Research Taxonomy

by

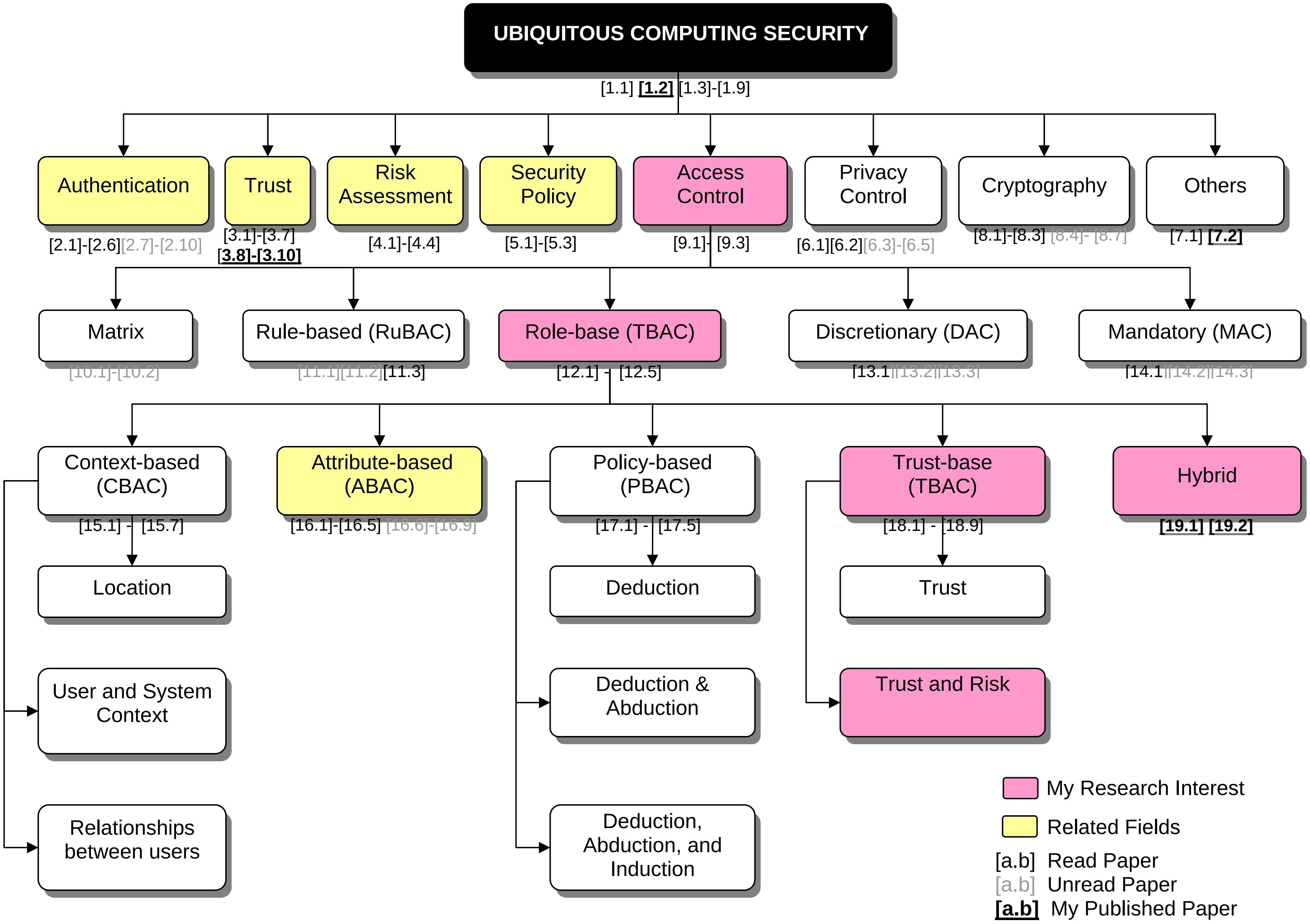
Le Xuan Hung, PhD Fellow

u-Security Research Group
lxhung@oslab.khu.ac.kr

Table of Content

Research Taxonomy.. 3
Term Descriptions.. 4
Milestones.. 9
Bibliography 10

Research Taxonomy



Term Descriptions

1. Authentication

In computer security, authentication is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in. The sender being authenticated may be a person using a computer, a computer itself or a computer program. A blind credential, in contrast, does not establish identity at all, but only a narrow right or status of the user or program.

In a web of trust, "authentication" is a way to ensure users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so.

2. Trust

Trust in computer security includes Trust Negotiation and Trust Management. Trust Negotiation deals with establishing trust between two parties who attempt to communicate with each other without any prior relationship. Trust Management concerns about maintaining all factors related to trust negotiation. Figure 1 shows an example of trust negotiation between a doctor (Dr. Jones) and a patient's primary care physician.

Fig. 2.1 describes a scenario where Dr. Jones wishes to access the EMR of a new patient, Ms. Sally White, who is visiting from out of town.

- He sends a request to the office of Ms. White's primary care physician, asking for her digitally signed medical re cord along with the credential containing the key used to sign it.
- To authenticate the requesting party, the primary care physician's trust negotiation system responds with a message containing a policy stating that records will only be disclosed to licensed medical doctors.
- In order to satisfy this policy and establish adequate trust, Dr. Jones supplies a digital credential signed by the local medical association asserting his status as a licensed practicing physician.
- The primary care physician's server confirms Dr. Jones' digital credential by verifying its signature using a credential issued by a uusted third party (e.g., a national licensing association). This fulfills the primary care physician's policy, resulting in a sufficient level of trust to complete the transaction.
- The server then encrypts Ms. White's EMR using a unique shared session key and sends it via the Internet along with a credential asserting the primary care physician's status as a licensed medical doctor.
- Dr. Jones decrypts the EMR and verifies its legitimacy using the primary care physician's credential. The use of trust negotiation in this scenario provides a mechanism for the authorized, confidential transfer of Sally's medical record.

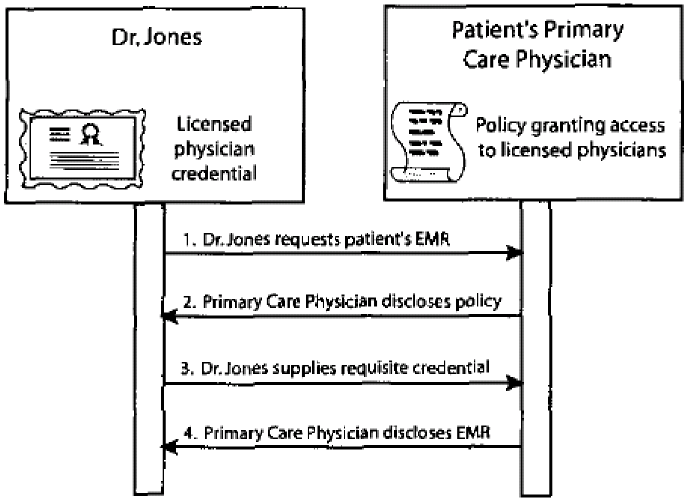

Dr. Jones
Licensed physician credential
Patient's Primary Care Physician
Policy granting access to licensed physicians
1. Dr. Jones requests patient's EMR
2. Primary Care Physician discloses policy
3. Dr. Jones supplies requisite credential
4. Primary Care Physician discloses EMR

Fig. 2.1. Using Trust negotiation to control access to EMR information.

3. Risk

There are many definitions of risk depending on the specific application and situational contexts. Generally, risk is related to the expected losses which can be caused by a risky event and to the probability of this event. The harsher the loss and the more likely the event, the worse the risk. Measuring risk is often difficult; rare failures can be hard to estimate, and loss of human life is generally considered irreplaceable

In information security a "risk" is defined as a function of three variables:

- the probability that there's a threat
- the probability that there are any vulnerabilities
- the potential impact.

If any of these variables approaches zero, the overall risk approaches zero.

4. Security Policy

Security policy is set of all policy statements of the system or organization defined to protect information. It states who are authorized to access to what resource, how to disclosure sensitive information, etc. Usually, security policy goes together with the mechanism using it. It includes access control policy, firewall policy, etc.

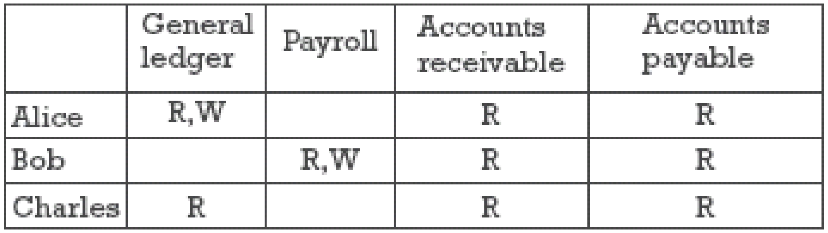
5. Access Control: General View

Access Control is one aspect of comprehensive computer security solution. Basically, it means to control access privileges from a user to a certain resource. Every time an user attempts to access to a resource, access control is enforced.

Typically, access control is criteria to preserving confidentiality and integrity of information. Confidentiality refers to the need to keep information secure and private. For example, sensitive medical information of a patient cannot be disclosure to unauthorized persons. Integrity refers to the concept of protecting information from being improperly altered or modified by unauthorized users. For example, most users want to ensure that bank account numbers used by financial software cannot be changed by anyone else and that only the user or an authorized security administrator can change passwords.

6. Matrix Access Control

Access Control term was considered in the late 1960s. The earliest work in defining a formal, mathematical description of access control is that of Lampson [10.1], who introduced the formal notions of subject and object and an access matrix that mediated the access of subjects to objects. An access matrix is a simple conceptual representation in which the (i,j) entry in the matrix specifies the rights that subject i has to object j. An example is shown in Figure 6.1. Subjects (processes invoked by users) are allowed to access objects such as files or peripherals according to the rights specified in the matrix. For example, user Bob is allowed read and write access to the payroll file, and read access to the accounts receivable and accounts payable file.



	General ledger	Payroll	Accounts receivable	Accounts payable
Alice	R,W		R	R
Bob		R,W	R	R
Charles	R		R	R

Fig. 6.1. Access Matrix

7. Rule-based Access Control (RuBAC)

In 1976, a new model, Rule-based Access Control was introduced by Bell [11.1]. It is an enhancement of matrix access control. It defines access control rules in a mathematical model. RuBAC allows users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control. “Rule-based access” is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems.

8. Mandatory Access Control (MAC)

DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file. DAC policy tends to be very flexible and is widely used in the commercial and government sectors

9. Discretionary Access Control (DAC)

Mandatory access control (MAC) policy means that access control policy decisions are made by a central authority, not by the individual owner of an object, and the owner cannot change access rights. An example of MAC occurs in military security, where an individual data owner does not decide who has a Top Secret clearance, nor can the owner change the classification of an object from Top Secret to Secret

The need for a MAC mechanism arises when the security policy of a system dictates that:

- Protection decisions must not be decided by the object owner.
- The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object

owner).

10. Role-based Access Control (RBAC)

Role-based Access Control was emerging approach in late 1990s and became NIST standard in 2004. It is an approach to restricting system access to authorized users. It is a newer and alternative approach to Mandatory Access Control (MAC) and Discretionary Access Control (DAC). The fundamental of RBAC is that it controls the access privileges of users based on their roles, not individual. Each user is assigned some role. Each role is mapped to certain permission such as read, write, etc. Fig 10.1 shows this relationship

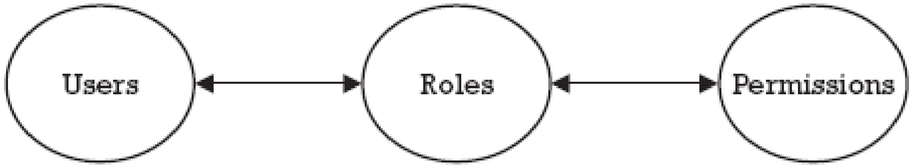


Fig. 10.1. Users, roles and permission relationship

Within an organization, roles are created for various job functions. The permissions to perform certain operations ('permissions') are assigned to specific roles. Members of staff (or other system users) are assigned particular roles, and through those role assignments acquire the permissions to perform particular system functions.

Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning the appropriate roles to the user, which simplifies common operations such as adding a user, or changing a user's department

RBAC has became foundation for afterward access control approaches such as context-based access control (CBAC), policy-based access control (PBAC), trust-based access control (TBAC), etc.

11. Context-based Access Control (CBAC)

Basically, Context-based Access Control is an improvement of Role-based Access Control to take advantage of context in context-awareness systems. In this case, context includes user context (e.g time, location, etc), system context (e.g. system state, network bandwidth, etc), environment context (e.g. temperature, humidity, etc). CBAC restricts user’s permissions according to current context at accessing time.

For example, Dr. Jones is visiting a patent at bed number 22. Based on his location the system know that he is visiting bed 22 patient, so it automatically transmits EMR of the patient to Dr. Jones’s PDA. Once he leaves to another location, he no longer views EMR of this patient.

12. Attribute-based Access Control (ABAC)

Attribute-based Access Control is another approach which is based on digital credential to authorize access permission to users.

In the past, access decisions were based on the identity of the entity requesting a resource, in open systems such as the Internet, this approach is ineffective when the resource owner and the requester belong to different security domains controlled by different authorities that are unknown to each other. One alternative is to use digital credentials for satisfying access policies. Digital credentials, the digital equivalent of paper credentials, are digitally signed assertions about the credential owner by a credential issuer. Each digital credential contains an attribute (or set of attributes) about the owner. The decision to allow or deny access to a resource is based on the attributes in the requester's credentials, such as age, citizenship, employment, group membership, or credit status. This approach is called attribute-based access control

13. Trust-based Access Control (TBAC)

In highly dynamic environment like ubiquitous computing, it's not always possible to maintain a pre-defined Access Control List (ACL) because this requires prior knowledge about who is trying to access and what their access rights are.

Under this circumstance, controlling access permission of unknown users based on trust level on those users is an emerging approach. A good scenario for TBAC is Ubiquitous Healthcare environments (U-Healthcare).In such environments, electronic medical record (EMR) plays a core portion of the systems. EMR should be shared to appropriate person like licensed doctors, treating nurse, etc in order to give better care to patients. However, it's not possible to maintain all types of users and what kinds of access permission they may have. Applying trust in this case solves the problem. It would be how much the system trusts on a user so that the system can disclosure sensitive medical information.

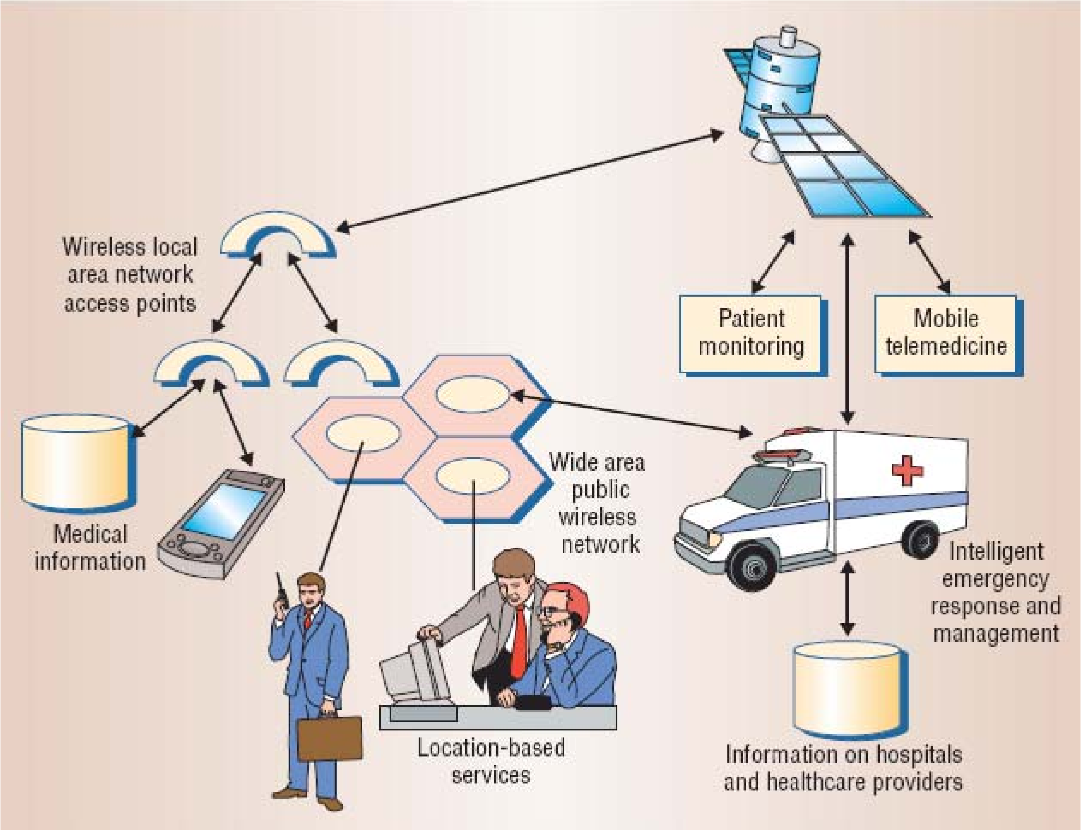
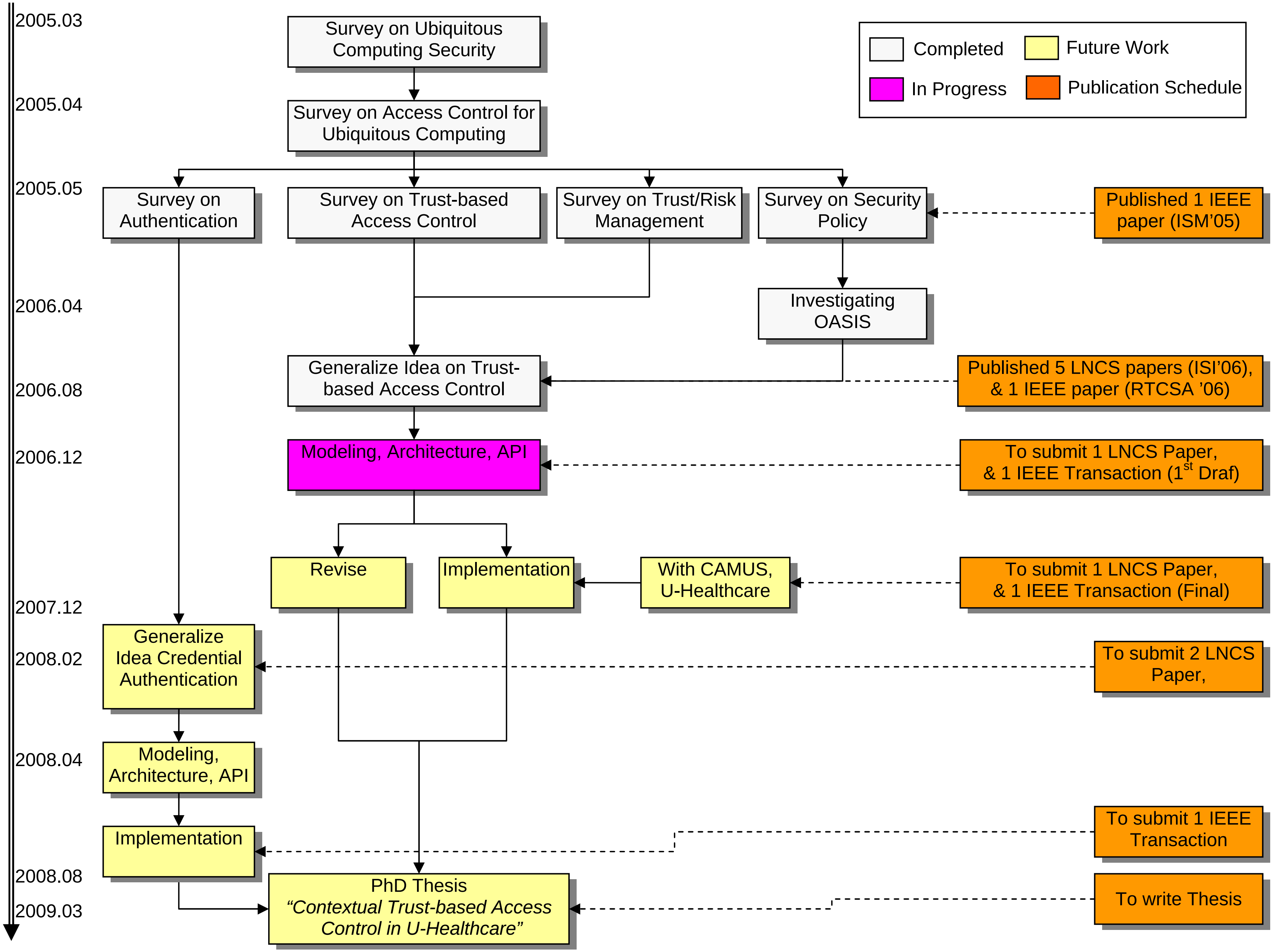

Wireless local area network access points
Patient monitoring
Mobile telemedicine
Medical information
Wide area public wireless network
Intelligent emergency response and management
Location-based services
Information on hospitals and healthcare providers

Fig. 13.1. Pervasive Healthcare Scenario. Medical information should be shared to legitimate users to give a better care while restricting to the others

Milestones



□ Completed
🟨 Future Work
🟪 In Progress
🟧 Publication Schedule

2005.03
Survey on Ubiquitous Computing Security

2005.04
Survey on Access Control for Ubiquitous Computing

2005.05
Survey on Authentication
Survey on Trust-based Access Control
Survey on Trust/Risk Management
Survey on Security Policy
Published 1 IEEE paper (ISM'05)

2006.04
Investigating OASIS

2006.08
Generalize Idea on Trust-based Access Control
Published 5 LNCS papers (ISI'06), & 1 IEEE paper (RTCSA '06)

2006.12
Modeling, Architecture, API
To submit 1 LNCS Paper, & 1 IEEE Transaction (1st Draf)

Revise
Implementation
With CAMUS, U-Healthcare
To submit 1 LNCS Paper, & 1 IEEE Transaction (Final)

2007.12

2008.02
Generalize Idea Credential Authentication
To submit 2 LNCS Paper,

2008.04
Modeling, Architecture, API

Implementation
To submit 1 IEEE Transaction

2008.08

2009.03
PhD Thesis *"Contextual Trust-based Access Control in U-Healthcare"*
To write Thesis

Bibliography

<u>Total: 100 referenced papers</u>

1. General

[1.1] Frank Stajano. Security for Ubiquitous Computing. John Wiley & Sons Ltd. 2002.

[1.2] Le Xuan Hung; Tran Van Phuong; Pho Duc Giang; Yonil Zhung; Sungyoung Lee; Young-Koo Lee. Security for Ubiquitous Computing: Problems and Proposed Solution. 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 2006. 16-18 Aug. 2006 Page(s):110 – 116.

[1.3] T. Kagal, L. Finin and A. Josh. Trust-Based Security in Pervasive Computing Environments. IEEE Computer, pages 154--157, December 2001.

[1.4] Roshan K. Thomas, Ravi Sandhu, "Models, Protocols, and Architectures for Secure Pervasive Computing: Challenges and Research Directions. Second IEEE Annual Conference on Pervasive Computing and Communications Workshops PERCOMW 2004

[1.5] P. Nixon, W. Wagealla, C. English and S. Terzis. Security, Privacy and Trust Issues in Smart Environments. University of Strathclyde, Computer and Information Sciences, Smartlab Technical Report (Smartlab-2004-01), 2004.

[1.6] Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane1, and M. D. Mickunas. Towards security and privacy for pervasive computing. In Proceedings of International Symposium on Software Security, Tokyo, Japan, 2002

[1.7] Jalal Al-Muhtadi, Anand Ranganathan, Roy Campbell and M. Dennis Mickunas, "Cerberus: A Context-Aware Security Scheme for Smart Spaces," in the Proceedings of the First IEEE Annual Conference on Pervasive Computing and Communications (PerCom 2003), pp. 489-496, Fort Worth, Texas, March 26, 2003

[1.8] David Llewellyn-Jones, Madjid Merabti, Qi Shi, Bob Askwith, "A Security Framework for Executables in a Ubiquitous Computing Environment", Globecom 2004, Dallas, USA

[1.9] J. Al-Muhtadi, M. Anand, M. D. Mickunas, R. Campbell. Secure smart homes using Jini and UIUC SESAME. Proceedings of the 16th Annual Computer Security Applications Conference 2000 pp. 77.

2. Authentication

[2.1] Ren, K.; Wenjing Lou; Kwangjo Kim; Deng, R.;A novel privacy preserving authentication and access control scheme for pervasive computing environments , IEEE Transactions on Vehicular Technology. Volume 55, Issue 4, July 2006 Page(s):1373 - 1384

[2.2] Weaver, A.C. Biometric authentication. IEEE Journal on Computer. Volume 39, Issue 2, Feb. 2006 Page(s):96 – 97

[2.3] Dass, S.C.; Yongfang Zhu; Jain, A.K.; Validating a Biometric Authentication System: Sample Size Requirements. IEEE Transactions on Pattern Analysis and Machine Intelligence. Volume 28, Issue 12, Dec. 2006 Page(s):1902 – 1319.

[2.4] Laurent BUSSARD and Yves ROUDIER. Authentication in Ubiquitous Computing. Workshop on Security in Ubiquitous Computing

UBICOMP 2002, Göteborg Sweden, 29 Sept 2002.

[2.5] Al-Muhtadi, J. Ranganathan, A. Campbell, R. Mickunas, M.D. A flexible, privacy-preserving authentication framework for ubiquitous computing environments. Proceedings of the 22nd International Conference on Distributed Computing Systems 2002 pp. 771-776

[2.6] J.-M. Seigneur, S. Farrell, C. D. Jensen. Secure ubiquitous computing based on entity recognition. Ubicomp2002 Security Workshop, 2002

[2.7] Reiner Sailer, James R. Giles . Pervasive Authentication Domains for Automatic Pervasive Device Authorization. Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops. 2004 pp.177

[2.8] Nicholson, A.J.; Corner, M.D.; Noble, B.D. Security Using Transient Authentication. IEEE Transactions on Mobile Device Mobile Computing. Volume 5, Issue 11, Nov. 2006 Page(s):1489 - 1502

[2.9] Jain, A.K.; Pankanti, S.. A touch of money [biometric authentication systems]. IEEE Spectrum Volume 43, Issue 7, July 2006 Page(s):22 - 27

[2.10] Malassiotis, S.; Aifanti, N.; Strintzis, M.G. Personal authentication using 3-D finger geometry. IEEE Transactions on Information Forensics and Security Volume 1, Issue 1, March 2006 Page(s):12 - 21

3. Trust Management

[3.1] L. Xiong, L. Liu. PeerTrust: Supporting Reputation-Based Trust in Peer-to-Peer Communities. IEEE Transactions on Knowledge and Data Engineering (TKDE), Special Issue on Peer-to-Peer Based Data Management, July 2004 (Vol. 16, No. 7) pp. 843-857

[3.2] R. He, J. Niu, M. Yuan, and J. Hu, “A novel cloud-based trust. model for pervasive computing,” 4th International Conference on Computer and Information Technology (CIT'04). 2004 pp: 693 - 700

[3.3] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In Proceedings 1996 IEEE Symposium on Security and Privacy, pages 164--173, May 1996

[3.4] C English, P. Nixon, and S. terzis. Dynamic trust models for ubiquitous computing environment. In Proceedings of the Ubicom 2002

[3.5] Cahill, V., Shand, B., Gray, E., Bryce, C., Dimmock, N.: Using trust for secure collaboration in uncertain environments. IEEE Pervasive Computing 2 (2003) 52--61

[3.6] Shankar N., Arbaugh W. "On Trust for Ubiquitous Computing." Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Gteborg Sweden

[3.7] Weiwei Yuan, Donghai Guan, Le Xuan Hung, Sungyoung Lee, and Youngkoo Lee, A Trust Model with Dynamic Decision Making For Ubiquitous Envrionments. The 14th IEEE International Conference on Networks (ICON2006), Singapore, Sep 13-15, 2006

[3.8] Le Xuan Hung, Hassan Jammeel, Seong Jin Cho, Yuan Weiwei, Sungyoung Lee and Young-Koo Lee, A Trust Model for Uncertainty in Ubiquitous Environments.. IEEE Intelligent and Security Informatics (ISI-2006), May 23-24, 2006 San Diego, USA. ISBN: 3-540-34478-0. LNCS Vol. 3975/2006pp 755-757

[3.9] Hassan Jameel, Le Xuan Hung, Sungyoung Lee and Young-Koo Lee. A Trust Model for Ubiquitous Systems based on Vectors of Trust

Values. 3rd International IEEE Security in Storage Workshop San Francisco, California USA, December 13, 2005

4. Risk Assessment

[4.1] Jason I. Hong: Minimizing Security Risks in Ubicomp Systems. IEEE Computer 38(12): 118-119 (2005)

[4.2] Stephen D. Kleban, Scott H. Clearwater: Computation-at-risk: employing the grid for computational risk management. IEEE International Conference on Cluster Computing pp: 347-352

[4.3] Y. Chen, C. Jensen, E. Gray, V. Cahill and J-M Seigneur, “A General Risk Assessment of Security in Pervasive Computing”, Technical Report TCD-CS-2003-45, Department of Computer Science, Trinity College Dublin, 6 November 2003

[4.4] Peter Chapin, Christian Skalka, and X. Sean Wang, “Risk assessment in distributed authorization”, Proceedings of the 2005 ACM workshop on Formal methods in security engineering, Fairfax, VA, USA, November 11-11, 2005.

5. Security Policy

[5.1] Jean Bacon, Ken Moody, and Walt Yao. A model of OASIS role-based access control and its support for active security. ACM Transactions on Information and System Security (TISSEC), 5(4):492--540, November 2002.

[5.2] Nicholas Damianou, Naranker Dulay, Emil Lupu, Morris Sloman. The Ponder Policy Specification Language. International workshop on policies for distributed systems and networks (POLICY 2001), Hewlett-Packard Lab, Bristrol, England

[5.3] Kouadri Mostéfaoui, G. and Brézillon, P. (2004) Modeling Context-Based Security Policies with Contextual Graphs. CoMoRea’04, Workshop on Context Modeling and Reasoning. In the Workshops Proceedings of the 2nd IEEE International Conference on Pervasive Computing and Communication (PerCom’04), Orlando, Florida 14-17 March 2004, ISBN 0-7695-2106-1, pp 28-32.

6. Privacy

[6.1] Jason I. Hong, James A. Landay. An architecture for privacy-sensitive ubiquitous computing International Conference On Mobile Systems, Applications And Services Boston, MA, USA 2004, pp: 177 – 189.

[6.2] Marc Langheinrich. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In: Gregory D. Abowd, Barry Brumitt, Steven A. Shafer (Eds.): Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001), LNCS No. 220, Springer-Verlag, pp. 273--291, Atlanta, USA, 2001

[6.3] Pho Duc Giang, Le Xuan Hung, Yonil Zhung, Sungyoung Lee, and Young-Koo Lee. A Home Firewall Solution for Securing Smart Spaces. IEEE Intelligent and Security Informatics (ISI-2006), May 23-24, 2006 San Diego, USA. ISBN: 3-540-34478-0. LNCS Vol. 3975/2006. pp 760-761

[6.4] Michael Reiter and Aviel Rubin. Anonymous web transactions with crowds. Communications of the ACM, 42(2):32--38, 1999

[6.5] Scott Lederer. Everyday Privacy in Ubiquitous Computing Environments. Ubicomp 2002 Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing

[6.6] Jalal Al-Muhtadi, Roy Campbell, Apu Kapadia, M. Dennis Mickunas, and Seung Yi. Routing through the mist: Privacy preserving communication in ubiquitous computing environments. In Proceedigns of IEEE International Conference of Distributed Computing Systems (ICDCS), pages 65--74, Vienna, Austria, Jul 2002

7. Firewall

[7.1] Kara, A. Aizu Univ., Fukushima. Secure remote access from office to home ; IEEE Communications Magazine, Oct 2001 Volume: 39, Issue: 10 pp(s): 68-72

[7.2] Pho Duc Giang, Le Xuan Hung, Yonil Zhung, Sungyoung Lee, and Young-Koo Lee. A Home Firewall Solution for Securing Smart Spaces. IEEE Intelligent and Security Informatics (ISI-2006), May 23-24, 2006 San Diego, USA. ISBN: 3-540-34478-0. LNCS Vol. 3975/2006. pp 760-761

8. Cryptography

[8.1] W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, IT-22, 6, 1976, pp.644-654

[8.2] Simple public key infrastructure (IETF SPKI), Feb. 1998. http://www.ietf.org/html.charters/spki-charter.html.

[8.3] RFC 2015 - MIME Security with Pretty Good Privacy (PGP)

[8.4] Hassan Jameel, Riaz Ahmed Shaikh, Sungyoung Lee and Heejo Lee Human Identification through Image Evaluation using Secret Predicates to be published in Topics in Cryptology CT-RSA 2007, The Cryptographers Track at the RSA Conference 2007, San Francisco, CA, USA, February 5-9, 2007

[8.5] Eslami, Y.; Sheikholeslami, A.; Gulak, P.G.; Masui, S.; Mukaida, K. An area-efficient universal cryptography processor for smart cards. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Volume 14, Issue 1, Jan. 2006 Page(s):43 - 56

[8.6] Kartalopoulos, S.V. A primer on cryptography in communications. IEEE Communications Magazine, Volume 44, Issue 4, April 2006 Page(s):146 - 151

[8.7] Gennaro, R.; Randomness in cryptography IEEE Security & Privacy Magazine, Volume 4, Issue 2, March-April 2006 Page(s):64 - 67

9. Access Control: General

[9.1] YAMADA Shigeki (1) ; KAMIOKA Eiji. Access control for security and privacy in ubiquitous computing environments : Ubiquitous Networks. IEICE transactions on communications (IEICE trans. commun.) 2005, vol. 88, no3, pp. 846-856

[9.2] Geetanjali Sampemane, Prasad Naldurg, Roy H. Campbell, "Access Control for Active Spaces," acsac, p. 343, 18th Annual Computer Security Applications Conference (ACSAC '02), 2002.

[9.3] Urs Hengartner, Peter Steenkiste Carnegie. Access control to people location information. ACM Transactions on Information and System Security (TISSEC), Volume 8 , Issue 4 (November 2005

10. Matrix-based Access Control

[10.1] Lampson, B. W., “Dynamic Protection Structures,” AFIPS Conference Proceedings, 35, 1969, pp. 27–38.

[10.2] Ware, W. H., Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security, Santa Monica, CA: The RAND Corporation, February 1970.

11. Rule-based Access Control

[11.1] Bell, D. E., and L. J. LaPadula, Secure Computer Systems: Mathematical Foundations and Model, Bedford, MA: The Mitre Corporation, 1973

[11.2] Ramasubramanian, P. Kannan, A.. An active rule based approach to database security in e-commerce systems using temporal constraints ; . Conference on Convergent Technologies for Asia-Pacific Region TENCON 2003 Volume 3, 15-17 Oct. 2003 Page(s):1148 - 1152 Vol.3

[11.3] Al-Kahtani, M.A.; Ravi Sandhu; Rule-based RBAC with negative authorization 20th Annual Computer Security Applications Conference, 2004. 6-10 Dec. 2004 Page(s):405 - 415

12. Role-based Access Control

[12.1] David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli. Role-Based Access Control. Artech House Publishers (April 2003)

[12.2] D. Ferraiolo, R. Sandhu, S. Gavrila, D.R. Kuhn, R. Chandramouli, Proposed NIST Standard for Role-Based Access Control, ACM Transaction on Information and System Security, Vol. 4, No. 3, August 2001, pages 224-274

[12.3] Pereira, A.L.; Muppavarapu, V.; Chung, S.M. Role-based access control for grid database services using the community authorization service .; , IEEE Transactions on Dependable and Secure Computing. Volume 7, Issue 3, Sept. 2003 Page(s):202 - 207

[12.4] Joshi, J.B.D.; Bertino, E.; Latif, U.; Ghafoor, A. A generalized temporal role-based access control model. IEEE Transactions on Knowledge and Data Engineering, Volume 17, Issue 1, Jan 2005 Page(s):4 – 23.

[12.5] R. S. Sandhu, et al. "Role-Based Access Control Models", IEEE Computer 29(2): 38-47, IEEE Press

13. Discretionary Access Control (DAC)

[13.1] Vinter, S.T. Extended discretionary access controls Security and Privacy, 1988. Proceedings., 1988 IEEE Symposium on 18-21 April 1988 Page(s):39 – 49.

[13.2] Ninghui Li; Tripunitara, M.V. On safety in discretionary access control .; Symposium on Security and Privacy, 2005 IEEE 8-11 May 2005 Page(s):96 – 109.

[13.3] Sebes, E.J.; Feiertag, R.J. Implicit discretionary access propagation: a new interpretation of DAC. Proceedings of Computer Security

Foundations Workshop IV, 1991. 18-20 June 1991 Page(s):183 - 187

14. Mandatory Access Control (MAC)

[14.1] Thomas T. A mandatory access control mechanism for the UNIX file system. In: Proc. of the 4th IEEE Aerospace Computer Security Applications Conf. Dec. 1988

[14.2] Sailer, R.; Jaeger, T.; Valdez, E.; Caceres, R.; Perez, R.; Berger, S.; Griffin, J.L.; van Doorn, L.; Building a MAC-based security architecture for the Xen open-source hypervisor. 21st Annual Conference on Computer Security Applications , 5-9 Dec. 2005

[14.3] Yixin Jiang; Chuang Lin; Hao Yin; Zhangxi Tan. Security analysis of mandatory access control model ; IEEE International Conference on Systems, Man and Cybernetics, 2004 Volume 6, 10-13 Oct. 2004

15. Context-based Access Control

[15.1] . Zhang and M. Parashar. Dynamic context-aware access control for grid applications. In IEEE Computer Society Press, editor, 4th International Workshop on Grid Computing (Grid 2003), pages 101 – 108

[15.2] Antonio Corradi, Rebecca Montanari, Daniela Tibaldi, "Context-Based Access Control for Ubiquitous Service Provisioning," compsac, pp. 444-451, 28th Annual International Computer Software and Applications Conference (COMPSAC'04), 2004

[15.3] Weili Han, Junjing Zhang, Xiaobo Yao. Context-sensitive Access Control Model and Implementation. Fifth International Conference on Computer and Information Technology (CIT'05) September 2005 pp. 757-763

[15.4] Michael J. Covington, Prahlad Fogla, Zhiyuan Zhan, Mustaque Ahamad, "A Context-Aware Security Architecture for Emerging Applications," acsac, p. 249, 18th Annual Computer Security Applications Conference (ACSAC '02), 2002

[15.5] Shen Haibo; Hong Fan; A context-aware role-based access control model for Web services IEEE International Conference on e-Business Engineering, 2005. ICEBE 2005. 18-21 Oct. 2005 Page(s):220 - 223

[15.6] Shigetoshi Yokoyama, Eiji Kamioka, Shigeki Yamada, "An Anonymous Context Aware Access Control Architecture For Ubiquitous Services," mdm, p. 74, 7th International Conference on Mobile Data Management (MDM'06), 2006

[15.7] Gomez, L.; Moraru, L.; Simplot-Ryl, D.; Wrona, K.; Using Sensor and Location Information for Context-Aware Access Control The International Conference on Computer as a Tool, 2005. EUROCON 2005.Volume 1, 21-24 Nov. 2005 Page(s):68 – 71

16. Attribute-based Access Control (ABAC)

[16.1] Yuan, E.; Tong, J.; Attributed based access control (ABAC) for Web services Proceedings of IEEE International Conference on Web Services, (ICWS 2005) 11-15 July 2005.

[16.2] Keith Frikken, Mikhail Atallah, Jiangtao Li, "Attribute-Based Access Control with Hidden Policies and Hidden Credentials," IEEE Transactions on Computers, vol. 55, no. 10, pp. 1259-1270, Oct., 2006

[16.3] J.E. Holt, R.W. Bradshaw, K.E. Seamons, and H. Orman, “Hidden Credentials,” Proc. Second ACM Workshop Privacy in the Electronic

Soc., pp. 1-8, Oct. 2003

[16.4] N. Li, W.H. Winsborough, and J.C. Mitchell, “Distributed Credential Chain Discovery in Trust Management,” J. Computer Security, vol. 11, no. 1, pp. 35-86, Feb. 2003.

[16.5] K.E. Seamons, M. Winslett, and T. Yu, “Limiting the Disclosure of Access Control Policies During Automated Trust Negotiation,” Proc. Symp. Network and Distributed System Security, Feb. 2001

[16.6] Eric Yuan, Jin Tong. Attributed Based Access. Control (ABAC) for Web Services. Proceedings of the. IEEE International Conference on Web Services ICWS.2005

[16.7] Dongqing Xie; Yongjing Wang; Huayong Chen. A new role-based access control model using attribute certificate ; Fifth World Congress on Intelligent Control and Automation, 2004. WCICA 2004. Volume 5, 15-19 June 2004 Page(s):4335 – 4338

[16.8] Winsborough, W.H.; Jacobs, J.; Automated trust negotiation technology with attribute-based access control Proceedings of DARPA Information Survivability Conference and Exposition, 2003. Volume 2, 22-24 April 2003 Page(s):60 - 62

[16.9] Priebe, T.; Dobmeier, W.; Kamprath, N.; Availability. Supporting attribute-based access control with ontologies , The First International Conference on Reliability and Security, 2006. ARES 2006. 20-22 April 2006

17. Policy-based Access Control (PBAC)

[17.1] Demchenko, Y.; Gommans, L.; Tokmakoff, A.; van Buuren, R.; Policy Based Access Control in Dynamic Grid-based Collaborative Environment. International Symposium on Collaborative Technologies and Systems, 2006. CTS 2006. 14-17 May 2006 Page(s):64 – 73

[17.2] da Silva, J.F.; Gaspary, L.P.; Barcellos, M.P.; Detsch, A.; Policy-based access control in peer-to-peer grid systems The 6th IEEE/ACM International Workshop on Grid Computing, 2005. 13-14 Nov. 2005

[17.3] Koshutanski, H., Massacci, F., “Deduction, Abduction and Induction, the Reasoning Services for Access Control in Autonomic Communication”, proceedings of the 1st IFIP TC6 WG6.6 International Workshop on Autonomic Communication (WAC 2004), Berlin, Germany. Springer, October 2004.

[17.4] Demchenko, Y.; Gommans, L.; Tokmakoff, A.; van Buuren, R.; Policy Based Access Control in Dynamic Grid-based Collaborative Environment. International Symposium on Collaborative Technologies and Systems, 2006. CTS 2006. 14-17 May 2006 Page(s):64 – 73

[17.5] Maria Riaz, Saad Liaquat Kiani, Sungyoung Lee, Sang-Man Han, and Young-Koo Lee, "Service Delivery in Context Aware Environments: Lookup and Access Control Issues," The 11th IEEE International Conference on Embedded and Real-time Computing Systems and Applications (RTCSA 2005), 17-19 August 05, HongKong

18. Trust-based Access Control (TBAC)

[18.1] J. Park et al. The UCON_{ABC} usage control model. ACM Transaction on Information and System Security 2004

[18.2] Elisa Bertino et al. Secure knowledge Management: Confidentiality, Trust, and Privacy. IEEE Transactions on Sys. Man, and Cybernetic, May 2006

[18.3] Ninghui Li et al. Design of a role-based trust management framework. IEEE Symposium on Security and Privacy (SP) 2002.

[18.4] T. Ryutov, L. Zhou, C. Neuman, N. Foukia, T. Leithead, and K. E. Seamons. Adaptive Trust Negotiation and Access Control for Grids. 6th IEEE/ACM International Workshop on Grid Computing, Seattle, WA, November 2005.

[18.5] N. Li, J.C. Mitchell, and W.H. Winsborough, "Design of a Role-Based Trust Management Framework," Proc. IEEE Symp. Security and Privacy, pp. 114-130, May 2002

[18.6] Nathan Dimmock et al. Risk models for trust-based access control (TBAC). Third Annual Conference on Trust Management (iTrust 2005), LNCS, May 2005

[18.7] N. Dimmock et al. Using Trust and Risk in Role-Based Access Control Policies. Proceedings of Symposium on Access Control Models and Technologies, ACM, 2004

[18.8] Adams, W.J. Davis, N.J., IV . Toward a decentralized trust-based access control system for dynamic collaboration. Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005.

[18.9] Dimmock, N.: How much is 'enough'? Risk in trust-based access control. Proceedings of the Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'03).

19. Hybrid Access Control

[19.1] Le Xuan Hung, Nguyen Ngoc Diep, Yonil Zhung, Sungyoung Lee and Young-Koo Lee. A Flexible and Scalable Access Control for Ubiquitous Computing Environments. IEEE Intelligent and Security Informatics (ISI-2006), May 23-24, 2006 San Diego, ISBN: 3-540-34478-0. LNCS Vol. 3975/2006 pp 688-689

[19.2] Nguyen Ngoc Diep, Le Xuan Hung, Yonil Zhung, Syngyoung Lee Young-Koo Lee and Heejo Lee. Enforcing Access Control Using Risk Assessment. 4th European Conference on Universal Multiservice Networks (ECUMN) 14-16 February, 2007 - Toulouse, France