Personal Statement, *Angelos D. Keromytis*

Introduction

Increasing reliance on computers and communication networks has resulted from their advanced capabilities, which are most apparent in the Internet. This reliance has some undesirable repercussions, such as the risk of unwanted access to private, often critical, information. The move towards ubiquitous computing and networking will only exacerbate the problem.

Successfully addressing this security problem is hard. Some of the necessary building blocks are available: strong encryption and authentication algorithms, a few reasonably well-analyzed security protocols, "safe" programming languages, *etc*. Where new mechanisms are needed, security research can (more or less) reliably generate results. However, the integration and use of these results in real systems has been far from smooth. Indeed, one could argue that no significant progress in deploying large-scale security mechanisms has occurred thus far; solutions tend to be localized, reactive, and ad hoc.

We need not look far for the reasons behind this stalemate:

- *Manageability:* most security systems range from difficult to impossible to manage. As a result, if security is implemented, it is habitually circumvented or disabled by the same users or administrators that need it the most. From my point of view, the failure lies with:
    - *Management tools*. In particular, we need robust and scalable mechanisms for specifying, verifying, distributing, and enforcing **security policy,** especially in large networks. Of particular interest are **market-based** approaches to management, which could lead to, at least partially, self-managing systems.
    - *Evolution*. Software maintenance tends to account for a significant part (estimates place it at around 90%) of a system's cost over time. Furthermore, since systems are deployed with security vulnerabilities, mechanisms for automatically updating the components of a large network are clearly needed. An approach borrowing elements from **active networking** could be applied in this problem.
- *Security education:* until recently, network security was a major priority only for the military and intelligence communities. Despite some increased awareness of the security problem, products, systems, and networks are designed and deployed with minimal or no security (or worse , with *bad* security). The main reason is that computer professionals have not been trained to consider this aspect of system design, as they have been taught about programming, networking, algorithms, *etc*.

An academic environment addresses both of these issues: it provides an excellent environment to conduct and disseminate security research without military or commercial constraints. Perhaps more importantly, the next generations of students can be educated in this essential part of systems design.

In the next few pages I describe my research, teaching goals, and future research directions in computer and network security.

Research Focus

Improving security involves a careful mix of two research paths: first, the *core* security mechanisms must be properly designed and implemented; then, management of those mechanisms must be tractable, efficient, and ultimately, usable. In both cases, a necessary prerequisite is an experimental computer science approach, based on experience with real systems.

In my undergraduate years at the University of Crete, I worked first as a systems administrator for the University of Crete Computer Center, then as a network engineer for ForthNet (initially a public-funded entity for providing Internet connectivity, now the largest ISP/ASP in Greece). In both positions, I was faced with an impossible management situation due to lack of proper management tools; when these existed, they were typically developed in-house and provided an ad-hoc solution to a specific problem. Although there was considerable goal overlap between the tools I had to use or develop in both environments, each introduced its own view of the world and peculiarities. The need for a more methodical approach to security management was apparent.

In 1996, I joined the Distributed Systems Laboratory, at the CIS Department of the University of Pennsylvania, working with Dr. Jonathan Smith. As part of my research and in collaboration with Matt Blaze, Joan Feigenbaum, and John Ioannidis (AT&T Research), I developed the **KeyNote** trust-management system, a simple and flexible system that unifies the notions of security policy, credentials, access control, and authorization. KeyNote provides a uniform syntax and flexible processing mechanism for handling the security policy requirements of different applications. As part of the design process, KeyNote was constructed to have provable properties with respect to correctness and safety of operation. Thus it provides a good basis on which we built management tools for such diverse applications as IPsec [BIK01-1], distributed firewalls [BIKS00], micropayment and digital rights management systems [BIK01-2], and a market-based resource control architecture for active networks [AHIKS00].

Having built many of the mechanisms necessary for system and network management, the next logical step was to develop an architecture for managing the security of large, diverse networks, more flexible and efficient way than is currently available. The **STRONGMAN** project has become the focus of my thesis work. STRONGMAN builds on KeyNote to provide a scalable and extensible architecture for handling security management. The main three concepts introduced are lazy instantiation of policies, decentralized management, and policy layer interaction. KeyNote is used as a policy interoperability layer, and provides a syntax and policy resolution semantics common across all applications and network elements. Thus, STRONGMAN may be viewed as the glue that welds together a set of security components, each individual managed by KeyNote, into a coherent and manageable system.

Education

As I have already mentioned, I consider education a key to improving the security situation. However, education involves more than a simple one-unidirectional transfer of information. In my teaching experience, I have discovered that a more interactive approach to teaching is not only something I personally enjoy, but it also helps the students focus on the topic under discussion and discover on their own the concepts and principles behind it. This approach proved particularly effective in the course I taught in the Spring 1998 semester.

One particular course I would like to teach is a seminar with material from all of the core undergraduate classes, such as operating systems, architecture, networks, programming languages, *etc*. presented from the security point of view. A major focus of the seminar would be applying the gathered knowledge in the implementation of a team-based projects; doing a course project helps students understand the material, as opposed to just remembering it by simply reading it (or forgetting it after hearing it in a lecture). This "principle" of experimental computer science works equally well for graduate and undergraduate courses.

Future Work

STRONGMAN, through its use of KeyNote as a policy substrate, allows for policy evolution as security requirements change. However, this evolution is restricted by both the initial design criteria and the implementation of the specific protocols and applications managed by STRONGMAN. One solution to this is to introduce some measure of programmability in the enforcement mechanism itself. Work in the area of active networks should prove useful in this context.

Ubiquitous networking, especially with the advent of wireless networks and the expected appearance of Personal-Area Networks (PANs), significantly increases the potential risks to technology users. Lightweight devices are expected to come into contact with large numbers of other devices and interact with them with little or no knowledge on the part of the user. Support for mobility, and thus constant discovery and adaptation to new environments is needed in such networks. New security mechanisms and management techniques are needed for systems and networks of this type, if these are to become truly useful and not simply a new security liability. I believe the lessons learned from STRONGMAN and KeyNote, with respect to decentralized trust management, will prove particularly suitable in such environements. In particular, KeyNote can be overlaid by user-friendly (and intuitive) management mechanisms which allow easy and flexible configuration.

Finally, as recent studies have shown, a significant problem with computer security is the persistence of vulnerabilities in deployed systems, long after they have been discovered. Security patches are often not applied because of oversight or large overhead involved. Clearly, systems for automated distribution and application of patches are required. However, systems structure also has to change, to support graceful software updating. While there is both experience with such systems (*e.g.,* phone systems) and more recent research in the area, integration of such solutions has stumbled on the fact that they often require a clean slate in designing the system (*e.g.,* adoption of a safe programming language or underlying runtime system). Instead, we need an approach that gracefully accomodates incremental refinement and works well with existing projects. The open source community presents a good forum in which to study this problem and experiment with various approaches.

References

- [AHIKS00] Anagnostakis, K. G., Hicks, M. W., Ioannidis, S., Keromytis, A. D., Smith, J. M., "*Scalable Resource Control in Active Networks*".
  Proceedings of the *International Workshop for Active Networks (IWAN) 2000,* pp. 343 - 357.
  October 2000, Tokyo, Japan.

- [BIK01-1] Blaze, M., Ioannidis, J., Keromytis, A. D., "*Trust Management for IPsec*".
  To appear in Proceedings of the Internet Society *Symposium on Network and Distributed Systems Security (SNDSS) 2001.* February 2001, San Diego, CA.

- [BIK01-2] Blaze, M., Ioannidis, J., Keromytis, A. D., "*Offline Micropayments without Trusted Hardware*".
  To appear in Proceedings of *Financial Cryptography (FC) 2001.* February 2001, Cayman Islands.

- [BIKS00] Ioannidis, S., Keromytis, A. D., Bellovin, S., Smith, J. M., "*Implementing a Distributed Firewall*".
  Proceedings of the ACM *Computer and Communications Security (CCS) 2000,* pp. 190 - 199.
  November 2000, Athens, Greece.