Access Control Challenges for Cyber-Physical Systems

Indrakshi Ray and Indrajit Ray
Computer Science Department
Colorado State University
Fort Collins, CO 80523-1873
{*iray,indrajit*}*@cs.colostate.edu*

Abstract

With the growth of wireless networks and mobile devices, we are moving closer towards an era of cyber-physical systems (CPSs). Such systems have the potential to benefit numerous applications in areas as diverse as military, financial, and health care. However, security issues must be addressed before CPSs can be widely deployed. The problem is serious because CPSs involve interactions between a large number of entities that can span different organizational boundaries. Unlike traditional applications, these applications do not usually have well-defined security perimeters and are dynamic in nature. Moreover, these applications use knowledge of surrounding physical spaces. This requires security policies to use contextual information that, in turn, must be adequately protected from security breaches. Uncontrolled disclosure of information or unconstrained interactions among entities can lead to very serious consequences. Traditional access control policies and mechanisms rarely address these issues and are thus inadequate for CPSs. New models and mechanisms are needed to protect such applications.

1. Motivation

With the growth of pervasive computing technologies, cyber-physical systems (CPSs) are becoming a reality. Such systems often use numerous, casually accessible, often invisible computing and sensor devices, that are frequently mobile or embedded in the environment and that are inter-connected to each other with wireless or wired technology. This allows CPSs to provide services and functionalities that use the knowledge of surrounding physical spaces. However, the very knowledge that allows CPSs to provide enhanced functionality can be exploited to cause security and privacy breaches. One must therefore ensure that the sensitive resources are adequately protected from unauthorized access. Addressing this problem involves understanding what resources an entity has access to, which entities it should interact with, what information can be released to an entity, how to protect the information used or produced by an entity, which entities can be trusted and to what extent, and how these trust relationships change over time.

Consider a potential use of such technology: real-time health care for patients in assisted living. A cardiac patient lives independently in a smart home equipped with sensors and wireless controllers. The patient's movements are tracked by sensors and wireless controllers send this information to a monitoring service that oversees the patient's condition and initiates appropriate action, such as, alerting emergency services. To operate, the monitoring service needs access to the patient's medical history maintained by a health care provider. In an emergency, these records must be shared with the admitting hospital which will perform examinations, such as X-rays and ECGs. The hospital may have to consult experts unfamiliar with the patient or search for similar reports to interpret the patient's case. Security and privacy are a major concern for such applications. Preventing data transmission to the monitoring service or sending false data may be fatal. Sending too many false alarms can cripple emergency services. Disclosing the patient's health data to prospective employers may cause financial hardship and disclosing the data to unapproved doctors causes breach of privacy. Comparing a patient's report to unauthentic reports of other patients may result in incorrect diagnosis. These severe consequences motivate the need to consider security issues when designing secure cyber-physical systems.

Cyber-physical systems are different from conventional information processing systems in that they involve interactions between the cyber world and the physical world. Thus, securing such systems involve

physical security, information systems security and, most importantly, securing the interaction between the physical world and the cyber world. Security policies and mechanisms developed for traditional applications are inadequate for cyber-physical applications for several reasons. First, these applications are complex and do not have a well-defined security perimeter – the entities that a system will interact with or the resources that will be accessed are not always known in advance. This makes almost all traditional access control models unsuitable for cyber-physical systems since they base the access decisions on the successful authentication of predefined users. Second, these applications are extremely dynamic in nature – the accessing entities may change, resources requiring protection may be created or modified, and an entity's access to resources may change while such systems are deployed. Protecting resources during application execution remains challenging. In fact, what constitutes secure operation in a dynamic environment is not yet known. Third, they use the knowledge of surrounding physical spaces to provide services. This requires security policies to use contextual information. For instance, access to a resource may be contingent upon environmental contexts, such as the location of the user and time of day. This contextual information can be used to infer the activities of the user and cause a privacy breach. Contextual information must, therefore, be protected by access control policies. Fourth, pervasive applications integrate the physical world with the cyber world. Thus, the effects of physical security must also be considered when designing access control policies. For example, if a change in environmental conditions causes the access control configuration to change, one must ensure that the sensors monitoring the environment are adequately protected. Fifth, applications in cyber-physical systems may need to interact, cooperate and share resources to accomplish a given mission. Secure interoperation in a dynamic environment is still an open problem. Last, but not least, cyber-physical systems often involve devices with various computation and communication capabilities, some of which are severely resource constrained. This will influence the access control mechanisms that can be used for such systems.

Researchers are working on various issues that may be important for cyber-physical systems. Examples include the development of new access control models and technologies [10, 13, 14, 18, 34, 35, 37, 41], formalizing the notion of trust [1, 5, 11, 12, 20, 21, 23, 26, 30, 32, 33, 38, 39, 44, 45, 47, 48], and trust management and trust negotiation strategies [3, 6, 7, 31, 40, 4, 46, 50, 51]. Some researchers [2, 8, 15, 24] have addressed security, privacy and trust issues of pervasive computing environments and others [9, 16, 36, 49, 53] focussed on trust-based approaches for communication in sensor and ad hoc networks. Researchers have also addressed the issue of secure interoperation to some extent [17, 19, 25, 27, 28, 29, 43, 52]. However, authorization and access control, which is often the first line of defense against security breaches, has not been addressed adequately in cyber-physical systems. What is missing is an access control model for cyber-physical systems that integrates both the cyber and the physical components of such systems and allows events in the physical world to interact with and change the access control configuration. Secure operation must be defined for dynamic environments and the cyber-physical systems should adhere to them. What is also missing is a notion of secure interoperation for cyber-physical systems where different systems will interact in a dynamic environment to achieve a common mission. Access control policies should ensure that additional security breaches do not occur because of the interoperation of the various systems.

2. Directions for Future Research

Our preliminary research indicates that access control for cyber-physical systems depends on the following factors: (i) trustworthiness of entities, (ii) environmental context, and (iii) application context. Trustworthiness of entities play an important role in access control. This is because cyber-physical systems have no well-defined security perimeters – interactions between entities may be unknown in advance. Moreover, since many entities in cyber-physical systems belong to the physical world, there is a need to integrate the effects of physical security into access control decisions in the cyber world. The overarching theme between the two types of access control – physical and cyber – is a notion of trust. The type of interaction an entity performs with another often depends on the trust relationship between the two. In traditional access control models, the notion of trust is implicit. That is, authenticated users are fully trusted and get all the associated permissions, whereas un-authenticated users are totally untrusted and get no permission. Treating trust as a binary concept – either an entity is trusted completely or not at all severely constrains operation in cyber-physical systems. On the other hand, complete trust may not be achievable every time because an entity may have only incomplete knowledge of its counterpart. Entities will not interact with untrusted counterparts. This will often result in unavailability of systems and services. Note, however, in the physical world access decisions are frequently made on varying degrees of trust.

One research task, therefore, is to formulate an appropriate non-binary trust model suitable for a cyber-physical environment. The model must accommodate the notion of different degrees of trust, identify how to quantify and measure the trust value for the various devices and users in cyber-physical systems, and define how trust evolves in a dynamic setting. One such general trust model, proposed by Ray et al. [33], shows how trust can be represented using Jøsang's opinion model [22], describes the factors on which trust depends, and shows how to quantify the trust relationship. A lot of work, however, remains to be done before such a model can be adapted for cyber-physical applications. One area that needs further research is investigating how to compute trustworthiness of different types of entities (device, user and data) that exist in cyber-physical systems, possibly in the absence of complete information. A second area of research involves providing a formal basis that allows one to compare the different trust relationships that exist in cyber-physical systems. Since multiple entities are involved in a cyber-physical system, a third area of research needs to focus on how to compute group trust in a dynamic environment.

The next task is to identify what types of access control policies are suitable for cyber-physical systems. Although a lot of research appears in security policies, not much of this is directly applicable to cyber-physical systems. Traditional access control policies do not consider environmental contexts, such as location and time, when making access decisions. Traditional policies assume a very static configuration and the mechanisms enforcing these policies are relatively easy to implement. In cyber-physical systems, the access control requirements change when the system context is modified. Consequently, new notions of secure access control in the context of dynamic systems are needed. The security models developed for cyber-physical applications should conform to them. In short, the research task is to identify the types of policies needed in pervasive computing systems, propose models that formalize their syntax and semantics, and propose a notion of secure execution for dynamic applications.

Environmental contexts, such as location and time, play a crucial role in access decisions of cyber-physical systems. For example, a paramedic can make major medical decisions while accompanying the patient in an ambulance, but may not be allowed to do once he is admitted. Thus, access control models must take into account environmental factors before making access decisions [34, 35, 42]. Application contexts, unlike environmental contexts, are very application specific. The application context depends on the data obtained from sensors and other devices. For example, in our example application, a patient may be hooked up to a system that continuously monitors his health. A sudden increase in the blood sugar level may trigger some action that gives an actuator permission to inject insulin to stabilize the condition. Each application context generates a specific configuration of the system. One must first define what it means for access control protection in a given application context, and also ensure that security breaches do not occur while the application context is being changed. For any given application context, the time and location of access together with the trustworthiness of the entities determine the access privileges of an user or a device. Note that, for a different application context, the privilege of this entity may change even if the other parameters (trustworthiness, location and time) remain the same. An access control model that captures all these requirements is needed for cyber-physical systems.

Different cyber-physical systems may need to interact to achieve a common mission. For example, if the smart home is on fire, the cyber-physical system of the fire department must interact with that monitoring the patient's health to accomplish the rescue mission. Under normal circumstances, these applications operate in isolation. However, in case of the rescue mission, all these applications need to interact and share resources to accomplish the goal. The issue is how to formalize the notion of secure interoperation that takes into account such ad hoc interaction among individual applications. This will require identifying the threats that can occur because of the interactions and what types of policies are needed to protect against those type of breaches. Secure interoperation requires an application to operate under different sets of policies. On one hand, the application must deal with its own policies. On the other hand, it must deal with the mission's policies. Conflicts might occur because of the interaction of different policies. Research is needed to identify how to detect and resolve conflicts. Conflict resolution should be such that it allows the mission to be accomplished without causing any security breach. Moreover, the effect of the different policies on the application must be analyzed to ensure that its execution is safe and secure.

Acknowledgment

This work was partially supported by the U.S. AFOSR under contract FA9550-07-1-0042.

References

[1] A. Abdul-Rahman and S. Hailes. Supporting Trust in Virtual Communities. In *Proceedings of the 33rd An-*

nual Hawaii International Conference on System Sciences, Maui, Hawaii, January 2000.

[2] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas. Cerberus: A Context-Aware Security Scheme for Smart Spaces. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications*, Dallas-Fort Worth, TX, March 2003.

[3] E. Bertino, E. Ferrari, and A. Squicciarini. Trust-X: A Peer to Peer Framework for Trust Establishment. *IEEE Transactions on Knowledge and Data Engineering*, 16(7):827–842, July 2004.

[4] E. Bertino, E. Ferrari, and A. C. Squicciarini. Privacy Preserving Trust Negotiations. In *Proceedings of the 4th International Workshop on Privacy Enhancing Technologies*, Toronto, Canada, May 2004.

[5] T. Beth, M. Borcherding, and B. Klein. Valuation of Trust in Open Networks. In *Proceedings of the 3rd European Symposium on Research in Computer Security*, volume 875 of *Lecture Notes in Computer Science*, Brighton, UK, November 1994.

[6] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis. The Role of Trust Management in Distributed System. In J. Vitek and C. Jensen, editors, *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, Lencture Notes in Computer Science State-of-the-Art Survey. Springer-Verlag, 1999.

[7] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 1996.

[8] R. Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane, and M. D. Mickunas. Towards Security and Privacy for Active Spaces. In *Proceedings of the Mext-NSF-JSPS International Symposium*, Tokyo, Japan, November 2002.

[9] S. Chakraborty, N. Poolsappasit, and I. Ray. Reliable Delivery of Event Triggered Obligation Policies from Sensors to Actuators in Pervasive Computing Environments. In *Proceedings of the 21st Annual IFIP TC-11 WG 11.3 Working Conference on Data and Applications Security*, Redondo Beach, CA, July 2007.

[10] S. Chakraborty and I. Ray. TrustBAC: Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems. In *Proceedings of the 11th ACM Symposium on Access Control Models and Technologies*, Lake Tahoe, CA, June 2006.

[11] S. Chakraborty and I. Ray. p-Trust: A New Model of Trust to Allow Finer Control over Privacy in Peer-to-Peer Framework. *Journal of Computers*, 2(2), April 2007.

[12] M. Clifford, C. Lavine, and M. Bishop. The Solar Trust Model. In *Proceedings of the 14th Annual Computer Security Applications Conference*, Phoenix, AZ, December 1998.

[13] M. J. Covington, P. Fogla, Z. Zhan, and M. Ahamad. A Context-Aware Security Architecture for Emerging Applications. In *Proceedings of the Annual Computer Security Applications Conference*, Las Vegas, NV, December 2002.

[14] M. J. Covington, W. Long, S. Srinivasan, A. Dey, M. Ahamad, and G. Abowd. Securing Context-Aware Applications Using Environment Roles. In *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies*, Chantilly, VA, May 2001.

[15] C. English, P. Nixon, S. Terzis, A. McGettrick, and H. Lowe. Dynamic Trust Models for Ubiquitous Computing Environments. In *Proceedings of the 4th International Conference on Ubiquitous Computing*, Goteberg, Sweden, September 2002.

[16] S. Ganeriwal and M. Srivastava. Reputation-Based Framework for High Integrity Sensor Networks. In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria, VA, October 2004.

[17] L. Gong and X. Qian. Computational Issues in Secure Interoperation. *IEEE Transactions on Software Engineering*, 22(1):43–52, January 1996.

[18] U. Hengartner and P. Steenkiste. Implementing Access Control to People Location Information. In *Proceedings of the Symposium on Access Control Models and Technologies*, Yorktown Heights, NY, June 2004.

[19] J. Jin and G. J. Ahn. Role-based Access Management for Ad-hoc Collaborative Sharing . In *Proceedings of the 11th ACM Symposium on Access Control Models and Technologies*, pages 200–209, Lake Tahoe, CA, U.S.A., June 2006.

[20] A. J. I. Jones and B. S. Firozabadi. On the Characterization of a Trusting Agent – Aspects of a Formal Approach. In C.Castelfranchi and Y.Tan, editors, *Trust and Deception in Virtual Societies*. Kluwer Academic Publishers, 2000.

[21] C. M. Jonker and J. Treur. Formal Analysis of Models for the Dynamics of Trust Based on Experience. In *Proceedings of the 9th European Workshop on Modelling Autonomous Agents in a Multi-Agent System Engineering*, Berlin, July 1999.

[22] A. Jøsang. A Subjective Metric of Authentication. In *Proceedings of the 5th European Symposium on Research in Computer Security*, volume 1485 of *Lecture Notes in Computer Science*, Louvain-la-Neuve, Belgium, September 1998.

[23] A. Jøsang. An Algebra for Assessing Trust in Certification Chains. In *Proceedings of the Network and Distributed Systems Security Symposium*, San Diego, CA, February 1999.

[24] L. Kagal, T. Finin, and A. Joshi. Trust Based Security in a Pervasive Computing Environment. *IEEE Computer*, 34(12):154–157, December 2001.

[25] D. Keppler, V. Swarup, and S. Jajodia. Redirection Policies for Mission-based Information Sharing . In *Proceedings of the 11th ACM Symposium on Access Control Models and Technologies*, Lake Tahoe, CA, U.S.A., June 2006.

[26] L. X. Li and L. Liu. A Reputation-Based Trust Model For Peer-To-Peer Ecommerce Communities. In *Proceedings of IEEE Conference on E-Commerce*, Newport Beach, CA, June 2003.

[27] D. Lin, P. Rao, E. Bertino, N. Li, and J. Lobo. Policy Decomposition for Collaborative Access Control. In *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies*, Estes Park, CO, U.S.A., June 2008.

[28] P. Mazzoleni, B. Crispo, S. Sivasubramanian, and E. Bertino. XACML Policy Integration Algorithms. *ACM Transactions on Information and System Security*, 11(1):1–29, February 2008.

[29] C. C. Pan, P. Mitra, and P. Liu. Semantic Access Control for Information Interoperation. In *Proceedings of the 11th ACM Symposium on Access Control Models and Technologies*, Lake Tahoe, CA, U.S.A., June 2006.

[30] S. Purser. A Simple Graphical Tool For Modelling Trust. *Computers & Security*, 20(6):479–484, September 2001.

[31] I. Ray, E. Bertino, A. C. Squicciarini, and E. Ferrari. Anonymity Preserving Techniques in Trust Negotiations. In *Proceedings of the Workshop on Privacy Enhancing Technologies*, Dubrovnik, Croatia, May 2005.

[32] I. Ray and S. Chakraborty. A Vector Model of Trust for Developing Trustworthy Systems. In *Proceedings of the 9th European Symposium on Research in Computer Security*, Sophia Antipolis, France, September 2004.

[33] I. Ray, I. Ray, and S. Chakraborty. An Interoperable Context Sensitive Model of Trust. *Journal of Intelligent Information Systems*, 32(1):75–104, February 2009.

[34] I. Ray and M. Toahchoodee. A Spatio-Temporal Role-Based Access Control Model. In *Proceedings of the 21st Annual IFIP TC-11 WG 11.3 Working Conference on Data and Applications Security*, Redondo Beach, CA, July 2007.

[35] I. Ray and M. Toahchoodee. A Spatio-Temporal Access Control Model Supporting Delegation for Pervasive Computing Applications. In *Proceedings of the 5th International Conference on Trust, Privacy and Security in Digital Business*, Turin, Italy, September 2008.

[36] K. Ren, T. Li, Z. Wan, F. Bao, R.H. Deng, and K. Kim. Highly Reliable Trust Establishment Scheme in Ad Hoc Networks. *Computer Networks*, 45(6):687–699, August 2004.

[37] G. Sampemane, P. Naldurg, and R. H. Campbell. Access Control for Active Spaces. In *Proceedings of the Annual Computer Security Applications Conference* , Las Vegas, NV, December 2002.

[38] B. Shand, N. Dimmock, and J. Bacon. Trust for Ubiquitous, Transparent Collaboration. In *Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications*, Dallas – Ft. Worth, TX, March 2003.

[39] G. Simmons and C. Meadows. The Role of Trust in Information Integrity Protocols. *Journal of Computer Security*, 3(1):199–209, 1994.

[40] A. Squicciarini, E. Bertino, E. Ferrari, and I. Ray. Achieving Privacy in Trust Negotiations with an Ontology-Based Approach. *IEEE Transactions on Dependable and Secure Computing*, 3(1):13–30, January-March 2006.

[41] M. Toahchoodee and I. Ray. On the Formal Analysis of a Spatio-Temporal Role-Based Access Control Model. In *Proceedings of the 22nd Annual IFIP TC-11 WG 11.3 Working Conference on Data and Applications Security*, London, U.K., July 2008.

[42] M. Toahchoodee, I. Ray, K. Anastasakis, G. Georg, and B. Bordbar. Ensuring Spatio-Temporal Access Control for Real-World Applications . In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*, Stresa, Italy, June 2009.

[43] J. Warner, V. Atluri, R. Mukkamala, and J. Vaidya. Using Semantics for Automatic Enforcement of Access Control Policies among Dynamic Coalitions. In *Proceedings of the 12th ACM Symposium on Access Control Models and Technologies*, Sophia Antipolis, France, June 2007.

[44] W. H. Winsborough and N. Li. Protecting Sensitive Attributes in Automated Trust Negotiation. In *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, Washington D.C., November 2002.

[45] W. H. Winsborough and N. Li. Towards Practical Automated Trust Negotiation. In *Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks*, Monterey, CA, May 2002.

[46] W. H. Winsborough and N. Li. Safety in Automated Trust Negotiation. In *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 2004.

[47] R. Yahalom and B. Klein. Trust-based Navigation in Distributed Systems. *Computing Systems*, 7(1):45–73, Winter 1994.

[48] R. Yahalom, B. Klein, and T. Beth. Trust Relationship in Secure Systems: A Distributed Authentication Perspective. In *Proceedings of the IEEE Computer Society Symposium on Security and Privacy*, Oakland, CA, May 1993.

[49] Z. Yan, P. Zhang, and T. Virtanen. Trust Evaluation Based Security Solution in Ad Hoc Networks. In *Proceedings of the 7th Nordic Workshop on Secure IT Systems*, Gjøvik, Norway, 2003.

[50] T. Yu and M. Winslett. A Unified Scheme for Resource Protection in Automated Trust Negotiation. In *Proceedings of the IEEE Symposium on Security and Privacy*. Oakland, CA, May 2003.

[51] T. Yu, M. Winslett, and K. E. Seamons. Supporting Structured Credentials and Sensitive Policies through Interoperable Strategies for Automated Trust Negotiation. *ACM Transactions on Information and System Security*, 6(1):1–42, February 2003.

[52] X. Zhang, M. Nakae, M.J. Covington, and R.S. Sandhu. Toward a Usage-Based Security Framework for Collaborative Computing Systems. *ACM Transactions on Information and System Security*, 11(1), February 2008.

[53] H. Zhu, F. Bao, R.H. Deng, and K. Kim. Computing of Trust in Wireless Networks. In *Proceedings of the 60th IEEE Vehicular Technology Conference*, Los Angeles, CA, September 2004.