

IBM Research's impact on computer security includes such foundational cryptographic achievements as the Data Encryption Standard (DES) and the Hashed Message Authentication Code (HMAC), the groundbreaking ethical hacking work of the Global Security Analysis Lab, as well as innovative secure systems, such as the Postfix mailer program and the tamper-responding 4758 secure co-processor. Within IBM, technical work has resulted in advancing security-related tools in support of IBM Global Services, solutions for the Systems and Technology Group, and important contributions to security-related products for Tivoli Software. Current research spans a wide range of fields: from cryptography, digital image processing and biometrics to secure computer hardware, security engineering, and privacy management.

CRYPTOGRAPHY

Cryptography is the foundation for all computer and communications security and privacy. IBM researchers investigate a broad range of topics that span both fundamental theory and real-world applications, including the mathematical foundations of cryptography; the design and analysis of cryptographic functions and protocols; the study of general secure multiparty computation; and the specification of new standards for cryptographic applications. For example, researchers made essential contributions to the cryptographic design of Virtual Private Networks (VPNs) via the Internet Protocol Security (IPSec) and Internet Key Exchange (IKE) protocols, as well as to the design of the Secure Electronic Transaction (SET) protocol, standardized by the credit card industry for secure credit-card based payments over the Internet. IBM researchers have also put forth the fundamental notion of "universally composable" protocols that ensures security not only when run in isolation, but also when composed with other protocols. Another exciting line of research, pioneered and developed at IBM Research, is quantum cryptography, which investigates non-standard models of secure communications based on the inherent properties of photons.

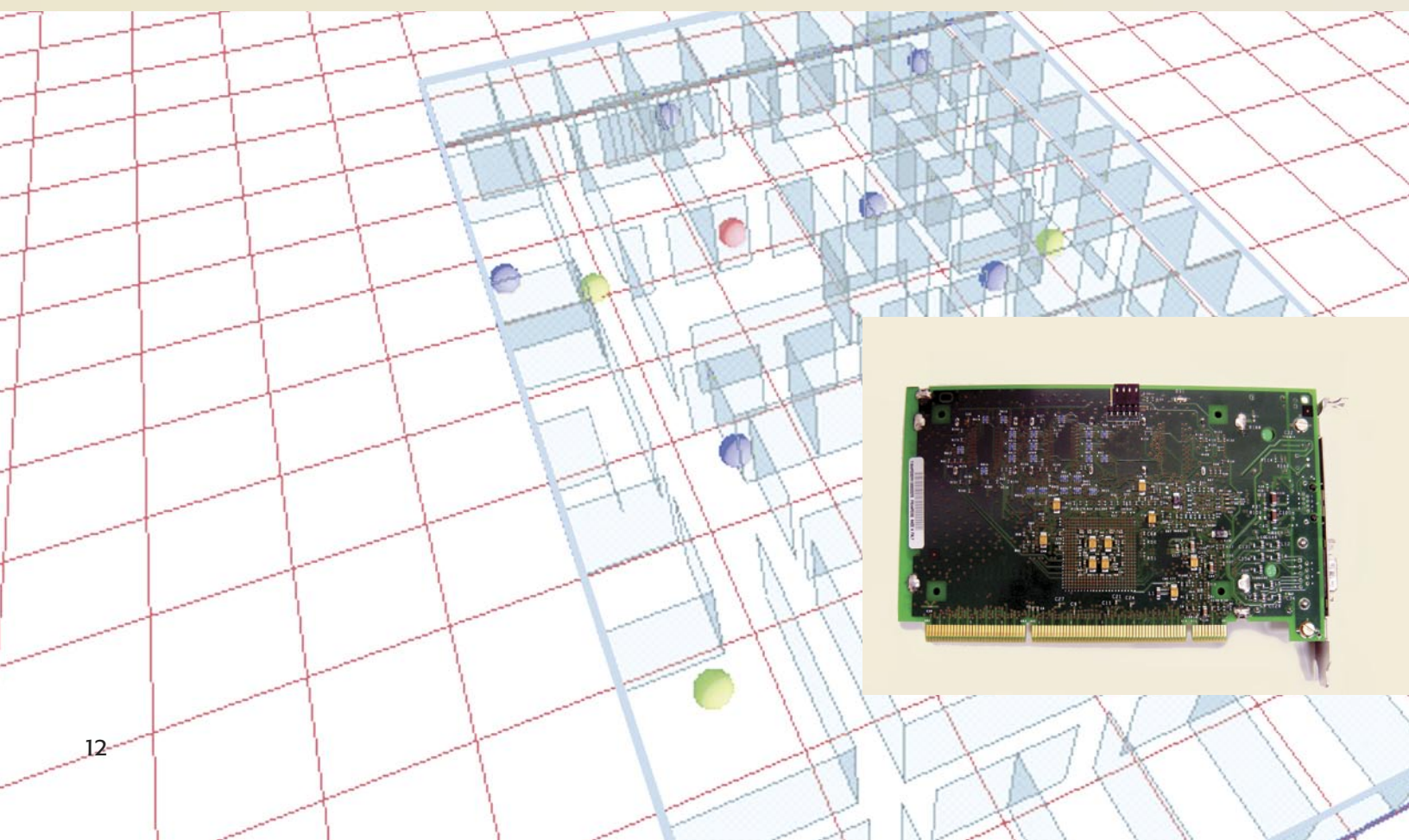
SYSTEMS SECURITY

IBM's integrity-based computing research seeks to provide stronger security guarantees by using hardware, virtualization technologies, operating systems, and middleware/ applications based on open software and standards, including open source contributions involving the Xen hypervisor, Trusted Computing Group's Trusted Platform Module (TPM), and the Linux™ operating system. One of IBM Research's accomplishments is enabling Xen to enforce controlled sharing among its virtual machines using mandatory access control policies. This allows multiple workloads to run on a single platform and share restricted resources, while still enforcing secrecy and integrity guarantees.

In another project, integrity measurement enhancements to Linux allow virtual machines to prove their integrity status to remote systems. Additionally, Linux security is being extended in a number of ways, including new authentication mechanisms that combine biometric authentication with secrets, and extensions to the Linux Security Modules framework to enable network access control that uses IPSec connections. Together, these system mechanisms provide the foundation for building trusted computing bases that span multiple Xen/Linux systems to support true, secure distributed computing. In particular, these advances facilitate the realization of Trusted Virtual Domains (TVDs), a new model developed by IBM Research for achieving IT and business security. TVDs provide an operating environment that has verified containment and trust properties, while greatly simplifying a user's role in specifying and validating these properties.

SOFTWARE ENGINEERING FOR SECURITY

IBM Research is using its experience in security analysis, the development of secure applications, as well as its broad expertise in programming languages, to improve the way software is engineered to attain security goals. Program analysis tools are being developed to find security flaws and enable their correction. These tools can be integrated with open source tools, including the GNU Compiler Collection (GCC) and the Eclipse platform. In addition, security evaluation tools are being developed to aid in software assurance and other security-specific tasks. Based on their extensive experience in building secure applications and knowledge of common security flaws, IBM researchers have developed a security engineering course to demonstrate effective practices that lead to designing and implementing more secure systems.



The secure coprocessor (1) consists of an inner copper enclosure (2), encapsulated in multiple layers of a tamper-sensing and responding membrane (3), and encased in resin (4).

