

Step 1: User request to access a "Thing";

Step 2: "Thing" sends an authentication request to its RA for verification purpose;

Step 3: RA request User ID;

Step 4: User response with HRA information;

Step 5: RA verifies the user HRA information and sends ID verification request to the HRA;

Step 5.1: HRA challenge the user with a question;

Step 5.2: User response the challenge with an answer;

Step 6: HRA response ID OK or not;

Step 7: RA response the "Thing" about the user ID and issue a session key with the user as we described.

The IoT needs to authenticate entities that are accessing the pervasive network in order to provide service to only registered members. The entity may be an IoT user or a device. The IoT is able to support a wide range of ages of users and reflect their own characteristics and needs. As a result, we can selectively use our favorite authentication method among existing authentication methods. The authentication mechanisms are safe and reliable. Our proposed authentication mechanism satisfies these requirements. The RA verifies the certificate contents and the identity of the "thing". Two RA models exist in general PKI. In the first model, the RA collects and verifies the necessary information for the requesting entity before a request for a certificate is submitted to the HRA. The HRA trusts the information in the request because the RA already verified it. In the second model, the HRA provides the RA with information regarding a certificate request that it has already received. The RA reviews the contents and determines if the information accurately describes the user. The RA provides the HRA with a "yes" or "no" answer. It is a device of the kind that has the same or more computing power, memory, and data protection module. Therefore, the RA generates key pairs and requests and receives certificates for all "things".

C. Access Control

A novel scheme for user access control in IoT would bring solutions to the problems addressed above. Access control algorithm decides whether new connection is accepted when communication quality is already ensured. When a new service call arrives, if bandwidth in the community is still available, the call will be processed. If there is not enough bandwidth when a new call arrives, the call will be congested (discarded) or put on the waiting list. In the IoT, there are two types of calls that need admittance connection. One is new service calls launched by mobile users in the current community. The second is switching service needed by mobile users in other communities to switch to their current community. From the user's perspective, an interruption during the call is more unacceptable than being unable to make a call. That is why switching service has higher priority in admittance control strategy.

In IoT, different networks have different features. IoT supplies limited service bandwidth, but it has short transmission delay. Wireless LAN can increase the service bandwidth, but it has long transmission delay. In a heterogeneous network, it is crucial to supply the optimal wireless host based on Quality of Service (QoS) request of each service to networks that have different resources and services. According to different demands of service quality, service flow can be divided and scheduled. Service streams can be rated as different service levels and are transmitted in separate networks, which improve the service quality of the whole IoT network.

In terms of nodes in coupling-interconnected IoT network, data stream received or sent can be divided in nodes in IoT network. The principles of division vary based on service requirement. Divided data stream can only be transmitted on IoT. Flow converges when data stream gets to the terminal or nodes can be improved so that service quality in IoT network. A new IoT admittance control algorithm is hence designed. When a new connection arrives, the admittance control mechanism will judge whether there are free resources available for interconnected networks that launch connection requests. It will also decide what mechanism is needed to accept current connection request.

When we have flow scheduling in multiple services in IoT network, all of the data streams' waiting and priority management are in charge of the united flow scheduler and under the united admittance control. Admittance control algorithm optimizes the system volume and reduces the quality decline caused by increasing data missing rate so that both of which can be balanced.

It is easy to control centralizing by using strategy-based resource management. By using such a method, the network state can have consistency, and the IoT of different network technologies can be managed together. Methods based on strategy make it easy to implement united control over heterogeneous network and to set up local control in sub-networks by using hierarchical strategy mechanism.

A *role* represents a specific function within an organization and can be seen as a set of actions or responsibilities associated with this function. In a RBAC model, all grant authorizations deal with roles rather than being granted directly to users.

Users are then made members of roles, which thereby acquires the roles' authorizations. User access to resources is controlled by roles. Each user is authorized to play certain roles, and based on his own role, he/she can access the resources and operate them correspondingly. As a role organizes a set of related authorizations together, it can simplify the authorization management. Whenever a user needs a certain type of authority to perform an activity, he/she only has to be granted the authority of a proper role, rather than directly assigned the specific authorizations. Furthermore, when he/she changes his/her function inside the organization, he/she needs to revoke the permission function of the role. Complicated cascaded authorization revoke operations are no longer needed.

RBAC ensures that only authorized users are given access to certain data or resources. It also supports three well-known security principles: information hiding, least-privilege, and separation of duties.

Role hierarchy in RBAC is a natural way of organizing roles to reflect the organization's lines of authority and responsibility. By convention, junior roles appear at the bottom of the hierarchic role diagrams and senior roles at the top. The hierarchic diagrams are partial orders. Therefore, they are reflexive, transitive, and anti-symmetric.

Several RBAC models are provided when integrating constraints, sessions and other information into the basic model. The access policy could vary based on different types of applications.

D. *Security Analysis*

In this section, we will analyze whether our proposed protocol is secure or not.

1) Eavesdropping Attack

Each run produces a different session key, and knowledge of past session keys does not allow deduction of future session keys. In our scheme, the session key is calculated by one way hash and session secrets. Know that only the user and RA know the *abP*, which is computed from the random ephemeral key. That is, even if the previous session secrets are revealed, the other secrets will remain unknown to the adversary.

2) Man-in-the-middle Attack

Compromising of a long term secret key, such as SA' at some point in the future, does not lead to compromise of communications in the past. Note that in our scheme, even if the adversary compromises the RA's secret key, it cannot compromise the previous session key because the adversary cannot know the ephemeral key a or b such that it cannot compute the session key. Also, our protocols satisfy both partial forward secrecy and perfect forward secrecy since it is hard to compute the session key without knowing the ephemeral key a or b .

3) Key Control Attack

Both communication entities select a random number to generate the session key, which would be discarded after the session expired. Neither one can control the outcome of the session by, for example, restricting it to lie in some predetermined small set. In other words, neither entity can force the session key to a pre-selected value. Hence, our proposed protocol can resist any key control attack.

4) Replay Attack

In case a malicious one gained a valid session key or captured network traffic in the IoT, the protocol should resist replay attack by introducing a nonce in every transmitted message. However, it is an optional choice that could vary on different applications. Besides, the session key could be used for identification. Therefore, replayed message from unidentified person will be discarded.

III. Conclusion

This paper mainly analyzes existing authentication and access control methods, and then, it designs a feasible one for the IoT. Analysis results show that our approach can prevent attacks like eavesdropping, the man-in-the middle, key control attack, and replay attacks.

Acknowledgement

This work is supported in part by The U.S. National Science Foundation (NSF), under grants: CNS-0716211, CCF-0829827, CNS-0737325, and CNS-1059265.

The authors would like to acknowledge the support, in part, from the Ministry of Science and Technology of China under grant number 2011CB302801 and Macau Science and Technology Development Fund grant number 008/2010/A1.

References

[1] L. Atzori, A. Iera, and G. Morabito, “The Internet of things: a survey,” *Computer Networks*, vol. 54, issue 15, 2010, pp 2787-2805.

[2] R. H. Weber, “Internet of things – need for a new legal environment?” *Computer Law & Security Review*, vol. 25, issue 6, Nov. 2009, pp 522-527.

[3] R. H. Weber, “Internet of things – new security and privacy challenges,” *Computer Law & Security Review*, vol. 26, issue 1, Jan. 2010, pp. 23-30.

[4] H. Huang and H. Wang, “Studying on Internet of things based on fingerprint identification,” in: *Proceedings of 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, 2010, pp. 628-630.

[5] L. Xiong, X. Zhou, and W. Liu, “Research on the architecture of trusted security system based on the Internet of things,” in: *Proceedings of the 4th International Conference on Intelligent Computation Technology and Automation*, 2011, pp. 1172- 1175.

[6] K. Wang, J. Bao, M. Wu, and W. Lu, “Research on security management for Internet of things,” in*: Proceedings of 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, 2010, pp. 133-137.

[7] A. Sarma and J. Girao, “Identities in the future Internet of things,” *Wireless Personal Communications: An International Journal*, vol. 49, issue 3, May 2009, pp. 353-363.

[8] A. Vapen, D. Byers, and N. Shahmehri, “2-clickAuth – optical challenge-response authentication,” in: *Proceedings of 2010 International Conference on Availability, Reliability and Security*, 2010, pp. 79-86.

[9] Z. Benenson, F. Gartner, and D. Kesdogan, “An algorithmic framework for robust access control in wireless sensor networks,” in *Wireless Sensor Networks, 2005. Proceedings of the Second European Workshop on*, pp. 158-165.

[10] X.H. Le, S. Lee, I. Butun, M. Khalid, and R. Sankar, “An energy efficient access control for sensor networks based on elliptic curve cryptography,” *Journal of Communications and Networks*, 2009.

[11] Y. Shen, J. Ma, and Q. Pei, “An access control scheme in wireless sensor networks,” in *Network and Parallel Computing Workshops*, 2007. NPC Workshops. IFIP International Conference on, 2007, pp. 362-367.

[12] K. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks.” *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, 2006.

[13] H. Tseng, R. Jan, and W. Yang, “An improved dynamic user authentication scheme for wireless sensor networks.” *IEEE Global Communications Conference*, 2007.

[14] H. Wang and Q. Li, “Distributed user access control in sensor networks,” *Distributed Computing in Sensor Systems*, pp. 305-320.

[15] H. Wang, B. Sheng, and Q. Li, “Elliptic curve cryptography-based access control in sensor networks,” *International Journal of Security and Networks*, vol. 1, no. 3, pp. 127-137, 2006.

[16] H. Wang, B. Sheng, C. Tan, and Q. Li, “Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control.” *The 28th International Conference on distributed Computing Systems, ICDCS’08*, 2008, pp. 11-18.

[17] Y. Zhou, Y. Zhang, and Y. Fang, “Access control in wireless sensor networks,” *Ad Hoc Networks*, vol. 5, no. 1, pp. 3-13, 2007.

[18] H.F. Huang, “A novel access control protocol for secure sensor networks”, *Journal of Computer Standards and Interfaces*, vol. 31, issue 2, Elsevier, 2009.

[19] W. Tsai and Q. Shao, “Role-based access-control using reference ontology in clouds,” in: *Proceedings of the 10th International Symposium on Autonomous Decentralized Systems*, 2011, pp. 121-128.

[20] H. Lim, M. Kim, J. Lee, D. Seo, and T. M. Chung, “Reducing communication overhead for nested NEMO networks: roaming authentication and access control structure,” *IEEE Transactions on Vehicular Technology*, Issue 99, June 2011, pp. 1-17.

[21] D. G. Lee, J. Han, D. S. Park, and I. Y. Lee, “Intelligent pervasive network authentication – s/key based device authentication,” in: *The 6th IEEE Consumer Communications and Networking Conference (CCNC 2009)*, Jan. 2009, Las Vegas, NV, pp. 1-5.

[22] J. Zheng, J. Li, M. J. Lee, and M. Anshel, "A lightweight encryption and authentication scheme for wireless sensor networks," International Journal of Security and Networks, Vol. 1, No.3/4 pp. 138 - 146, 2006.

[23] M. Lei, Y. Xiao, S. V. Vrbsky, and C.-C. Li, “Virtual Password Using Random Linear Functions for On-line Services, ATMs, and Pervasive Computing," Computer Communications Journal, Elsevier, Vol. 31, No. 18, Dec. 2008, pp. 4367-4375.

[24] Y. Jiang, C. Lin, M. Shi, and X. Shen, “A self-encryption authentication protocol for teleconference services,” *International Journal of Security and Networks*, Vol. 1, Nos.3/4 pp. 198 - 205, 2006.

[25] Y. Xiao, C.-C. Li, M. Lei, and S. V. Vrbsky, “Secret Little Functions and Codebook for Protecting Users from Password Theft,” in: *Proc. of IEEE ICC 2008*, pp.1525-1529.

[26] C. Tartary and H. Wang, “Efficient multicast stream authentication for the fully adversarial network model,” *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp. 175 - 191, 2007.

[27] M. Lei, Y. Xiao, S. V. Vrbsky, C.-C. Li, and L. Liu, “A Virtual Password Scheme to Protect Passwords,” in: *Proc. of IEEE ICC 2008*, pp.1536-1540.

[28] M. Abdalla, E. Bresson, O. Chevassut, B. Moller, and D. Pointcheval, “Strong password-based authentication in TLS using the three-party group Diffie–Hellman protocol,” *International Journal of Security and Networks*, Vol. 2, Nos. 3/4, pp. 284 - 296, 2007.

[29] Y. Xiao, C.-C. Li, M. Lei, and S. V. Vrbsky, “Differentiated virtual passwords, secret little functions, and codebooks for protecting users from password theft,” *IEEE Systems Journal*, DOI: 10.1109/JSYST.2012.2183755, accepted

[30] M. Asadpour, B. Sattarzadeh, and A. Movaghar, “Anonymous authentication protocol for GSM networks,” *International Journal of Security and Networks*, Vol. 3, No. 1, pp. 54 - 62, 2008.

[31] I. Krontiris and T. Dimitriou, “Scatter – secure code authentication for efficient reprogramming in wireless sensor networks,” *International Journal of Sensor Networks*, Vol. 10, Nos. 1/2, 2011, pp.14-24.

[32] X. Lin, X. Ling, H. Zhu, P. Ho, and X. Shen, “A novel localized authentication scheme in IEEE 802.11 based Wireless Mesh Networks,” *International Journal of Security and Networks*, Vol. 3, No. 2, pp. 122 - 132, 2008.

[33] K. Kim, J. Jeon, and K. Yoo, “Efficient and secure password authentication schemes for low-power devices,” *International Journal of Sensor Networks*, Vol. 2, Nos.1/2, pp. 77 - 81, 2006.

[34] A. Scannell, A. Varshavsky, A. LaMarca, and E. De Lara, “Proximity-based authentication of mobile devices,” *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp. 4 - 16, 2009.

[35] A. Scannell, A. Varshavsky, A. LaMarca, and E. De Lara, “Proximity-based authentication of mobile devices,” *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp. 4 - 16, 2009.

[36] J. M. McCune, A. Perrig, and M. K. Reiter, “Seeing-Is-Believing: using camera phones for human-verifiable authentication,” *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp. 43 - 56, 2009.

[37] S. Laur and S. Pasini, “User-aided data authentication,” *International Journal of Security and Networks*, Vol. 4, Nos. 1/2, pp. 69 - 86, 2009.

[38] S. Lee and K. M. Sivalingam, “An efficient One-Time Password authentication scheme using a smart card,” *International Journal of Security and Networks*, Vol. 4, No.3, pp. 145 - 152, 2009

[39] S. Huang and S. Shieh, “Authentication and secret search mechanisms for RFID-aware wireless sensor networks,” *International Journal of Security and Networks*, Vol. 5, No.1 pp. 15 - 25 , 2010

[40] M. Yang, “Lightweight authentication protocol for mobile RFID networks,” *International Journal of Security and Networks*, Vol. 5, No.1 pp. 53 - 62, 2010, DOI: 10.1504/IJSN.2010.030723

[41] J. Wang and G.L. Smith, “A cross-layer authentication design for secure video transportation in wireless sensor network,” *International Journal of Security and Networks*, Vol. 5, No.1 pp. 63 - 76, 2010, DOI: 10.1504/IJSN.2010.030724

[42] M. J. Sharma and V. C. M. Leung, “Improved IP multimedia subsystem authentication mechanism for 3G-WLAN networks,” *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 90-100.

[43] A. Fathy, T. ElBatt, and M. Youssef, “A source authentication scheme using network coding,” *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 112-122.

[44] T. Choi, H.B. Acharya, and M. G. Gouda, “Is that you? Authentication in a network without identities,” *International Journal of Security and Networks*, Vol. 6, No. 4, 2011, pp. 181 - 190.

[45] X. Zhao, L. Li, and G. Xue, “Authenticating strangers in online social networks,” *International Journal of Security and Networks*, Vol. 6, No. 4, 2011, pp. 237 - 248.

[46] R. Li, J. Li, and H. Chen, “DKMS: distributed hierarchical access control for multimedia networks,” *International Journal of Security and Networks*, Vol. 2, Nos. 1/2, pp. 3 - 10, 2007.

[47] M. Barua, X. Liang, R. Lu, X. Shen, “ESPAC: enabling security and patient-centric access control for eHealth in cloud computing,” *International Journal of Security and Networks*, Vol. 6 Nos. 2/3, 2011, pp. 67-76.

[48] X. Du, M. Guizani, Y. Xiao, and H. Chen, “A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks,” *IEEE Transactions on Wireless Communications*, Vol.8, No.3, Mar. 2009, pp. 1223-1229.

[49] W. Stallings, *Cryptography and Network Security, Principles and Practice, 5th Ed.*, Prentice Hall, 2010.

[50] M. Vandenwauver, R. Govaerts, and J. Vandewalle, “Overview of authentication protocols,” in: *The Institute of Electrical and Electronics Engineers 31st Annual 1997 International Carnahan Conference on Security Technology*, Oct. 1997, Canberra, Australia, pp.108-113.