Themes and Highlights of the New Security Paradigms Workshop 2000

Chair: Steven J. Greenwald
Independent INFOSEC Consultant
2521 NE 135 Street
North Miami, Florida 33181 USA
Web: http://www.gate.net/~sjg6
Email: sjg6@gate.net
Voice: +1(305) 944-7842
Fax: +1(305) 489-8129

Panelists: Simon N. Foley
Department of Computer Science
University College, Cork, Ireland
Email: s.foley@cs.ucc.ie
Voice: +353 21 902929
Fax: +352 21 274390

Cynthia Irvine
Code CS/Ic
Computer Science Department
Naval Postgraduate School
Monterey, CA 93943 USA
Email: irvine@cs.nps.navy.mil
Voice: +1 (831) 656-2461
Fax: +1 (831) 656-2814

Kai Rannenberg
Microsoft Research Cambridge, UK
St. George House
1 Guildhall Street
GB Cambridge CB2 3NH
Web: http://www.research.microsoft.com/users/kair
Email: kair@microsoft.com
Voice: +44-1223-744760
Fax: +44-1223-744777

Emilia Rosti
Dipartimento di Scienze dell'Informazione
Universit× degli Studi di Milano
Via Comelico 39
20135 Milano - Italy
Email: rose@dsi.unimi.it
Voice: +39-02-55006258
Fax: +39-02-55006253

Session Abstract

This panel will highlight a selection of some of the most interesting and provocative papers from the 2000 New Security Paradigms Workshop (NSPW), held 19 - 21 September in Ballycotton, County Cork, Ireland <`http://www.nspw.org`>. For nine years, NSPW has provided a productive and highly interactive forum in which innovated new approaches (and radical older approaches) to information security have been offered, refined, and published. This is a perennial and popular panel at NISSC.

In keeping with the NSPW philosophy, this panel will challenge many of the dominant paradigms in information security. It will be highly interactive; in the NSPW tradition we expect lively exchanges between the panelists and the audience. Come prepared with an open mind and a willingness to question and comment on what our panelists present and be sure to strap on your seat belt!

The panel will consist of four authors selected with great pain and difficulty from the great papers presented at the last NSPW. We have chosen these four with NISSC specifically in mind, using the criteria that they be the most interesting and provocative for you, the NISSC attendee.

Simon Foley's *Conduit Cascades and Secure Synchronization* promises to be a treat. If you happen to use, manage, or are just generally concerned with the security of Personal Digital Assistants (PDAs), then this is something you won't want to miss. Little concern has been given to the security policy implementations of these almost ubiquitous devices. Dr. Foley proposes a framework for analyzing the security vulnerabilities that can result from synchronizing PDAs with their host workstation. This also generalizes into the field of the problems associated with access control when systems are composed of secure and non-secure components. In short, we have a problem when PDAs are single-user systems with little or no access control, yet are expected to synchronize with multi-user host systems that have access control requirements; that synchronization can be used to bypass the access control on the host system.

Cynthia Irvine's *Quality of Security Service* promises to be especially interesting to anyone concerned with the security of the broad range of applications running in today's heterogeneous distributed systems. Should security be incorporated into the new paradigm of Quality of Service? We've all noted the contradiction that while security polices are rigid, we need flexible security implementations. What is proposed is the idea that security policies have ranges specifying lower bounds for implementation mechanisms and assurance. Mechanisms above that lower bound may be sufficient to meet functional and assurance requirements. The Quality of Security Service model has the goal of making security a flexible performance attribute for greater system manageability. This is important not just for the commercial world, but also for the military (*e.g.*, this can enhance survivability of tactical and operational systems).

Kai Rannenberg's *Multilateral Security* is a look at how things aren't as clear cut as we often assume. For example, we generally assume that there is no need to protect users from operators, that properly constructed security policies need only be enforced properly to maintain security, *etc.* However, these comforting abstractions don't always apply when the conflicting interests that we seem to be encountering more and more today are involved. In effect, we have competing security polices and requirements. If you've ever found yourself juggling different security policies and requirements, this should be of interest.

Emilia Rosti's *Disarming Offense to Facilitate Defense* is a critical look at how a strict host protection posture towards security can not suffice, and how our own systems can be subverted and used to attack other systems. This is a concern that all of us should have in this day and age where the "attack *du jour*" is all too common, and trusted hosts are all too often unwittingly involved in participating in criminal attacks. Disarming hosts via the use of filters is the proposed solution. If you are worried about your system being hijacked and then liable for an attack, being used for attacks by insiders, and similar things, then you're going to want to listen to Dr. Rosti's presentation.

Background of the audience you are trying to attract: We wish to attract audience members who are interested in the following items.

- New security paradigms.
- The latest challenges to the status quo.
- Provocative new work.
- A highly interactive panel with audience participation.

Conduit Cascades and Secure Synchronization

Simon N. Foley,
Department of Computer Science,
University College, Cork, Ireland.

The primary objective of this work is to propose an approach to analyzing the access-control vulnerabilities that can arise from using Personal Digital Assistants (PDAs) as part of an application system. While PDAs are typically single-user systems supporting little or no access-control, they are expected to synchronize with multi-user host systems that do have access-control requirements. This synchronization may be used to bypass host system access-controls.

For example, an employee working in sales and engineering departments is subject to the security requirement that sales data may not be written to engineering datasets. If we are not confident about the employee's PDA upholding this requirement then synchronization must ensure that at any one time, either sales or engineering information is carried on the employee's PDA, but not both. Other scenarios are possible, for example, the PDA carries both engineering and sales datasets for information purposes. However, only sales data can be two-way synchronized with the host system.

Achieving this security analysis requires a paradigm-shift on what an access-control policy represents. Conventional access-control policies specify the access constraints that are to be enforced by a protection mechanism such as a security kernel or security-wrapper based architecture. We depart from this view by assuming that an access-control policy defines the access-limitations that we believe to be reflected by a particular component; whether upheld explicitly by a protection mechanism or implicitly as a result of our belief in the way a component with no protection mechanism behaves. Thus, while a PDA such as a Palm handheld does not have an access-control mechanism, we can still specify, albeit with low confidence, the access limitations that we believe the installed software implicitly provides.

Our approach leads to a new paradigm for modeling and analyzing the access-control vulnerabilities of systems that are comprised of components of varying security. These components represent systems, handhelds, or alternatively, COTS components whose potential accesses are articulated as a security policy. It is not necessary for these components to have an *explicit* access control mechanism; the security policy represents the access limitations that we believe the component effectively upholds. Thus, in one sense, every component in the system can be regarded as contributing (in varying degrees) to the overall trusted computing base. In our framework we can distinguish the merit of each component's contribution. Security analysis determines how the interaction between these statements influences our confidence in security being upheld.

An Argument for Quality of Security Service

Cynthia E. Irvine
Department of Computer Science
Naval Postgraduate School
Monterey, CA 93943
irvine@cs.nps.navy.mil

Timothy Levin
Anteon Corporation
Monterey, CA
levin@cs.nps.navy.mil

Position Statement

In the past, computing jobs could be accomplished using a fixed set of resources and mechanisms that were specified *a priori*. Within that context, security was presented as an all or nothing choice. System designers were told that security policy enforcement had to be achieved using a particular set of mechanisms. Security engineers were considered pariahs bringing the plagues of inflexibility, incompatibility, and low performance to system development.

The world has changed.

The broad range of applications that must be executed in today's heterogeneous distributed systems requires an adaptable and responsive infrastructure. Because the load on hosts and the network that interconnects them varies, recent research has been directed toward the provision of Quality of Service mechanisms (QoSMs) to allow for control of choices.

Security must also be a part of the new Quality of Service (QoS) paradigm. How can security be flexible, when policy requirements appear to be rigid? First, security policies are not singular. The policy actually has a range: it specifies a greatest lower bound for the mechanisms and the assurance required for their enforcement. A range of mechanisms above that lower bound may be available that is sufficient to meet both functional and assurance requirements. Second, if security is included in a synergistic approach to QoS, then Quality of Security Service (QoSS) can be viewed as a component. When security resources present a range of acceptable choices, the QoSM can manage security as another QoS attribute just as it does network latency and bandwidth. Thus instead of being a performance burden, security is a flexible performance attribute that can contribute to the manageability of the system.

We have developed a model in which the provision of security services can be represented within an overall benefit function to characterize the level of QoS being provided to applications. Here, security is one of many factors, including precision, accuracy, and timing, that constitute the overall QoS solution space for distributed system effectiveness.

Quality of Security Service is introduced above in the context of commercial applications, but is especially pertinent to military systems where its management can enhance the survivability of tactical and operational systems. For example, a QoSS request can specify a range of possible security solutions such that if resources for the ideal choice are not available, secondary choices can be utilized to fulfill the mission.

Multilateral Security – Why and How?

Kai Rannenberg, Microsoft Research, Cambridge, UK, kair@microsoft.com

Many security approaches assume that it is quite clear who has to be protected against whom. E.g. the TCSEC focus on protecting system owners and operators against external attackers and misbehaving internal users. Protecting users against operators is not considered a major issue. Also it is often assumed that a security policy can definitively describe which actions are authorized and that it has only to be enforced properly to maintain a secure state. These clean cuts don't really apply when several parties with different or conflicting interests are involved, as e.g. in phone systems or the Internet:

- Subscribers need protection from others, especially from network operators or service providers monitoring their communication.
- Providers need protection from fraud, e.g. through unpaid and unaccountable calls, for which no subscriber takes responsibility.

Multilateral Security therefore aims at a balance between the competing security requirements of different parties. It takes into account the security requirements of all involved parties and also considers them as potential attackers. This is especially important for open communication systems, as one cannot expect the various parties to trust each other. Multilateral Security comprises:

1. Considering Conflicts:
   a. Different parties involved in a system may have different, perhaps conflicting interests and security goals.
2. Respecting Interests:
   a. Parties can define their own interests.
   b. Conflicts can be recognized and negotiated.
   c. Negotiated results can be reliably enforced.
3. Supporting Sovereignty:
   a. Each party is only minimally required to place trust in the *honesty* of others.
   b. Each party is only minimally required to place trust in the *technology* of others.

The Kolleg "Security in Communications" investigated Multilateral Security for communications and focussed on negotiation, secure infrastructures and evaluation criteria (cf. full paper in this volume describing e.g. a personal reachability and security manager). Six design principles helped the success of the projects:

1. *Data Economy*: The best design strategy to fulfil confidentiality requirements of users who have no control over their own personal data is the *avoidance of data*. Data that do not exist or are not transmitted need no protection from unauthorized use.
2. *Careful allocation*: If the creation of some data is unavoidable, *ownership* and *location* of such data have to be allocated carefully. Often data should be distributed among different parties (*decentralization*) to make misuse less attractive and to limit the potential consequences.
3. *User ability to control*: Where possible parties should be able to balance their own security requirements against those from others. In case of trade-offs between goals, users should be able to control the situation, e.g. by easy configurations and useful status information.
4. *Usability of security mechanisms*: Only usable mechanisms can be used. This challenge showed to be not an issue of offering *the* right solution to users, as *the* users don't exist, but to offer something for different users at different stages of interest and competence.
5. *Opportunities for individual negotiation*: Negotiation can only work if there are real options and opportunities to negotiate on. Enhanced technology can open further opportunities, but also economic and regulatory frameworks might be needed, e.g. to balance great differences in the power between the partners.
6. *Discernable security in products and services*: Better security can only be used and marketed if its advantages can be recognized. Enhancing the ISO/IEC Evaluation Criteria for IT Security [ISO/IEC 15408] and their sister document, the CC, was a step into this direction.

Much of this work was done when the author was at Telematics Dept., IIG, Freiburg University, Germany

Disarming offense to facilitate defense

Position Statement

E. Rosti
Dipartimento di Scienze dell'Informazione
Università degli Studi di Milano
Via Comelico 39, 20135 Milano – Italy
rose@dsi.unimi.it

The driving idea behind research in system security has always been devising methodologies, tools, and techniques to protect hosts from intrusions they can be victim of. Many useful solutions to improve computer systems protection were developed, such as firewalls, intrusion detection systems, network scanners, strong authentication mechanisms, were developed. However, the evolution of the computing arena, the shift of the computing paradigm towards a network centered computation, the rampant development of the e-society, have brought out some limitations of the "defensive" approach. In particular, we identify three security related problems for which no solution can be provided by "improving host protection measures":

- liability: the idea that computer users are responsible for the actions performed by their computer against other machines, even if they are not the actual actors, has become widespread in the legal world; as computer intrusions have become more and more popular, jeopardizing companies assets, legal prosecution of intruders is absorbing an enormous amount of resources, both public and private;
- system performance: security tools such as firewalls and intrusion detection systems introduce a delay in a networked system. With nowadays network bandwidths and speeds, such a delay is generally negligible. However, as network speed, bandwidth, and number of attacks increase, the delay introduced by the analysis of the incoming traffic is bound to become relevant;
- attack nature: some types of attacks, e.g., DoS and spoofing, cannot be detected at the target host. There are cases where heuristics are used to avoid them.

We propose a new approach to address security problems. Because a computer may as well be a victim and an attacker, if we want to reduce security threats, we should not only protect our systems but also prevent them from doing any harm. The new research direction for computer security we propose is the definition of new techniques and methodologies for developing non-offending, or *disarmed* systems. We define a *disarmed host* as *a host equipped with tools that turn off the host attacking capabilities and that force the host to be re-installed for it to be subverted.* The tools that turn off the offending capabilities can be thought of as filters that monitor the host activity and block it when it does not conform to a "good" behavior or, vice-versa, when it matches an "anomalous" behavior, depending on the approach followed. Such filters can be thought of as intrusion inhibitors and behave like intrusion detection systems on the attacking host. They can be effective in blocking activities that can be classified as attacks at the source host. Attacks that can be blocked at the target are well known to the security community since they have been among the major subjects of computer security studies. Their characterization has lead to the definition of signatures databases for intrusion detection systems. On the contrary, little if any characterization has been used of attacks from the source perspective in order to block offending activities as they are being performed at the source. As an example, attacks that use IP spoofing are easier to detect at the source but can hardly ever be detected at the destination, even if heuristics such as DNS reverse lookup may be adopted to discover the spoofing in most cases.

We believe that the disarming technology can be easily adopted in local environments. In this case, its deployment can provide an effective solution to problems such as liability, attacks from insiders, and insiders misuse of the organization's systems. The large scale deployment of a disarming technology would represent a further step towards a definitive answer to the problems of security tools performance and distributed tools for intrusion. Imposing such an approach, however, on a geographic scale and have it work is not an easy goal but we believe it to be a reasonable one. The proposed solution is not a silver bullet and could be bypassed by sophisticated users like any software protection. Nonetheless, disarming filters could be an effective protection against abuses by unexperienced users (the so called "script kiddies") that use ready made exploit programs down-loaded from well known Internet sites. They can also restrain the offensive capabilities of hosts that could be easily seized by crackers. Since we will implement them as kernel modules, an intruder who wants to bypass them would have to install a stripped version of the operating system, which may not be so immediate to do nor go so unnoticed. A hardware implementation based on ASIC technology could be adopted as encouraging results will be obtained and the approach further refined.