

# Grand Research Challenges in IT Security and Assurance

Brett D. Fleisch  
Computer Science and Engineering Department  
University of California, Riverside  
Riverside, CA 92521  
brett@cs.ucr.edu

## Abstract

*This position statement presents five grand research challenges that need to be addressed over the next decade in Computer Security and IT Security and Assurance. These five areas include: the need to provide security for wireless devices and for Grid applications so that both can be used as commodity components for military applications, the need for theoretical breakthroughs and fundamental insights that could lead to better understanding of the principles and abstractions we are currently using for IT security, the need for better sandboxes and for sandboxes to become first-class abstractions, the need to keep our cell phones secure from viruses and worms, and the emergence of networked physical security and surveillance as a significant IT research area.*

## 1. Introduction

Ubiquitous wireless networks will support billions of Internet connected cell phones, embedded processors, handheld devices, sensors, and actuators; this will lead to radical new applications in biomedicine, transportation, environmental monitoring, and interpersonal communication and collaboration. The combination of wireless LANs, the third generation of cellular phones, satellites, and the increasing use of unlicensed wireless bands will cover the world with connectivity enabling both scientific research and increased emergency preparedness. Building on advances in micro-electronic mechanical systems (MEMS) and nanotechnology, smart sensors can be deployed widely, will be capable of multiple types of detection, and will survive for long time periods. The integration of real-time multisensor data with data mining across large distributed data archives opens further avenues for adaptive monitoring and observation, situational awareness, and emergency response.

## 2. Grid and Wireless Device Security for Military Applications

The military is reticent to use the Grid[1] and wireless devices remain a security problem. While there is tremendous power to be harnessed using the Grid and handheld devices, the security underlying these technologies must conform to DOD security directives. For example, the directives require nonrepudiated network authentication from the device to the network and Federal Information Processing Standard 140-1 or 140-2 accreditation with standard encryption technology. Pacom and DOD are doing a better job of sharing information internally and with coalition forces. Improvement has been attributed to IT solutions that are increasingly being built with the military in mind. Nonetheless, security sits squarely in the lap of future researchers and visionaries. A challenge over the next decade is to provide security, interoperability and scalability for the military that use wireless technology enabled by the Grid.

## 3. Theoretical Breakthroughs and fundamental advances in IS/IT

Principles of security espoused 30 years ago during the design of Multics by Saltzer and Schroeder[2] have been guiding defacto standards in secure system design. However, over the past several decades there has not been enough work to clarify and add insight into what theoretical properties these security policies admit.

Consider mobile code downloaded from the Internet. Schneider recently considers least privilege [2] for a base system and some extension (say downloaded code from the Internet) *Ext*. How does the base system obtain *Ext* and more importantly how does the base system obtain or compute the set of least privileges for *Ext*? Theoretical insights as discussed in [2] add understanding to the bounds and limitations of our policies and mechanisms. Fundamental insights and breakthroughs in the theoretical areas of computer security are needed in the future.

## 4. Sandboxing computations

A sandbox should become a *first-class* abstraction. There should be generic operations to create the sandbox, destroy the sandbox, to set certain quality of service that the sandbox provides. The sandbox should provide the ability to obtain a certain level of quality of service in terms of security provisions or in terms of performance that it provides. At times we prefer little security and very high performance; at other times exceptionally high security knowing a performance cost may be paid to perform additional security checks.

In addition, the sandbox should map to an implementation that may be considerably different in one environment than another. For example, after a sandbox object is “created” we would enter a user’s job in the sandbox. Specifically, after we create a sandbox we may insert a java applet into the sandbox before it executes. A mobile code applet could be best supported with Software Fault Isolation (SFI) through a binary rewriting tool. In other environments, it may be prudent to pay the cost to merely rely on separate address spaces to separate processes from one another and guarantee non-interference. The mapping of a sandbox could be to one computer, to multiple computers in a cluster or to a set of computers that form a Virtual Organization (VO)[1].

Sandboxes are a key abstraction to protection. Sandboxes should be generalized and should be mapped to a wide variety of implementations depending on the environment. In some circumstances the sandbox could map to a virtual machine; in other environments that sandbox may consist of a hybrid conglomerate of mechanisms specifically designed to support fault containment, isolation, and security. We therefore must address the issue of how to create sandboxes with different policy characteristics that pertain to local implementations. When sandboxes cross organizational boundaries we must mitigate policy differences to guarantee that local security policies are not violated and global policies with the computation are not compromised.

## 5. Keeping our phones secure from viruses

Future mobile phones are expected to become more sophisticated and simultaneously more prone to attack. Java, is the most significant of software languages that lets phones download software, and it is expected to be installed on more than 100 million phones by the end of 2003. Cell phones will support Wideband Code Division Multiple Access) networks and GSM/GPRS 900/1800 and 1900 Mhz frequency bands. These phones will integrate cameras with rotational 180 degree video capture of sound and still images. Internet access via WAP 2.0 allows these phone to stream data up to 384 kbs and offers download of application based on Java as well as connectivity to peripheral devices such as laptop computers using Bluetooth, USB or infrared. File formats such as MPEG-4 and music files like MP3 and AAC.

Expandable memory will be typically supported with snap-in memory cards.

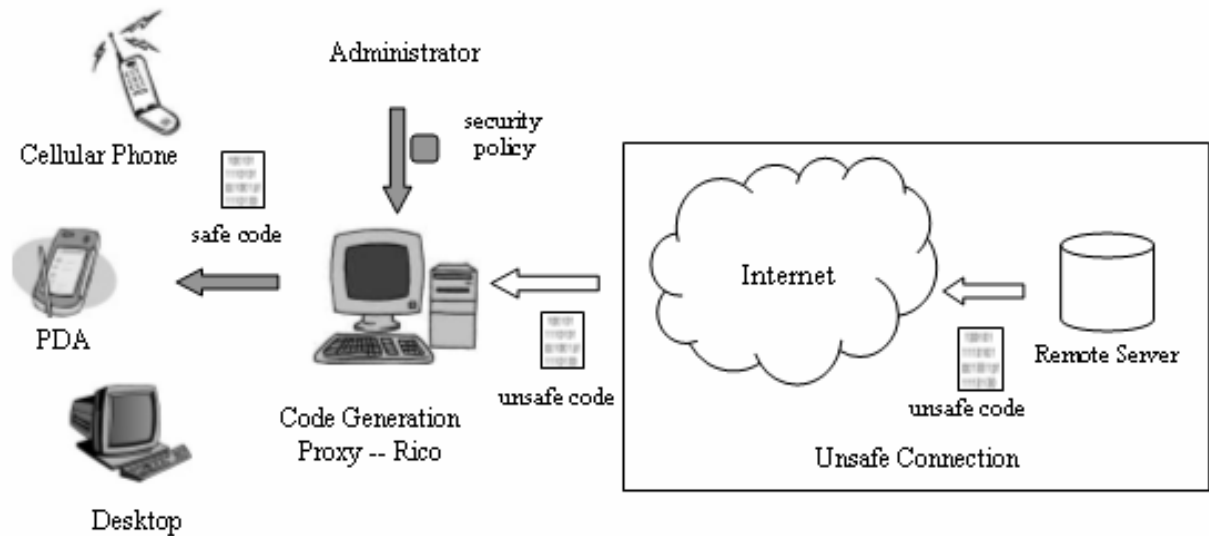
In March 2003, Santa Clara, Calif.-based Network Associates, a security software maker, called viruses an “emerging security threat” to mobile devices. Cellular providers must take proactive steps to keep our phones from becoming the fodder of hackers. There is no question that cell phones are becoming an indispensable part of our lives. Our research group is researching and deploying technology that can apply policies to executable applets to increase security and integrity of cell phones applications. Rico is shown in Figure 1 and discussed further in [4].

## 6. Physical Security Systems will become IP based and network Integrated

Video and other sensors have been traditionally used as a part of physical security. Physical security has been largely ignored by the IT revolution and the days of isolated CCTV systems are ending. IP-based cameras and integrated networked physical security systems have begun to displace coax-and-crt systems. A new conference in the area suggests that networked physical security systems can be viewed as a special case of sensor networks; however, the key research issues are often different. For example, video cameras place significant demands on both processors and network bandwidth. Since the primary goal is security, unlike other sensor network area issues, the issues associated with cyber security and encryption need to be addressed. A special conference in the area has been established to examine the issue of networked video surveillance, interaction of cybersecurity with physical security, network technology for physical security and emergency response, sensor fusion for security systems, coding/compression of networked video for security, and automated video detection/tracking[5].

## 7. References

- [1] The Anatomy of the Grid: Enabling Scalable Virtual Organizations. I. Foster, C. Kesselman, S. Tuecke. *International J. Supercomputer Applications*, 15(3), 2001.
- [2] The Protection of Information in Computer Systems, J. A. Saltzer and M. Schroeder, *Fourth ACM Symposium on Operating System Principles*, October 1973.
- [3] Least Privilege and More. F. Schneider, *Computer Systems: Papers for Roger Needham*. Andrew Herbert and Karen Sparck Jones, eds., 209--213. Revised version invited for *IEEE Security and Privacy in press*.
- [4] Rico: A Security Proxy for Mobile Code, Y. Song and B. D. Fleisch, to appear in *Journal of Computers and Security* Elsevier Advanced Technology, Elsevier Press, 2003.
- [5] IEEE International Conference on Information Technology: Coding and Computing (ITCC 2004), The Orleans, Las Vegas, Nevada, USA, April 5-7, 2004.



## 8. Biography

Professor Brett D. Fleisch is currently serving as Associate Professor of Computer Science and Engineering at the University of California, Riverside. He received the Ph.D. degree in Computer Science from UCLA in July 1989. He received the B.A. degree in Computer Science at the University of Rochester, the M.S. degree in Computer Science at Columbia University in 1981 and 1983, respectively. He joined the UCLA computer science department in September 1983 where he served as Research Assistant in the Locus group. His dissertation was entitled "*Distributed Shared Memory in a Loosely Coupled Environment*".

In the past, Fleisch has served as a consultant and summer employee at Xerox Corporation's, Webster Research Center, IBM Corporation's Thomas J. Watson Research Center, the Educational Testing Service in Princeton, New Jersey, The College Board (West Coast offices) and the State of California, Department of Motor Vehicles. In addition, he has also worked at Hewlett-Packard Laboratories, Carnegie-Mellon University, Locus Computing Corporation, and has served as a teaching assistant in the UCLA Computer Science Department. In January 2003 he recently spent a six month sabbatical period at the University of Illinois, Chicago working in conjunction with faculty there while cooperating with researchers at Argonne National Labs in Argonne, Illinois. His research interests are in operating systems, mobile code systems, security, DSM, fault-tolerance, reliability and availability. Dr. Fleisch has been funded by the National Science Foundation, Digital Equipment Corporation, International Business Machines

Corporation (IBM), Hewlett-Packard Laboratories, Computer Marketplace Incorporated, Sun Microsystems, the Office of Naval Research and the UC Micro program. Dr. Fleisch is a member of the ACM, IEEE Computer Society, and USENIX.