SECURITY AND TECHNOLOGY: A BETTER MOUSETRAP

Dennis S. Miyoshi and Mary W. Green

***Dennis S. Miyoshi** and **Mary W. Green** are with Sandia National Laboratories, Albuquerque, New Mexico. Mr. Miyoshi, who joined Sandia in 1969, is director of Nuclear Security Systems, where one of his interests is in using the technologies developed in his organization to deal with security at all levels of business and private life. He has a B.S. in physics from Stanford University, Palo Alto, California, and a Ph.D. in experimental physics from Cornell University, Ithaca, New York. Ms. Green is a technology transfer engineer for the Nuclear Security Systems Directorate, and has been with Sandia for seven years. She has a B.A. in music, B.S. in mathematics, and M.S. in statistics from St. Mary's University, San Antonio, Texas; and an M.S.in computer science from Trinity University, also in San Antonio.*

Sandia National Laboratories is the Department of Energy's lead laboratory in physical security research and development. It is now working to transfer this technology base to the private sectors, where we believe society will benefit greatly from improved security systems. We discuss projects that typify Sandia's efforts and exemplify the opportunities this technology provides.

Introduction

Concern for security pervades every aspect of our personal and working lives, from the domestic to the government level. Violent crime and fraud such as misappropriated government funds take a terrible toll on our national resources, and result in higher interest rates and lower productivity.

Developing and properly applying security-related technology can produce a mutually satisfactory scenario where technology develops concepts or hardware that create jobs, and the products reduce users' losses that would have resulted from crime and fraud. Efficiency increases, enabling users to lower prices and thereby gain a larger market share. If the user is a government agency, properly applied security measures reduce fraud and waste, thus reducing the cost of government.

Sandia National Laboratories has been involved in physical security technology for the past four decades to enable the Department of Energy (DOE) to properly protect U. S. nuclear assets. The passage of the National Competitiveness Technology Transfer Act of 1989 has allowed Sandia to support commercial physical security applications, and to adapt a broad spectrum of technologies to everyday security problems.

This paper outlines several security concepts that can be used to improve U. S. competitiveness. The ideas are descriptive rather than technical because of the preliminary nature of the concepts. We hope the reader can envision the broad scope of our approach to technology transfer, and can sense our excitement as we develop these ideas.

The Technology Base

Sandia has been involved in researching and developing security technologies for the DOE since emerging terrorist threats caused concern over protecting our nation's nuclear assets. Several hundred million dollars have been invested by the DOE in developing Sandia's expertise in physical security technology in such areas as technology testing facilities, analytical modeling tools, and systems engineering development.

This security technology also has been applied to solve problems in other government agencies such as the Department of Defense, FBI, Secret Service, the Drug Enforcement Agency, State Department, and Bureau of Engraving and Printing. Spin-offs from the security program have dealt with varied applications such as treaty verification, advanced conventional munitions, and nuclear non-proliferation.

The Present Challenge

Sandia National Laboratories, under the DOE's direction, is at work to transform this technology base into simpler, less-expensive technology that industry can use to solve everyday problems. We are also challenged to develop solutions that enhance, rather than burden, our operational efficiency to improve the national competitive edge. We would like to work with industry to understand their problems, apply security systems engineering principles to help solve them, and then develop technical solutions that industry can mass produce. We want to use the DOE-developed technology base in security systems as a springboard into other endeavors that could improve the United States' industrial competitiveness.

The Technology Transfer Program in Security Systems

Sandia has projects in the following areas:

- New innovations in security products
- Improving existing security products through test and evaluation
- Security concepts to improve operations
- Security concepts to reduce fraud and waste
- Industry-specific security system concepts.

New Product Innovations: FAX Machine Security. There is great concern in government and private industry about the proliferation of facsimile (FAX) machines. These machines provide an easy way to send copies of documents outside a facility with minimal chance of detection. Sandia is investigating alternatives to prevent the accidental or intentional misuse of these devices. One scenario involves developing a FAX network controller to capture the image being transmitted, analyze it, and intelligently determine whether the image is suitable for transmission to the recipient.

The controller could also handle multiple destinations and retransmittals, could block incoming "junk FAXs" from undesirable senders, and would maintain a "private" FAXbox for viewing only by an authorized user. Other features would include graded access control to the FAX machine up to and including biometrics (a *biometric* is a physical feature, such as a handprint, that can identify an individual), and the ability to analyze data on transaction information for audit purposes. Developing the FAX network controller is proceeding in stages aimed at allowing early implementation of a rudimentary capability such as image capture for random review; later stages would include image analysis and machine access control.

New Product Innovations: Firearm Control System. Another possible new security product is a "firearm control system" (or "smart" gun) that analyzes biometric information before allowing a firearm to be discharged. This feature would substantially reduce the chance of law officers being shot with their own weapons, and would eliminate accidental shootings by children playing with loaded firearms.

A biometric feature such as a handprint is used to characterize the individual holding the weapon. If there is a match between the handprint and the template stored electronically within the firearm control system, the firearm can be discharged. More than one handprint can be authorized, thereby allowing others to fire the weapon, or to allow firing with either hand.

New Product Innovations: Document Control System. As bureaucracy increases, so does the need for documentation. Many government agencies and private corporations are turning to *optical media* to store their documents. Many of these documents are sensitive or classified, and require protective measures for access control and audit trails. Sandia has developed a document control system for the DOE that can manage paper records as well as optical information. Its security features do not exist in other commercially-available systems. We currently have a standalone workstation, and are developing a local area network (LAN) version that will allow multiple users to share a common data file, input scanner, and printer. Individual workstations would only be able to read data files; any scanning or printing would be done at a central repository. A two-man rule to control the scanner and printer could be implemented for additional security; two authorized operators would be needed to activate the system. Because over 50,000 pages of typical typewritten paper can be stored on a single 5.25" optical disk, a roomful of paper records can be reduced to a few disks, especially because duplicate copies normally held by other individuals would not be needed.

Improving Existing Security Products. Sandia is assisting U. S. manufacturers in improving their security products in the face of foreign competition. This is helping improve the balance of payments, create new jobs, and improve the economic competitiveness of our security manufacturing industry.

In some countries, competition is government subsidized. This results in lower production costs and lower prices for the foreign product. Sometimes, the U. S. government buys cheaper foreign products, instead of technically-superior U. S. equipment, because of insufficient testing data. Our efforts can be as simple as providing testing, evaluations, and technical feedback to the manufacturer on performance, or as involved as a joint program co-sponsored by DOE to improve manufacturability, performance, and maintainability of the U. S. security product.

An area of current interest involves working with security equipment manufacturers on incorporating equipment testability within the product itself. Almost all present-day security equipment requires activating a "red-light" to indicate the alarm condition for testing purposes. Because of the large personnel investment required for validation, such a technique is unsatisfactory for products that must be field-certified for performance meeting statistical criteria such as a "90 percent detection probability with a 95 percent confidence level." An improved approach involves the manufacturer providing an analog output that shows signal strength. Thus, fewer tests would be required for equipment acceptability. Manufacturers that provide this feature will find their products much more attractive because of reduced life-cycle costs. We intend to encourage using testability features in the selection criteria for purchasing security products. Similar concepts can be applied to low-end consumer products as well, such as home security products.

Improving Operations: The AirFare Card. We are investigating the possibility of developing an AirFare Card that will reduce losses to airlines because of fraudulent use of stolen airline tickets. The AirFare Card will be the size of a computer punch card and will operate like many fare cards presently used on rail commuter systems such as the Metro in Washington, D. C. The magnetic stripe will also contain an authentication code the reservation system will recognize as validating issue by a legitimate source.

Instead of being centrally managed, the AirFare Card will depend on a distributed database originating at the passenger's departure airport. Only changes and updates would be transmitted to the central database, thereby reducing message traffic and single-point failures. The local computer will handle passenger check-ins, baggage matching, and real-time monitoring of passenger boardings at the loading gates. Local airline managers thus will have real-time information on the status of each flight leaving their airports. Data entry on boarded passengers into the airline's billing computer will be automatic. The AirFare Card readers at the boarding gates will prevent duplicate seatings, and will make it easier to board standby passengers. The problem of no-shows can be eliminated, which in turn reduces overbookings, leading to less customer dissatisfaction.

Improving Operations: Voting by Phone. We are working on the concept of allowing voting by phone. Today, voting at the polls requires time away from work and home, is costly to the city, county, and state government, and is a frustrating experience for the voter. Our concept involves technology to permit the equivalent of absentee voting, but institutes a procedure for identity verification and a user-interactive system for registering voter preference, all over a telephone line. Additional features include data encryption to prevent eavesdropping, and data authentication to prevent substitution of bogus information.

Sandia believes such a system would result in higher voter turnout, savings in time to the voter and his employer, and reduced government expenses. It would also allow issues to be brought to voter attention in a more timely fashion. Follow-on capabilities would allow computer interfaces by modems, with ballots displayed on terminal screens; pro-and-con discussions could be options pulled up on the displays; foreign language interfaces could be developed, as could interfaces for the hearing-impaired and visually handicapped.

Security Concepts to Reduce Fraud and Waste. Tens of billions of dollars are currently being diverted from government and private industry because of fraud and waste. Biometric information can help reduce this drain on our resources. By adding biometric identifiers to credit cards, checks, food stamps, ATM cards, and Social Security accounts, many current fraudulent practices could be eliminated. The technology exists today to achieve any desired level of identity verification. The challenge will be applying the appropriate systems engineering and convincing the user of the solution's practicality.

For example, 22,000 credit cards are lost or stolen in the U. S. every day. Many of these cards are fraudulently used, leading to $4 billion in losses to the U. S. consumer each year. Most of these losses can be eliminated by requiring the use of associated biometric information before allowing purchases to be made. A cost-effective biometric device for this application might be a voice verification system to assure that a purchase is being made by the person to whom the credit card belongs. Voice print templates would be stored at the same location as card validation information. Consumers would be asked to use a phone hand-set at the point of sale to communicate with the voice verification system right after the magnetic stripe on the credit card is read. The entire validation process would add about 10 seconds to each transaction.

Industry-Specific Security Concepts: Aviation Security. The current concern over the terrorist threat to the traveling public has resulted in an increased awareness of the need for high security measures at airports. To give the airline industry the necessary system concepts and technologies to address this threat, Sandia is working with the Federal Aeronautics Administration (FAA), airlines, airport operators, security engineering firms, and equipment manufacturers. All parties recognize the need to proceed from a system engineering perspective, and for operational test and evaluation to validate system design concepts. We intend to share the results of our efforts with the aviation community to optimize the use of technology, funding, and the protection of the traveling public.

Industry-Specific Security Concepts: Banking. Thousands of bank robberies take place in the U. S. each year, resulting in significant financial risk to bank customers. In addition, fraud and insider activity add over $10 billion in losses to the cost of operating the banking industry. We are currently working with banks in both areas, and have developed security system concepts for handling armed robberies. Some of the concepts being tested are not costly if they are built into the design of a banking facility. Concepts are also being developed to address the insider adversary. Some of Sandia's concepts involve a major overhaul of the way the banking industry operates. For example, tellers would continue to process transactions, but would not handle cash, which would be dispensed from an machine. Adding these security features has the potential to also improve banking operating efficiencies, giving "two bangs for the buck."

Conclusion

The security concepts presented here represent a few of the potential alternatives for enhancing the security and well-being of our nation. Other concepts being considered can directly improve the personal security of the individual. We are enthusiastic about the potential contributions that the DOE technology security base can return to the U. S. taxpayer in the form of cost savings, improved operations, and easier interactions with government.

(Manuscript received May 9, 1991)