DEVELOPING PERVASIVE TRUST PARADIGM FOR AUTHENTICATION AND AUTHORIZATION

by L. Lilien

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

Developing Pervasive Trust Paradigm for Authentication and Authorization[*]

Leszek Lilien

Department of Computer Sciences and
Center for Education and Research in Information Assurance and Security (CERIAS)
Purdue University
West Lafayette, Indiana, U.S.A.
llilien@cs.purdue.edu

Abstract

Trust plays a growing role in research on security in open computing systems, including Grid computing. We propose using trust for authorization in such systems. Traditionally, authentication and authorization in computer systems guard only user interfaces, thus providing only a perimeter defense against attacks. We search for an authentication and authorization approach that satisfies the requirements of defense in depth. After reviewing and classifying a variety of security paradigms, we propose the paradigm of *Pervasive Trust.* It is analogous to a social model of interaction, where trust is constantly —if often unconsciously— applied. In an initial study, we investigated using our trust paradigm as the solid conceptual basis for the perimeter-defense authorization solution developed in our lab: a *trust-enhanced role-mapping* server. The server improves role-based access control mechanisms by providing and managing trust ratings for users.

1 Introduction

Security and Trust in Grid Computing The pivotal role of *security* for Grid computing is emphasized by the definition of the *grid problem* as: *flexible,* secure*, coordinated resource sharing among dynamic collections of individuals, institutions, and resources—what we refer to as virtual organizations* [Fost01]. In turn, the importantance of *trust* in Grid computing becomes obvious in statements like:

> *One primary goal of such a Grid environment is to encourage domain-to-domain interactions and increase the confidence of domains to use or share resources (a) without losing control over their own resources, and (b) ensuring confidentiality for others. To achieve this, the „*trust*" notion needs to be addressed* [...]. [Azze02]

and:

> *We believe that fundamental to the establishment of a grid computing framework where all (not just large organizations) are able to effectively tap into the resources available on the*

[*] This research was supported in part by NSF Grants IIS-0209059 and IIS-0242840.

Cracow Grid Workshop (CGW'03), Cracow, Poland, October 2003

global network is the establishment of trust *between grid application developers and resource donors. Resource donors must be able to* trust *that their security, safety, and privacy policies will be respected by programs that use their systems.* [Chan02]

Identity and Trust in Access Control The traditional, *identity*-based approaches to access control are inadequate or even inapplicable to open computing, including Grid computing. The main reason is that outsiders have no identity that is meaningful to the system[†] [Wins03]. They are either unknown to the system or its administrator at all, or are known for too short a period of time, or are unable or unwilling to present enough appropriate credentials (such as a student ID) —in each case their intentions and dependability cannot be judged.

The approach of granting user privileges based on *digital credentials*, presented directly to the system, has its share of problems. First, such credentials can be forged, which limits their credibility. Second, trustworthiness of even legitimate credentials is no better than the reputation of their issuer [Bhar02]. In both cases the issue of *trust*, either in credentials or in their issuers, sneaks in —even if only implicitly.

Why, then, not to make *trust* the explicit basis for access control in open computing? This is exactly what we propose in our search for new solutions for two aspects of access control: *authentication and authorization (A&A)*. We need next to establish how to best use the notion of trust for A&A. We believe that putting our solution on a solid basis requires finding or devising an appropriate *trust paradigm* for A&A.

Paper Organization In the next section we consider some of the best known *old security paradigms (OSP's)*, discuss their failures, and show an example how a large legacy system deals with these shortcomings. Section 3 presents an approach to defining *new security paradigms (NSP's)*. After identifying requirements for NSP's and reviewing existing security paradigms, it defines our NSP of *pervasive trust*. Section 4 illustrates how this NSP can be used for trust-enhanced role-based access control.

2 A Brief Overview of Old Security Paradigms

Old Security Paradigms (OSP's) Let us take a quick look at just two of the best known OSP's. The first one is the *perimeter defense (PD)* or the *information fortress* paradigm [Blak96], with obvious analogies between a fortress (walls, guarded gates, passwords, inhabitants and property within, saboteurs or spies and Trojan Horses) and a computer system (security perimeter and firewalls, access control, passwords, system components such as hardware and data within, viruses or worms and … Trojan Horses).

[†] In fact, even *closed* identity-based systems use *identity* merely as a tag that is actually associated with evaluation —external to the computer system— of the user's intentions or dependability. For example, a legitimate student Adam Pulaski receives a password from a system administrator just because he is a *student*, that is, has been admitted to the student community. The very fact of being a member of a community known to be well-behaving as computer users is a sufficient recommendation for the system administrator. Access rights are not based on the fact that the user is *Adam Pulaski*, a person whose dependability as an individual is really completely unknown.

The second ubiquitous OSP is what can be called the *CoIA* paradigm (called *PIA* in [Gree98]), equating computer security with just the triple: confidentiality, integrity, and availability.

Failures of OSP's Both OSP's have served well in the old age of separated behemoths, when each computer was its own island with no links to others. With technology changes, they are no longer adequate. In an (intentionally) somewhat provocative opinion of a computer security pioneer [Wulf03], the "fatally flawed basic assumption of perimeter defense" (a.k.a. an information fortress) is the top reason why "computer security made little progress between mid 70's and mid 90's." Another expert [Jaha03] concurred. Both explained that PD can't cope with a number of security problems, including insider attacks and DoS attacks.

Example of Enhancing OSP in Legacy System Since OSP's are no longer sufficient, they need be at least enhanced, better yet replaced with *New Security Paradigms (NSP's).* The former approach is really the only alternative for large legacy systems, such as the air traffic control system operated by the Federal Aviation Administration (FAA) [Meeh03].

The FAA system uses both "classical" OSP's. First, FAA security approach uses the PD paradigm. This large "information fortress," with hundreds of large nodes, has only 8 well guarded "gates" connecting it with the Internet, with IDS's, firewalls, hardened routers, and antiviral software. Second, FAA uses *enhanced CoIA*, by adding *access control* and *authentication*, in this order, on top of CoIA.

3 Developing New Security Paradigms

Replacing OSP's with New Security Paradigms (NSP's) Enhancing OSP's might be a necessity in a short to medium term. Developing NSP's is required for a true progress in computer security.

Why exactly OSP's are not sufficient and must be replaced? One of the most important technological reasons is progress towards *pervasive computing*. Communication will no longer be dominated by human-to-human contacts (like e-mail or WWW). The balance will increasingly tilt towards device-to-device communication, with smaller and smaller devices —such as notebooks, PDA's, cell phones, multifunctional watches, embedded processors, and microsensors— getting bigger and bigger share of the data exchange pie [Deva03].

The next question is how to replace OSP's, that is, how to search for NSP's. We propose and follow a three-step approach: (1) consider principles and key concepts for NSP's, (2) review known security paradigms, and (3) devise an appropriate NSP.

Principles and Key Concepts for NSP's NSP's must fulfill a number of requirements based on needs and observations of shortcomings of OSP's. From the FAA perspective [Meeh03] among the key features of NSP's should be:

- Broad system approach
- Robust architecture with multiple layers of protection
- Constant vigilance
- Dealing with pervasive and global challenge to critical infrastructure
- Dynamic net configuration and automatic recovery

- Combining social and technological solutions

According to other source [Blak96], among the principles that NSP's should satisfy are these rules:

- Security should be inherent, not add-on
- Do not depend on identity, don't [just] authenticate it
- Good enough is good enough. Perfect is too good
- Adapt and evolve
- Use ideas of security from open social systems

A few of these requirements translate into the need to devise a paradigm enabling authentication and authorization (A&A) to confront security attacks not only with a perimeter defense, not even with multiple defense lines, but with *defense in depth*[‡].

Review and Examples of Existing Security Paradigms In our pursuit of a paradigm suitable for A&A, we have reviewed a large variety of general (broadly applicable) and specialized security paradigms. The richest source of NSP's are the annual New Security Paradigms Workshops [NSPW03].

Based on their origin, the security paradigms can be grouped into categories with sources in: (a) closely related areas of computer research, including reliability, integrity, fault tolerance, or concurrency control; (b) biological phenomena, such as human organism and immune systems, genetics, epidemiology, and ecology; (c) physical phenomena, such as diffusion and percolation; (d) mathematical theories, including the game theory; (e) artificial and natural models of animal and human social systems, including the military theories and sciences, and business and economic disciplines, esp. accounting and auditing.

Due to space limitations, only a few examples of NSP's are shown in Table 1 below.

Selection of New Security Paradigm The examination of both principles for NSP's and numerous proposed NSP's gave us valuable insights for devising a new paradigm to be used as a foundation for constructing an extended A&A mechanism.

On the basis of this analysis, a powerful social paradigm can be selected. It accommodates the principles and required key concepts listed above, including the principle of defense in depth which facilitates building lines of resistance at the perimeter of the system, between its components, and deeply within the system.

We propose the paradigm of *Pervasive Trust (PT)*[§], in which trust relationships are ubiquitous throughout the system and underlie interactions among arbitrary human or artificial components (such as arbitrary system modules). Since computing is becoming pervasive, and *pervasive security* is called for [Deva03], using the notion of pervasive trust is only natural.

PT is analogous to a social model of interactions, where trust is constantly applied in interactions between people, businesses, institutions, animals (e.g. a guide dog),

[‡] Software sensors and embedded detectors [Zamb01] can be seen as an example of realizing this idea

[§] PT is not just use of trust in pervasive computing environments. Instead, it means using trust *pervasively* in any computing system.

Table 1 Examples of New Security Paradigms

Paradigm Name	Source	Analogy To	Reference
Compromise Tolerance	computer science	fault tolerance	[Kahn98]
Optimistic Access Control	computer science	optimistic concurrency control	[Pove99]
Human vs. Computer	biology	human organism	[Will96]
New Availability Model	biology	epidemiology	[LinR98]
Insecurity Flow	physics	percolation theory	[Mosk97]
MANET[**] Security	mathematics	game-theoretic Prisoner's Dilemma	[Mich02]
SafeBot	social sciences	bodyguard	[Film96]
Traffic Masking	social sciences	deception – intelligence services	[Timm97]
Small World	social sciences	the small-world phenomenon	[Čapk02]

and even artefacts ("Can I trust in my car for this arduous trip?" [††]). We believe that in social systems trust is *always* used, whether explicitly in *open or dynamic* systems (e.g. by a new inhabitant of a big city asking around for a good doctor) or implicitly in *closed and static* systems (e.g. by a villager who knows everybody in her village so well that she uses trust unconsciously).

Using trust as a security paradigm requires many decisions, since it is a very complex and multifaceted notion. Therefore, we expect (and also experience) that different researchers apply this idea to computer security in diverse ways. Our preferences —derived from the application environments we envision— assign certain characteristics to Pervasive Trust. Among the major ones are the following:

- There are *degrees* of trust — trust is not just binary since one can trust more or less
- "You can't trust *everybody* but you have to trust *somebody*" — trusting nobody is paranoid, and therefore, extremely expensive in every way
- A "seller" (or a "buyer") is ultimately responsible for deciding on the degree of trust required to offer (or to accept, respectively) an interaction — there is no replacement for "personal" responsibility

An important issue is initialization of trust in situations when trustworthiness of an unknown entity must be evaluated by a permission grantor (e.g. when an unknown device asks an ad hoc network for a permission to join it). The are two simple solu-

[**] MANET stands for *Mobile Ad hoc NETwork*.

[††] The Merriam-Webster Dictionary (2002) says: "*Trust - assured reliance on the character, ability, strength, or truth of someone or something*. Thus, one can speak of trust even in relation to artefacts.

tions. Firstly, the entity may be granted permission for the most restricted access to the system (e.g. the mobile device may not be allowed to make any updates, and may be allowed to query for unclassified data only). Secondly, the permission grantor can search for the relevant, in the context at hand, reputation ratings on the entity and base its decision on these recommendations (which are a "second-hand experience").

Identity-based access control is inadequate in open environments (e.g., vulnerable to masquerading). Instead, trust values are used here for *attribute-based* access control, with a multi-dimensional attribute set.

4 Testing Use of Pervasive Trust for Access Control

Use of Pervasive Trust with Role-based Access Control In an initial study, in which only perimeter-defense was considered, our colleagues investigated use of trust for authorization [Bhar02, Terz02].

The capability to use trust ratings for users was applied for enhancing the role-based access control (RBAC) mechanism. Trust management is performed in this system by a *trust-enhanced role-mapping (TERM)* server, which interacts with an RBAC subsystem and a *reputation server* in the process of user authorization.

Trust Ratings and Evidence Trust ratings are assigned by TERM to both *regular users* and *recommenders*, who are users providing reputation information on others. TERM uses two kinds of evidence for producing trust ratings: (a) direct, first-hand experiences (i.e. user's behavior reported to TERM by RBAC), and (b) recommendations, that is second-hand opinions of users about others users. TERM does not accept recommendations at a face value. Instead, it assigns to them a trustworthiness rating, which reflects recommender's credibility as estimated by TERM.

Scenario A typical scenario includes the following steps: (1) user requests TERM for a role assignment; (2) TERM assigns a role to the user, if necessary interacting with a reputation server; (3) based on the role assigned by TERM, the user is granted permissions associated with the role; (4) the user accesses the system via RBAC; (5) behavior of the user in his interactions with the system is reported by RBAC to TERM; (6) TERM shares its trust ratings with a reputation server. When TERM has no direct evidence related to a new user in Step 1, it can either ask the user for credentials, or can query a reputation server for ratings assigned to the user by remote TERM servers.

Components of TERM Server The TERM server[‡‡] components are:

- *Credential Management*, which simply transforms diverse formats of different credentials to evidence statements
- *Evidence Evaluation*, which evaluates credibility of evidence statements
- *Role Assignment*, which assigns roles to users based on evidence statements and role assignment policies
- *Trust Information Management*, which evaluates user's/issuer's trust information based on direct experience and recommendations

[‡‡] Software for the TERM server is freely available at http://raidlab.cs.purdue.edu/zhong/NSFtrust as a part of the TERA prototype.

5 Conclusions and Future Work

Conclusions We have gained significant insights for devising new and more innovative security solutions by reviewing and reevaluating a broad selection of existing security paradigms. This valuable experience has been applied for devising a new paradigm of *Pervasive Trust*.

We have verified that the Pervasive Trust paradigm can be a solid conceptual basis for a perimeter-defense authorization solution developed by colleagues in our lab, namely the *trust-enhanced role-mapping (TERM)* server. Trust ratings provided and managed by TERM were applied for improving the role-based access control mechanism.

Future Work The Pervasive Trust paradigm needs be further exercised by extending solutions based on it in two dimensions: from just authorization to authentication and authorization, and from perimeter defense to defense in depth.

Acknowledgements and Disclaimers

Acknowledgements The author is grateful to all researchers from the RAID Lab (http://raidlab.cs.purdue.edu) for the creative ambience. Credit for many ideas, insightful comments, and suggestions on security and trust is due to Prof. Bharat Bhargava and Ms. Yuhui Zhong. Author also gratefully acknowledges influences of fellow participants of the *Trust, Privacy, and Security* breakout session at the NSF IDM Workshop (cf. [Bhar03]), and of the researchers visited at EPFL (e.g. [Aber01]).

Disclaimers A few of the references are for verbal presentations. Their contents were recorded by the author. Any possible inaccuracies or misstatement of the presenters' statements or intentions, for which he asks forgiveness, are solely his responsibility.

References

[Aber01] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," *Proc. of the Tenth International Conference on Information and Knowledge Management (CIKM01)*, New York, Nov. 2001.

[Azze02] F. Azzedin and M. Maheswaran, "Evolving and Managing Trust in Grid Computing Systems," *IEEE Canadian Conference on Electrical & Computer Engineering (CCECE '02)*, Winnipeg, Manitoba, Canada, May 2002.

[Bhar03] B. Bhargava, C. Farkas, L. Lilien, and F. Makedon, "Trust, Privacy, and Security. Summary of Workshop Breakout Session," *NSF Information and Data Management (IDM) Workshop* held in Sept. 2003 in Seattle, Technical Report, CERIAS, Purdue University, West Lafayette, IN, Dec. 2003 (to appear).

[Bhar02] B. Bhargava and Y. Zhong, "Authorization Based on Evidence and Trust," in *Proc. of Data Warehouse and Knowledge Management Conference (DaWaK)*, Aix-en-Provence, France, Sept. 2002.

[Blak96] B. Blakeley, "The Emperor's old armor," *Proc. Workshop on New Security Paradigms*, Lake Arrowhead, CA, Sept. 1996.

[Čapk02] S. Čapkun, L. Buttyan, and J.-P.Hubaux, "Small Worlds in Security Systems: an Analysis of the PGP Certificate Graph," *Proc. Workshop on New Security Paradigms*, Virginia Beach, VA, Sept. 2002.

[Chan02] B. Chang, K. Crary, M. DeLap, R. Harper, J. Liszka, T. Murphy VII, and F. Pfenning, "Trustless grid computing in ConCert," Technical Report CMU-CS-02-152, Carnegie Mellon University, Pitssburgh, PA, June 2002.

[Deva03] S. Devadas, M. Franz, A, Myers, P. Rogaway, and M. Singhal, "Pervasive Security," Theme Panel #3, *NSF Inaugural Cyber Trust Principal Investigators Meeting and Research Directions Workshop*, Baltimore, Aug. 2003.

[Film96] R. Filman and T. Linden, "SafeBots: a Paradigm for Software Security Controls," *Proc. Workshop on New Security Paradigms*, Lake Arrowhead, CA, Sept. 1996.

[Fost01] I. Foster, C. Kesselman, and S. Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," *Intl. J. Supercomputer Applications*, 15(3), 2001.

[Gree98] S.J. Greenwald, "Discussion Topic: What is the Old Security Paradigm?," Proc. *Workshop on New Security Paradigms*, Charlottesville, VA, Sept. 1998.

[Jaha03] F. Jahanian, "The Changing Internet Ecology: New Threats to Infrastructure Security," Keynote Address #3, *NSF Inaugural Cyber Trust Principal Investigators Meeting and Research Directions Workshop*, Baltimore, Aug. 2003.

[Kahn98] C. Kahn, "Tolerating Penetrations and Insider Attacks by Requiring Independent Corroboration," *Proc. Workshop on New Security Paradigms*, Charlottesville, VA, Sept. 1998.

[LinR98] M.J. Lin, A.M. Ricciardi, and K. Marzullo, "A New Model for Availability in the Face of Self-Propagating Attacks," *Proc. Workshop on New Security Paradigms,* Charlottesville, VA, Sept. 1998.

[Meeh03] D. Meehan, "Cyber Defense - The Confluence of Operations Research and Computer Security," Keynote Address #2, *NSF Inaugural Cyber Trust Principal Investigators Meeting and Research Directions Workshop*, Baltimore, Aug. 2003.

[Mich02] P. Michiardi and R. Molva, "Game theoretic analysis of security in mobile ad hoc networks," Research Report No RR-02-070, Institut Eurecom, Sophia-Antipolis, France, Apr. 2002.

[Mosk97] I.S. Moskowitz and M.H. Kang, "An Insecurity Flow Model," *Proc. Workshop on New Security Paradigms*, Langdale, Cumbria, United Kingdom, Sept. 1997.

[NSPW03] *New Security Paradigms Workshop*, The ACM Digital Library, Dec. 2003.
http://portal.acm.org/browse_dl.cfm?linked=1&part=series&idx=SERIES101&coll=portal&dl=ACM&CFID=12534085&CFTOKEN=3141410

[Pove99] S. Povey, "Optimistic Security: A New Access Control Paradigm," *Proc. Workshop on New Security Paradigms*, Caledon Hills, Ontario, Canada, Sept. 1999.

[Terz02] E. Terzi, Y. Zhong, B. Bhargava, Pankaj, and S. Madria, "An Algorithm for Building User-Role Profiles in a Trust Environment," in *Proc. of Data Warehouse and Knowledge Management Conference (DaWaK-2002)*, Aix-en-Provence, France, Sept. 2002.

[Timm97] B. Timmerman, "A Security Model for Dynamic Adaptive Traffic Masking," *Proc. Workshop on New Security Paradigms*, Langdale, Cumbria, United Kingdom, Sept. 1997.

[Will96] J. Williams, "Just Sick About Security," *Proc. Workshop on New Security Paradigms*, Lake Arrowhead, CA, Sept. 1996.

[Wins03] M. Winslett, Home Page, UIUC, Dec. 2003.
http://www.cs.uiuc.edu/people/faculty/winslett.html

[Wulf03] B. Wulf, "A Grand Challenge in Information Security," Keynote Address #1, *NSF Cyber Trust PI Meeting and Research Directions Workshop*, Baltimore, Aug. 2003.

[Zamb01] D. Zamboni, "Using Internal Sensors for Computer Intrusion Detection," Ph.D. Thesis, CERIAS Technical Report 2001-42, CERIAS, Purdue University, West Lafayette, IN, Aug. 2001.