Back to Report List

May 1, 2001

Dear Participants:

The following document is a summary of the presentations and discussions that took place at the International Workshop on Information Security, October 25-27, 2000. The organizers of this workshop would like to express their sincere appreciation to all of the attendees and presenters.

The workshop, which was held in behalf of the IAEA's Department of Safeguards provided useful information and personal contacts to Safeguards staff involved with the implementation of security measures in the Safeguards network and computer applications.

The workshop agenda is included in this summary report. The organizers of this workshop have attempted to summarize the presentation and discussions that took place in this 3-day workshop. We apologize in advance for any omissions or mistakes in our summary. Please be assured any errors are fully the responsibility of the reporters and not the participants or presenters.

We believe the workshop achieved its goals of providing the IAEA a sound basis for enhancing their information security program. The personal interaction between IAEA staff and the other workshop participants (not only during the workshop itself and the poster session, but also during a very delightful evening at the Farnitano's - thank you, again, Mike and Doreen!) permitted ample opportunity for exchange of information and experiences.

Thank you again to all participants. I hope you will find this summary report useful.

Best regards,

Nancy Suski
Lawrence Livermore National Laboratory

Mike Farnitano
Brookhaven National Laboratory

Foreward

The workshop comprised 4 sessions:

1. "Current Status and Trends". In this session, IAEA staff presented an overview of the Department of Safeguards, its work, its network and security configuration and ongoing application development projects that have significant security impacts.

2. "Planning & Implementing an Information Security Program". Speakers from US national labs as well as commercial vendors delivered presentations on important steps and components of an information security program.

3. "Technology Opportunities". Speakers from US national labs and commercial vendors covered various important issues of information security and methods, products and new technologies that can be used to address them.

4. “Closing Plenary & Roundtable”. The last session was presented by a speaker from the Gartner Group, Bill Malik, whose presentation, "Securing the Infocosm", provided excellent information on the steps required to put in place an effective security program.

Agenda

International Workshop on Information Security
Long Island, New York
25-27 October 2000

October 25, 2000
Session 1: Current Status and Trends

8:00 – 8:30 AM	Morning Coffee	
8:30 – 8:40 AM	Welcome & Logistics	S. Pepper, ISPO N. Suski, LLNL
8:40 – 10:00 AM	Keynote Address	Prof. James Chandler, NIPLI
10:00 – 10:15 AM	Break	
10:15 – 10:30 AM	Overview of IAEA & Safeguards Mission and Organization	K. Chitumbo, IAEA
10:30 – 10:45 AM	Safeguards Security Policy	M. Seits, IAEA
10:45– 11:05 AM	IAEA & Safeguards Network & Communications Infrastructure including Remote Monitoring	R. Simmons, IAEA
11:05 – 11:20 AM	Current Secure Ring Architecture	Schneider, IAEA
11:20 – 11:35 AM	Requirements for Additional Protocol Data System	Chtcherbinine, IAEA
11:35– 11:50 AM	Overview of Initiatives for Strengthen Safeguards Systems (SISTANet)	Robb, IAEA
11:50 – 12:15 PM	Current Security Configuration of Safeguards Network Insfrastructure with “gaps”; Current Security Projects, Plans for the Future	M.Seits, IAEA
12:15 – 1:30 PM	Lunch	

Session 2:	**Planning & Implementing an Information Security Program**	
1:30 – 2:30 PM	Threat and Security Awareness	B. Cleveland, LLNL L. P earson, LLNL
2:30 – 3:00 PM	Nuclear Facility Information Systems Threat Environment – Understanding Who & Why	S. Lee, Dyncorp
3:00 – 3:30 PM	Discussion	
3:30 – 4:15 PM	Infrastructure Assurance	L. Kannberg, PNNL
4:15 – 5:00 PM	Vulnerability Assessments –How Vulnerable is Your Network?	S. Talcott, Aquila Technologies
5:00 – 5:30 PM	Discussion	
5:30 PM	Adjourn to Reception at Farnitano Residence	
October 26, 2000	**Session 2 (cont'd)**	
8:00 – 8:30 AM	Morning Coffee	
8:30 – 9:15 AM	Designing a Risk Based Program	D. Sackett, LLNL
9:15 – 9:45 AM	Requirements for Internet Security & Integrity	S. Perry, Computer Associates
9:45 – 10:15 AM	Discussion	
10:15 – 10 :30 AM	Break	
10:30 – 11:30 AM	Planning & Implementing an Incident Response Capability	J. Rhodes, LLNL
11:30 – 12:00 PM	Discussion	
12:00 – 1:30 PM	Lunch	
1:30 – 1:50 PM	Data Surety Issues in International Monitoring	K. Tolk, Sandia
Session 3:	**Technology Opportunities**	
1:50 – 2:10 PM	TopTen Intrusion Detection – How to plan, procure, & implement an intrusion detection system	J. Hoover, Dyncorp
2:10 – 2:30 PM	Encryption, Network, Intrusion – Extending Security to the User	S. Talcott, Aquila Tech. & Oblix
2:30– 2:55 PM	Web Security – Scaling to the global enterprise; Cryptography & the Enterprise System	O. McCusker, Sonalyst
2:55 – 3:15 PM	Security Web Applications via PKI	J. Rome, ORNL
3:15 – 3:30 PM	Break	
3:30 – 3:50 PM	DOD PKI: Important Deployment Challenges	A. Ferguson, Pricewaterhouse Coopers, LLP
3:50 – 4:10 PM	StatePointPlus	H. Kopp, Westinghouse D. Pattrick, Sandia
4:10 – 4:40 PM	ICSA.net	A. Potter, ICSA.net
4:40 – 5:00 PM	Unauthorized Modem & FAX Misuse	G. White, SecureLogix

***5:00 – 7:00 PM Adjourn to Exhibit/Poster Reception**

Otober 27, 2000

Session 4: **Round Table Discussion**
Facilitator: William Malik, Gartner Group

8:00 – 8:30 AM	Morning Coffee	
8:30 – 9:30 AM	Assessment of the Information Security Industry	William Malik VP and Research Area Director, Application Integration and Information Security, Gartner
9:30 – 12:00 PM	Round Table Discussion	
12:00 PM	Adjourn	

International Workshop on Information Security

Long Island, New York
25-27 October 2000

Wednesday Morning, October 25.

Session 1: Current Status and Trends

Ms. Nancy Suski, Program Manager, Non-proliferation, Arms Control, and International Security opened the meeting. She welcomed the participants and thanked the International Atomic Energy Agency (IAEA) and the International Safeguards Project Office (ISPO) at Brookhaven National Laboratory for their help in setting up the meeting. Ms. Susan Pepper, Head, ISPO, then spoke briefly about the objectives of the United States Support Program (USSP) which is managed by the ISPO. The Program provides extra-budgetary assistance for research and development projects to resolve problems in technical safeguards. This is part of the IAEA's overall mission to verify that nuclear material placed under IAEA safeguards is not diverted for non-peaceful purposes. Such help enhances the IAEA's technical capabilities, development of equipment, acquisition and development of software, and aspects of training and recent improvements in network security. Mr. Michael Farnitano (ISPO) added his welcome and gave a brief outline of logistics and the structure that the meeting would take. The participants then introduced themselves.

Key Note Address:

The first speaker was Professor James Chandler (National Intellectual Property Law) who gave the Keynote Address, setting the stage for the discussions. He took us back to the early days of the IAEA during the Cold War before the Information and Security Sections were established. Already, computers were becoming increasingly important in controlling operations, and ensuring their security was important. Then, as now, the IAEA's vision was to control the spread of nuclear material that potentially could be used to make nuclear weapons and lower the threat of mass destruction. He outlined two major problems.

First, the problem of securing information is a pressing one and the scope and nature of the threat still is unclear and concealed. The wide availability of information could give people the knowledge to make a bomb. He suggested that knowledge must be considered as intellectual property and placed within a controlled environment. The second component is controlling the material needed to make weapons. This meeting will focus on the first component of the threat – controlling the flow of information to keep humans safe. The task is not easily achieved.

Chandler discussed the escalating changes in language used for programs, up to the 4th and 5th generation, that renders ineffective previous encryption. These later programs may be degraded upon transfer (de-compiled). If a hacker were to attack a compiled version, and de-compile it to its source code, then any vulnerability in the program would be revealed. Hence, any programs employed by the IAEA must take this into account. Their formidable challenge is to develop new programs that will control the dissemination of information to those who need it and restrict it for others. Once the data is free over the network, it can be compromised.

There was a short period for questions during which Professor Chandler noted that key codes were no longer needed for encryption; also, he discussed some of the former hurdles in getting encryption programs from the United States.

IAEA Presentations:

The presentations that followed, delivered by the IAEA's staff, covered the all-important aspects of maintaining information security at the Agency and specifically in the Department of Safeguards. Safeguards staff presented an overview of the Department of Safeguards, its work, its network and security configuration and ongoing application development projects that have significant security impacts. The presentations included information on the current status, projects in planning as well as areas where there are still gaps that need to be addressed.

Overview of the IAEA & Safeguards Mission and Organization

Dr. K. Chitumbo, IAEA, began with an Overview of the IAEA & Safeguards Mission and Organization. He covered a variety of topics: the statutes and safeguards agreement under which they operate; nuclear verification; integrated and strengthened safeguards; and, additional protocols. He described the ways in which IAEA adhered to the statutes and agreements, and how the inventory of nuclear material is verified. Traditional safeguards for nuclear verification that include material-accounting reports from States, records from the operators of the declared facilities, and verification through inspections. The strengthened Safeguards system includes activities such as unannounced inspections, the collection of environmental samples, the acquisition of satellite images, and acquisition and analysis of open-source data and, of course, the State's submission of Additional Protocol information. He emphasized that the Agency has already engaged in various activities to improve the security of its information systems, such as physically securing access to information by putting in doors with locks and limiting entry to rooms. The Agency has also recently instituted the requirement for its staff to sign a "confidentiality undertaking" to insure that employees upheld their requirement to keep information secret after they left the IAEA. He considers that the Agency faces an enormous effort in ensuring that the flow of data will be adequate for analyses, and for informing member states, but at the same time, will stay within security bounds. The lack of the monies might well jeopardize the ability of the Agency to install the needed layers of security, and, in such a restricted economic environment, the IAEA must balance maximum effectiveness and efficiency attainable against those resources.

Safeguards Security Policy

Monica Seits described in detail the Safeguards Security Policy. The Policy covers the following documents: IAEA Statutes and the Administrative Manual; Safeguards Agreements and the Manual; Board of Governor Documents; Policy Series; and, Information Systems Security Policy. The Agency maintains a stringent regimen to protect against the disclosure of commercial-, technological-, and industrial-secrets. The Board of Governors has requested regular reporting on the progress of implementing these security requirements.   regime includes the responsibilities for staff and non-staff as defined in the confidentiality undertakings, user security-awareness training and disciplinary measures, to be taken if there is an unauthorized release or disclosure by staff of such confidential knowledge . She discussed various Agency-wide policies in force covering such areas as the use of e-mail and the Internet described in the Agency's administrative manual. The Safeguards Manual, which includes policies and procedures specific to Safeguards, defines the Department's security policy and procedures. There are procedures for handling, storing, and analyzing confidential information. Access to information is based upon a hierarchical need-to-know level, with the Director having access to information on all countries for which their division is responsible, section heads seeing information only on countries for which their section is responsible; and inspectors only to relevant countries and facilities. She moved on to describe the safeguards for remote monitoring (SG Policy Series #16) which mentions the importance of data authenticity as well as confidentiality. Finally, Seits described some missing essentials in safeguards security programme: (1) Threat and risk analyses, (2) an integrated security policy for information systems, (3) a network configuration-management system, and (4) regular vulnerability assessments. She proposed to the Director a comprehensive security policy to include a system description, specific policies, a security program, operating procedures, and usage guidelines. It is now under review.

During subsequent questions, Seits stated that a threat and risk analyses must be performed before a detailed security policy could be defined. Insiders are generally considered as most likely to attack computer security, however, performing background evaluations of potential staff members in an international organization is not really feasible because of political implications. She also acknowledged the IAEA's problems with obtaining strong encryption technologies.

IAEA& Safeguards Network & Communication Infrastructure including Remote Monitoring

L. Simmons, IAEA, followed by describing the IAEA& Safeguards Network & Communication Infrastructure including Remote Monitoring which is founded on a Microsoftbasis. The services provided range from file and print, e-mail, Internet access, remote monitoring, secure remote access for inspectors, mainframe connectivity, and database services in Windows. The system serves 600 users, including those at regional offices. In several slides, he gave an overview of the network with the frame relay lines to

Vienna from Toronto and Tokyo, which have secure link encryption, and the Safeguards firewall and the Secure Ring firewall. He discussed IP traffic and its ease of maintenance and debugging. He showed the supporting hardware, with the Bay Networks Centillion switches, Bay Networks hubs, and the Cisco 2500 routers for frame relay. The use of Compaq's Insite Manager proactively monitors hardware performance. Additional frame relay links were established (South Africa, Korea) and a fifth in South America will soon be in place. He pointed out that there was 24-hour remote monitoring, with receipt of the information in Vienna in near real-time. Collected data are encrypted at the nuclear facilities, transmitted (sometimes by satellite) and then transmitted to Vienna either directly or via the field offices. Inspectors in Vienna must have the appropriate decryption key to see the data. Future plans were to move to Windows 2000 with its good management features and its security, and to Ethernet

Replying to questions, Simmons pointed out that the IAEA's office in South America has not yet been implemented because suitable accommodations had not been found. There was some discussion of the quality of the images obtained from the remote monitoring sites; he considered them satisfactory for analyses (most are taken every six minutes, at 20 Kbytes/picture). Presently, the software is being improved to enhance their quality.

Current Secure Ring Architecture

The following talk, Current Secure Ring Architecture, was given by C. Schneider, IAEA. The purpose of the ring was to secure the handling, movement, and storage of information classified as "highly sensitive safeguards confidential". He highlighted the very real problems in updating a legacy system that also needed much maintenance and correction. The hardware is dispersed physically throughout three operational divisions in Safeguards, and there is a firewall controlling the access from the general Safeguards network and the secure ring. For capturing information that had been stored only as paper documents, different scanner and OCR systems are in use, the data is stored in an encrypted form, however, neither the scanning and OCR systems nor the encryption system are user-friendly. . Although the sensitive data is encrypted, the main security issue is the physical security of the network. The secure ring consists of a number of PCs with Pentium processors and SUN Spark stations along with back-up devices for the data; all machines are located in physically secure access controlled rooms. PC Shield is the system used to encrypt the data where each operations division has their own "encryption domain". PCShield also allows for strict access control based upon a person's need to know privileges. Some people are able only to read the information; while others are also allowed to change it.

In the ensuing discussion, Chitumbo reiterated that the IAEA was aware of the much insecurity in their network. The system is complex with many levels of access controls required for confidential information; it has many users (including some 253 inspectors). Highly sensitive information must be securely protected, yet it must be possible to integrate it with other information. The IAEA found that if it were possible to access the sensitive information only from the few secure rooms inspectors would be reluctant to leave their offices to access the data - even the highly sensitive data must be made available to those who require it from their own offices

Requirements for Additional Protocol Data System

Chtcherbinine, IAEA, discussed some measures for an additional protocol system that had been taken or were contemplated by the Agency in his presentation, Requirements for Additional Protocol Data System. The additional protocol (INFCIRC/540) is part of a strengthened safeguards system whereby states send comprehensive information on their nuclear program to the Agency. The application that processes this data will need to deal with data from different countries, store it, and extract meaningful information from it. The predominant focus is on a stronger, more intrusive verification of the nuclear fuel cycle within a member country. By covering the nuclear cycle completely, from mining of the uranium to disposing of nuclear waste, it will strengthen the Agency's ability to detect undeclared activities and diversion of material, and verify its absence. It will provide inspectors access to information on all corresponding stages of the nuclear cycle. Approval is needed from the member countries for short-term access for inspectors. So far 53 have signed, and the protocol is in force in 16 states. Eight states have given initial declarations. The incoming data is classified as highly sensitive safeguards confidential, and comes from geographically separated areas. The submission can include support documents, such as maps. The IAEA has an in-house developed information system for capturing these declarations to which access is controlled.

All these files are needed for departmental analyses of the information. Specifications for a secure system are being written, users will be able to access the data from their workstations using two-factor authentication: "what you know" (domain account), and "what you have" (one-time passwords generated by SecurID card). The data passing on the network will need to be encrypted. Users have expressed their security needs, including strict measures against copying and printing entire declarations, preventing people from accessing other areas, and preventing the data and system administrators from seeing the information. The leader of the IAEA State Working Team will manage access to the data. There are plans to log all successful accesses and attempts to access the system: access will be disabled after a specific number of invalid access attempts. Data will be backed up encrypted, and the backups will run unattended. Hardware will be located in a controlled area and will be connected to an un-interruptible power supply.

The question was raised whether the information from the member states still comes as hardcopy. Chtcherbinine reported that it does, but the IAEA is helping them to send their data electronically. However, this is difficult for countries whose computer systems differ from those at the Agency. Dr. Chitumbo stated that all transmitted data must be encrypted but the systems are not yet satisfactory. There are security issues with authenticating information. The issue of allowing system administrators to read files was taken up again. The speaker discussed the possibility of Windows 2000 in preventing their access.

Overview of the Initiatives for Strengthening Safeguards Systems (SISTANet)

In his Overview of the Initiatives for Strengthening Safeguards Systems (SISTANet), Robb (IAEA) stressed the need to strengthen security for collecting and analyzing information from diverse sources, including commercial ones, such as satellite imagery, then making them accessible under one interface for inspectors. New tools implemented as part of the SISTANet project would include Verity's information server and a knowledge organizer to structure and query the data, as well as satellite imagery software tools, and a Geospatial Information System (GIS) both of which will be designed by experts. For this task, the IAEA will rely on member states to supply satellite imagery analysts, and a GIS expert. He illustrated the set-up of SISTAnet in a slide. While this system offers an excellent web-based tool, Robb was not certain how it will work with the proper security barriers. As yet, there is no single in-house policy for people using the new system from separate locations within the network. He speculated upon the appropriate architecture to be used for security - UNIX, NT, or others. The system chosen must be broad, robust, yet fine-grained, so that its continued operation does not depend upon the software vendor's services. It also must be flexible to accommodate access to diverse systems such as SQL, Verity Knowledge Organizer, and DWH. However, until security can be guaranteed, sensitive data, derived from analysis using the aforementioned tools and various data sources, must be isolated with stand-alone workstations, within a secure room, however, such measures are not always practical, nor solely sufficient. SecurID cards are practical for controlling access to data. He pointed out that, even open source data, when analyzed, may become more sensitive, and should probably be classified. The network or standalone security system must be such that operators and member states fully entrust SISTAnet with their information, to allow it to achieve its full potential as a highly efficient decision-making tool.

The questions centered on the thorny issue of how to protect data yet allow proper access to it. Cultural biases must be considered, along with problems of trust in choosing the security system.

Security in Safeguards SQL Database

The next speaker from the Agency, Wimalaratne, covered Security in Safeguards SQL Database. He first outlined the evolution of security in the IAEA databases, mentioning that the NT3.51/SQL 6.0 environment could implement security at SQL server and database level only, while the NT4.0/SQL7.0 could ensure its closer integration with the operating system. He covered the current SQL environment and the types of security available in SQL (NT authenticated security, and mixed security). He showed a slide with the SQL Server Security Decision Tree and the steps followed to connect to the server. He discussed access control through Fixed User Roles (server security, process, disk and database security) and Fixed Database Roles (access administration, backup facilities, data readers, data writers, denying data writing, and restricting public access). Both are created at the SQL Server installation and are sufficient to ensure security for most applications. He delineated the top-to-bottom hierarchy of users, from the system administrator (SA), the database owner (DBO), the user database roles (a group of users defined in database with specific security parameters. To ensure authenticated security, NT groups are created within a domain, the SQL server set to the NT-authenticated mode, NT groups added as SQL logins, database roles established in the SQL database, and NT groups added. He also considered the Permission Structure of the DB: First, Statement Permissions allow members of fixed server roles to execute Create and Backup SQL statements; Second, Object Permissions allow users to execute Select, Insert and Delete commands on tables, views and stored procedures. Access to base tables would not be encouraged and is granted through views only. Security for regional nuclear data is implemented at table row and column level. Wimalaratne described the advantages and drawbacks of some server encryption features in various NT/SQL versions, such as SQL log-ID, SQL passwords, NT passwords, and LAN Login ID and Application role passwords. He briefly touched on the IAEA's plans for the future that included NT-authenticated security only, database encryption, and enhanced security in a W2000/SQL 2000 environment.

Current Security Configuration of Safeguards Network Infrastructure with "Gaps"; Current Security Projects, Plans for the Future

Seits (IAEA) gave the final presentation of the morning: Current Security Configuration of Safeguards Network Infrastructure with "Gaps"; Current Security Projects, Plans for the Future. Her presentation was very comprehensive and clear, setting out the measures the Agency had in place, what they hoped to do in future, and what the pressing problems were (the gaps). She began by reiterating the IAEA's goals to protect the confidentiality and integrity of the data and assure its authenticity and availability. The Security Policy sets the baseline, and the Security Program manages the changes. Seits discussed ten major components of the program. The first, physical security, has gaps in that there is no protection for either the workstations or the cabling. Currently, there is VIC area UN security and ground passes, restricted access to the Safeguards premises, computing facilities and offices, attended file stations, and locked steel-cabinets. The second component, training and user awareness, includes a computer-based course (to be updated regularly) and security bulletins, and a new security video now in production. (The monies for this come from the USSP). There are gaps in enforcing the security policy. Currently, there are two CheckPoint Firewall-1/VPN-1 firewall systems (item 3), and plans to upgrade the main firewall and modernize the secure ring. In future, Seits would like to see individual firewalls on servers, integration of intrusion detectors and firewalls, and encryption of all network traffic. The gaps in intrusion detection are in obtaining and reporting performance data on the firewalls, and in identifying "back doors" to the LAN. Virus control is good (# 4) with scanning software for incoming mail, on LAN file servers, and as part of the "standard desktop". Users' machines are updated automatically.

Intrusion detection (# 5) is handled by ISS RealSecure, to which additional engines, system and database agents will be added. Problems center on (a) the lack of training in using current software, (b) firewall logs that are not integrated, (c) lack of agents for the UNIX system, and (d) the poor incident-response procedure. For user authentication and access control (the sixth component) security is well managed, and encompasses user I.D., strong passwords, screensavers, and "security by value" access to database records. An exciting project is underway to test authentication by fingerprints (biometrics), with the expectation of employing this in future. Seits would like to install two- or three-factor authentication, including Smartcards, and protection against booting a workstation.

The seventh component, secure remote access, suffers from weak encryption in the frame-relay links, and slow response times for VPN. Presently, PGP is used to encrypt sensitive remote e-mail, and a CheckPoint 3-DES VPN-1 with SecurID has been implemented for a hundred users. The Agency plans to issue additional VPN licenses and SecurID tokens for a total of 250 users, and test the VPN for secure transfer of remote-monitoring data. For data encryption and key management (#8), the speaker noted that only weak encryption keys are available in the IAEA. The implementation of the Entrust key management system has not yet been completed. There is a lack of training in the use of the key management system Entrust. The use of Entrust could be expanded in the future and integrated in other applications.

Disaster Recovery was the ninth component she listed. A plan was developed to improve the capacity for recovery. The recovery systems should be tested every second year in future. The IAEA could improve its disaster recovery capability by procuring redundant equipment and improving the coverage from service maintenance contracts. A network security audit - also called penetration test (component 10) was completed by KPMG during the first quarter of 2000. SGIT also receives security advisories that provide information for closing security vulnerabilities. Yearly network audits (penetration tests) are planned, the next being 3Q or 4Q 2001. She finished by re-emphasizing the support received from the USSP, and the continued need for it.

Dr. Chitumbo said that he hoped people would appreciate the extent of the IAEA's security problems, and would be able to offer advice on how they best might proceed.

Wednesday Afternoon.

Session 2: Planning & Implementing an Information Security Program

Threat and Security Awareness

In this session speakers from the U.S. National Laboratories and commercial vendors discussed important steps of an information security system. It was hoped that the IAEA might use this information as a useful tool in performing their threat and risk analyses, an important first step in defining a security program.
Dr. Cleveland, Lawrence Livermore National Laboratory, opened the session speaking on Threat and Security Awareness. His presentation focussed upon human factors in ensuring security of information, particularly the “insider” problem. Thus, even if all technical problems have been resolved, there is still the very real possibility of inadvertent or malicious compromise of sensitive data from people within the organization. He listed three main concerns: (a) Human error, such as sending e-mail before thoroughly checking its content, or chatting indiscriminately over lunch; (b) cyber attacks; and, (c) outside interactions with others. Included under the last heading is disclosure of critical material at conferences, loss of laptop computers during travel, and espionage. Spying is a very serious theft that destroys and ruins peoples’ lives.

There is no easy answer to the problems of human factors. It is useful to hire an expert in human behavior. However, educating the staff about security is essential. They must fully understand the specific threats, know how to recognize them, and how to and to whom they should report issues. Each day, much technical information is made public and is avidly soaked up by foreign countries. While this activity is benign, the employee must be aware that sensitive information also is aggressively sought. For example, a stranger on a plane may engage in conversation with an employee about their work. The employee then should act as a partner in security, and report the incident. Reporting must be a non-threatening and friendly experience for staff, otherwise they will avoid it; a recent survey showed that very few such encounters are reported.

The threat must be assessed, preferably by a person familiar with “human” security. It should include determining which persons are interested in the information, analyzing network intrusions and the likely methods used, and interviewing staff. Collaborations with other safety officers are invaluable.

Cleveland emphasized that cyber-security briefings of new employees are important, as are personal ones for travelers before and after their absences. Recent relevant facts on breaches of security can be sent to staff electronically or on paper, and guest speakers can be invited to discuss security. Apparently innocuous people who socially interact with employees should be considered; often, sensitive material is discarded in the trash, and so becomes available to everyone, including janitors.

Dr. Chitumbo stated that when IAEA employees leave the Agency they are debriefed and reminded that it is still their duty to protect information and report any threats. However, the Agency has no way to enforce their commitment; they hope that the member countries have such leverage.

Nuclear Facility Information Systems Threat Environment – Understanding Who and Why

The following speaker, Mr. S. Lee (Dynocorp) explained Nuclear Facility Information Systems Threat Environment – Understanding Who and Why. He spoke about the social-science approach to the problem, and about delimiting the general challenges to security from the technical ones. The motivations behind the threats may be based upon terrorism or upon historical- and social science-dimensions.

In the nuclear industry, safety and security are at high risk. If industrial processes are upset, the resulting hazards are enormous, such as if a hacker were to penetrate the core systems and take over control of the reactor. Security is high there, and a mitigating factor is that the typical hacker probably is unfamiliar with the controls. Peripheral systems may be more easily penetrated, and although the outcome may not be catastrophic for safety, there could be cascading effects on other systems. The threats could come from several sources. Adversaries of the state with high potential ability to destroy nuclear programs have a record of targeting them. Terrorists who are experienced in technology might launch a virus, however, terrorists have a weak record of effective attacks, either technological or physical ones, and there is no pattern of challenges from any established terrorist group. Opponents of nuclear power tend to focus on protests, especially disrupting the transport of nuclear material. Their ideological factions advocate cyber protection. Property crime is not prevalent in the nuclear industry where little profit is to be made.

Lee next described technology-enabled threat players, i.e., insiders with trusted access, and hackers. The former group is rarely a menace in the nuclear industry, as they are in other industries. Hackers may be more so, as they are often young males, driven by technology, competitive among themselves, and hard to control. They are acting not for profit but for excitement; they intrude into networks, and disseminate viruses (and have a poor understanding of how viruses evolve). Comparison of the mental attributes of these groups reveals that hackers have the highest ability but unpredictable motivation, insiders have high ability but awareness of the consequences, while opponents of the nuclear industry have middling ability, are focused on peripheral systems, and are fearful of environmental disaster. Terrorists have a limited record of attacking nuclear systems, and criminals are the least likely to pose a threat.

In the ensuing question time, Lee stated that process control in nuclear plants is dominated by stand-alone systems, although there is a growing tendency to put their control on the web. Still, enemies of the state would find it difficult to take control, and hackers are primarily interested in the challenge of highly evolved technologies. Terrorists may target substations. He cited the example of the 1998 defacement of the web page of the Bhabha Atomic Research Center that appeared to be a protest against nuclear weapons. Rather, from the bad language, faulty grammar, and lack of mainstream activity, it probably was the work of a typical hacker. Nevertheless, the incident underscored the vulnerability of peripheral systems.

Lee drew several conclusions. A security system should be based upon good technical processes, and the analysis of threats to an organization's cyber security integrated with those elsewhere in the world. Information security should be coordinated with site security and with the country's police force. A broad view should be taken of information security concerns, perhaps to the extent of checking on the background lives of new employees.

The questions centered on the security checks made by the Agency. Dr. Chitumbo stated that the IAEA does not undertake background checks, nor, as experience has shown, can they rely upon the member States to do so. Even a minimal check for a criminal record is difficult and would cost a great deal. Also, they do not hold debriefings when an employee leaves. However, the Agency does not employ known hackers. Suski pointed out that it would be possible for a malicious former member of staff to get into the information system since unsuspecting current employees would let them do so. She noted that the security issue was greater at nuclear facilities rather than at headquarters. Further, the Green Movement might target such outposts. Chitumbo said that the Agency keeps its plans confidential, such as when inspectors will visit sites or obtain design information. Member countries undertake background checks on the inspectors involved and may refuse a proposed visit.

Energy Infrastructure Assurance

Dr. Kannberg (PNNL) then discussed Energy Infrastructure Assurance, first in the context of industrial trends, information technology, and restructuring, and second, from the Federal perspective, including a DOE vulnerability assessment. Industries are becoming increasingly interconnected and standardized. Security is not maintained through obscurity; systems have become open, with no proprietary protocols and special requirements (and hence, they are cheaper). Access to information is rising, especially to market systems. For example, through accessibility to electrical-power markets, people can obtain maps of their infrastructure systems. Also, different industries share a common infrastructure, such as the reliance by gas- and electricity- companies on public switch networks. The "just in time' economy also entails mutual dependence, as is well illustrated by the enormous expansion of the Internet, wherein the United States, being the most aggressive in adopting it, has become the most vulnerable.

Attacks by hackers show increasing sophistication. Already, more than half of the networks of the 50 largest banks have been penetrated, while gas- and electric-companies report more than 100,000 scans per year, twelve of which are malicious, on average. The hackers' denial-of-service attacks against e-commerce sites have been very successful. In response, the caseload of the FBI rose dramatically from 200 to 800 in the last two years, so that their efforts now are limited by lack of sufficient agents. IT security is gaining attention from auditing-, insurance-, and underwriting-companies who will spend close to $1.6 trillion worldwide to deal with cyber attacks. Dr. Kannberg cited several recent attacks or thwarted ones by hackers and terrorists in countries including

Belgium, U.K., and Russia. He noted that in 75% these cases there was insider help, while vendors were involved in the remainder.

Restructuring industries in response to economic markets has degraded security. Downsizing made some companies more dependent upon outside contracts, while mergers may result in a pool of embittered employees. The law often demands open access to information. Hence, it is vital to keep staff well trained and updated both in the use of information technology and in security issues. He emphasized the importance of security for critical national infrastructures that, if destroyed, could compromise the defense and economy of the United States. In May 1998, a Presidential Directive decreed that government and industry should get together to ensure this security.
Kannberg described the Infrastructure Assurance Outreach Program (IAOP) wherein the DOE's expertise is called upon to enhance the security of utilities'energy systems. Task I of the IAOP, preplanning and pre-assessment, covers non-disclosure agreements and identification of critical assets. Task II, the assessment itself, includes determining threats, network architectures, penetrations, physical- and operational- security, and administrative policies and procedures. Finally, the IAOP considers the consequences of unlawful access to energy systems. Then, from a risk analysis of the probability of attacks, the consequences, and their costs, systems are ranked in importance.

The speaker set out the features of good vulnerability assessments, as adopted by the IAOP. They must be conducted under a "memo of understanding" with non-disclosure fully addressed. Information must be encrypted, and no one other than team members can see it (the DOE does not get a report). At the conclusion, all information is destroyed. The utility allocates resources for the assessment (time and people). . Presently, the Nuclear Regulatory Commission is considering a similar study for nuclear power plants. However, most are relatively secure as they have analog systems, but the Balance-of-Plant control processes, electrical grids, and support infrastructures may have digital ones than can be penetrated. Kannberg considered the many problems to be overcome. Among the needs is one for a framework for risk analysis, uniform definitions of sensitive information and of assets and their value. Policies are required for consistently securing computing- and communication- systems, with human behavior as the ultimate challenge. Configuration management, interconnectivity, and dependencies must be understood and updated, and the authorities and boundaries of systems defined by logical partitioning; for example, how far into the vendor's structure does the boundary lie. This feature is particularly important in multi-national corporations where access must be controlled and influences limited. Finally, vendors' security must be validated.

In response to questions, Kannberg stated that utilities do not use encryption, with one exception. Their concern is that its use may delay the system, or even deny access if operators have forgotten the password. Electrical industries often abandon full security measures to ensure that their systems are fully operable.

Vulnerability Assessments – Industry Best Practices

The final talk of the afternoon, Vulnerability Assessments – Industry Best Practices, was given by Mr. S. Talcott, Aquila Technologies. He pointed out that the interest in information security is directly proportional to the perception of risks, threats, and liabilities; with the growth of the Internet and the increase in the number of computers, from the original four machines to 200 million, it has become an important issue. There are five essential steps in a vulnerability assessment: (a) Understand the environment of potential threats; (b) identify assets and access to them; (c) assess vulnerabilities, and ensure that management will "buy-in" to any policies; (d) design a risk-based program for protection, and, (e) develop an incident-response plan. The assessment must be geared to the organization's prevailing culture. Thus, educational institutions do not favor much security because they are focussed upon ready access to information. Talcott gave some examples of attacks that had occurred, including those into the network of his company. Initially, Aquila did not have a lot of restrictions on their firewall, but after a hacker had successfully penetrated it, the wall was tightened and accesses were logged, both successful and unsuccessful. Pie-graphs can be constructed from this record that are often useful in persuading management to accept security plans.

Talcott specified the two main sources of risk: First, those associated with the vendor's software; and, second, risk from people such as administrators of the system, malicious authorized users, and users' errors. The latter would include the loss of laptop computers, and failure to log-out of the system properly (this could reflect a cultural stance). Inevitably, the activity of users must be monitored; for instance, for their own convenience, people may disable virus-control systems and this must be prevented.

Several points should be at the forefront when making a security assessment. Exhaustive checks of the system should be made, especially of old, vulnerable ones, and the number, type, and severity of security exposures reported. Talcott proposed allowing system administrators to determine its security status, but having external security auditors assess the effectiveness of these administrators. However, he suggested that because of the IAEA's legacy network and relative lack of security, such modern audits may not be entirely suitable. Assessments might include those made by people within an organization, and by outsiders.

The security policy must be carefully developed and maintained. It would encompass internal security, remote access to, and control over access to, the Internet, administration of network systems and gateways, and prevention of attacks by viruses. " Denial-of-service" attacks should be carefully documented. Plans should be established for backups, and recovery from disasters. Written practices should govern management of the database, passwords, and accounts, and also cover procedures when people leave the organization. Talcott emphasized the importance of physical security and the various tools needed: host scanners; firewalls; passwords; encryption and privacy. Regular updates of network scanners are essential because of the millions of lines of code, added to daily, that create new holes and vulnerabilities. He concluded by reiterating that the assessment must be thorough and repeatable, and built-up correctly so that it remains valid in future. He cautioned, however, that the task would greatly increase the burden on the information technology staff.

Thursday Morning, October 26.

Session 2: Planning & Implementing an Information Security Program, continued

*Designing a Risk-based Progra*m

Dr. D. Sackett, Lawrence Livermore National Laboratory (LLNL), gave the opening presentation, Designing a Risk-based Program. She identified several main points. Foremost was the need to justify the funds required to set up the program. Since there is no such thing as complete security, the measures adopted should not be excessive. Cyber attacks, she said, are very visible, especially those directed against large institutions, such as the LLNL. The vulnerability of the organization should be addressed, and how much security is enough. The value of the information assets should be determined, and balanced properly by estimating the frequency and type of attacks, and their impacts. Her accompanying graphs showed spending on security for institutes of education, health care, military, high technology, and finance; the latter expended up to $1,000,000 per year, and the technological organizations slightly less. Costs also increased with an increasing number of employees.

Sackett identified risk categories as the integrity of data, system's availability, and confidentiality of information against which he compared the categories of loss, competitive advantage, costs of restoration, damage to reputation, and legal liabilities. The value of an asset is defined in terms of the impact of its loss upon the organization. Assessments should include physical-security measures, and the policies and procedure, practices, and culture of the information technology sector. Most often, the former is lacking. In concert with other speakers, he stressed the importance of breaches of security by insiders. Thus, in a 1996 study by the Department of Defense, only 4% of intrusions were detected, and of these, 73% were not reported. However, a recent survey showed that awareness of these problems by respondents has increased to 70% compared with 47% in 1996. Accordingly, the number detected has risen.

The speaker next described how to quantify the type and frequency of attacks basing estimates on previous experience and on data from similar organizations, after adjusting for differences. The impacts of an attack may include the corruption, disclosure, and theft of information, the loss of business or a web site, and public embarrassment. He found that while about 74% of institutions questioned reported annual financial losses, only 42% could quantify them. A major loss is that of proprietary information, with financial fraud as a close second. Abuse of usage of the Internet by employees is rapidly rising. He considered the problems in establishing security measures, which is hampered by the lack of accepted norms so that expert advice often must be sought to categorize the sensitivity and value of information: often, it is better to group assets. Security measures can be expensive to maintain involving money and time, as well as the difficult task of changing the culture of an organization; he illustrated this cost-benefit analysis with a graph.

Sackett discussed the value of a tiered computer-security plan, such as exists at LLNL, Because the same security measures usually are not needed for all assets. Thus, a multilevel approach can maintain the flow of information while securing the most sensitive data (an isolated network within a locked room). But, for many organizations, not much security is needed: maintaining security patches on all systems can be expensive and, instead, it might suffice to use locked screens, scans for viruses, and firewalls. Similarly, a change in the system's configuration may be cheaper.

In the ensuing discussion, Ms. Seits suggested installing an air gap at the highly classified areas at the Agency so that less security would be needed on other machines. Dr. Chitumbo reminded people that the IAEA's sensitive material had to be blended with less sensitive data, and questioned how this could be done inexpensively; The Agency has only $200,000 annually to spend on security measures. Seits suggested making analyses, and then using data reduction on unclassified material and incorporating it into the classified data. Other members of the audience asked about costs, and the speaker returned to his first point – the importance of justifying everything to management, even though this may be difficult. An example is the "hidden" costs of the system administrators. He highlighted the importance of security to the IAEA otherwise data might be lost, and along with it, the reputation of, and trust in, the Agency. A good way for the Agency to start might be to test a particular sensitive part of their network and demonstrate any impact.

Requirements for Internet Security and Integrity

Mr. Perry, Computer Associates, elaborated on the security theme with the Requirements for Internet Security and Integrity. This company is the largest vendor of security systems in the world, and Perry offered advice from his wide experience. His first suggestion was to have a good backup system to recover data, since all systems will be attacked sooner or later. He stressed the importance of focusing upon solutions, including defense measures, measures controlling access, and also operational management; he pointed out that much can be gleaned from the commercial sector that has experienced many challenges and justified their remedies.

Defense measures must be geared against internal and external sources. The former is particularly important because employees are responsible for about ten percent of the breaches of privacy. He first discussed antiviral systems, the major consideration being how quickly signatures can be brought up to date. He attributed the long outage of e-mails in some companies after the recent onslaught of the "I love you" virus to their inability to update the signature files. He described firewalls, both the costly and hard-to-administer hardware ones, and the easier software versions. He advocated using both, with the former outside the system and the latter inside. Inside software firewalls should be compartmentalized by security level to avoid internal attacks. Intrusion-detection systems are invaluable for controlling access; some companies and schools employ URL blocking to prevent complete access to Internet sites. Another option might be to use ActiveX. Vendors may be helpful in finding the vulnerabilities of a system if an independent assessment is not made.

Under access control, he discussed the value to security of having virtual private networks internally and between two organizations via the Internet. This approach may prove cheaper, and can be set up with off-the-shelf components. Digital certificates with two-way authentication have the advantage that they allow only a specified receiver to open a message. Systems can be configured with access control at various levels, with automatic audit trails and logs, and alerts. Tools must be installed to consolidate audit logs, to periodically check systems that seem to have no vulnerabilities, and to check passwords. Centralized management must ensure that data in laptops, which often are lost, are backed-up, and that new software systems from vendors are in place and operable, and all patches are installed.

In the questions that followed, Perry told the audience that the same commercial products now are used by many countries, particularly after their recent relaxation of export laws (except by France). He also suggested several Internet sites as sources of information on attacks and resolving security problems.

Planning and Implementing an Incident Response Capability

Ms. S. Sparks (Lawrence Livermore National Laboratory) took up the security theme after the break with Planning and Implementing an Incident Response Capability. She began by describing the U.S. Department of Energy's Computer Incident Advisory Capability (CAC) that was established some ten years ago and is always available. For the first eight years, the budget was consistent, despite the increasing workload. Now, more monies have become available and a new phase of operation has started. In concert with previous speakers, she reiterated the reality of computer crime. In a survey sent to 4000 people, 521 of whom replied, 90% had experienced breaches of security, and 70% reported that these abuses were serious (theft of data, fraud, denial-of-service attacks). Also, 74% had financial losses, mostly because of the theft of proprietary information. She outlined the growth of the CAC system from 1997 when few DOE sites reported, to May this year when 50% were reporting. She recently noted a huge peak in problems with insiders, involving waste, fraud, and abuse.

Sparks turned to IAEA's problems with security of information and the role it plays in their success. What would be the impact of breaches? What are the most critical data? She stressed the importance of having a pro-active incident-response (IR) team to limit damage and the length of time that the system is unavailable, to determine the cause, and recommend deterrents. Having a rapid response time is a vital component, as is having knowledgeable people to decide what to do, such as whether to publicize incidents. She recommended the value of a site-security handbook, particularly for organizations with multiple sites. IR teams should distribute information to employees, work with other teams, and with law-enforcement officials; they should participate in investigating international incidents. To be pro-active, the IR team should arrange workshops and training, maintain the information servers, and act as a clearinghouse for information about security issues and new techniques and tools. They also should be closely involved with vendors and with any vulnerability assessments made. Members of the team should have strong technical skills, well-developed interpersonal skills, and integrity, maturity, discretion. In a series of comprehensive slides, Sparks listed the actions that should be taken, and the considerations given, before establishing the IR; these include formulating policies, procedures, and methods for handling incidents and fully characterizing them, taking into close account the organization's own operating structure. For example, customers should be kept within the loop and informed of incidents. Each incident should be examined in detail and documented including all actions taken by the IR team. Intrusion detection and patch installation should be practiced.

The challenges to setting up a secure information system may involve answering difficult questions, such as who is the "enemy", who can one trust, and who should be served. More pragmatic considerations are who will champion the need for a security system and promote its value, what its scope will be, and how existing resources can be leveraged and new ones obtained.

In concluding, Sparks described FIRST, the Forum of Incident Response and Security Teams, a voluntary world-wide cooperation among government and private organizations aimed at preventing security problems. Within Europe, certain countries have closely combined their efforts. She showed three overheads listing the guidelines, organizations, and their web sites, together a number of publications.

In opening the lengthy and vigorous discussion that followed, Ms. Suski said that the knowledge gained by the IAEA participants would help the Agency to set the level of security needed. They first would try to get the staff to accept the security concept, identify a champion, and then go to management, although this might take time. The audience confirmed the value of having someone to argue strongly in favor of security measures, particularly in view of the sensitivity of some of IAEA's data and hence, its cost.

Dr. Tolk (Sandia National Laboratory) reiterated the importance of being familiar with the normal behavior of people using the network so anomalies would be easily recognized, such as increased activity during the night. He had written a computer security desk-reference for Sandia Laboratory, and is in contact with a few knowledgeable staff who keep others informed of new developments. In this context, he mentioned the second attack by the so-called "love-bug" caused when a person moved e-mail to Juno after the first attack, thereby reintroducing the virus into the Laboratory's network.

Mr. McCusker identified the requirement for a strong security program when dealing with data from different countries, as the Agency does; it may be especially difficult to coordinate a multinational security program. Ms.Pepper (BNL) talked about the difference between accidental and malicious breaches from insiders, and which does the most damage. While the former may not be seen as a threat, it undoubtedly is vulnerability, and may be more damaging in the long run than the latter. She emphasized the value of combating accidents with training. Sparks cautioned about definitions and taking care not to describe an incident as an accident when it is a threat. Commercial companies do not discount misuse so easily, and persons who use outside e-mail servers and by-pass the firewall, as in the Juno incident, might face dismissal.

Dr. Chitumbo gave the IAEA's perspective on setting priorities for security within their limited budget. He believes that it will be costly to ensure the security of many of their old systems. Suski reminded the IAEA to look first at the threats, the environs, and the Agency's culture, and to work within those parameters to assess risks, and the costs of intrusions. Dr. Kannberg suggested thinking of the security problem in terms of insurance – risk-based loss and the degree of its probability. Premiums for insurance decline as people do more for themselves to lower risks. Risks also fall as people themselves accept some risks. Therefore, the IAEA might consider what risks are acceptable when looking at their budget. Security is of the utmost importance to the IAEA: a loss of credibility could be almost fatal for them. He mentioned that some insurance policies have been written against such loss of information, but, so far, no compensation has been paid because the insurance companies require audits, and may have written clauses and loopholes into contracts to avoid payment. Also, policies soon become dated as new methods of intrusion are devised. McCusker suggested that the Agency might take a global view of their security system, breaking it apart to focus of different geopolitical regions and installing several layers of security within a country.

Thursday Afternoon

Session 3: Technology Opportunities

Speakers from the U.S, National Laboratories and commercial vendors covered various important issues of information security and methods, products, and new technologies that can be used to address them. The IAEA found it useful to hear about products that cover the major security areas and others that deal with specialized areas.

Data Surety Issues in International Monitoring

The third session was opened with a presentation from Dr. K Tolk (Sandia National Laboratory) Data Surety Issues in International Monitoring. His talk centered on three issues: Authentication of sensor data; encryption of sensor data; and, classified information. Data from sensors is authenticated to ensure that it came from a specified source at the specified time and that it was not altered after collection. Authentication can be applied to information at its source, before transmission out of the sensor's tamper-indicating enclosure. Private key- (MAC) and public key- (digital signature) technologies can be used – the latter is the easier one. The system for authentication preferably should be placed close to the sensor itself. Further, data may be sent to an intermediate system for a second authentication, providing a high level of digital security. The host country is assumed to present a threat to authentication of data equivalent to that of a National Authority.

Encryption prevents sensitive information being seen by unauthorized people. The host country may require encryption to prevent its disclosure to third parties; the IAEA may want encryption so that the host cannot see that data. Tolk gave several examples of unclassified information that the host may consider sensitive, including the type and amount of material at the facility, the amount within a typical container, the location of material within a facility, and the domestic safeguards procedures. The IAEA may not want the host to be aware of the failure of sensors, or the thresholds and sensitivity of the surveillance equipment. They also may wish to prevent the host having details of the measured quantities of materials so that declarations could be altered and materials diverted. Hence, the network should be quite separate from the sensors, and the data encrypted. IAEA and the host country may share some classified information. This might include the amount and location of weapons-useable material at a facility, the amount and type of material in a specific container, the unique identifier of the seal on domestic tamper-indicating devices, and the type and location of domestic safeguards, such as cameras and the number of guards employed.

The essentials for security during the transmission and storage of data rely upon its encryption using Class 1 cryptography from the NSA before it is moved or stored on an open network (there are no longer U.S. export restrictions on Class I cryptography). Unencrypted classified information, and computers processing that information, must be kept in a vault, or a vault-type room. The vault should be equipped with steel doors, electronic digital locks, and sealed windows and ceilings. Further, to get a level of assurance on the authentication of data that does not come from an NT platform, the system must be able to analyze all lines of code and then seal the box.

The questions that followed centered on the value of new security locks, such as those that read the fingerprint of the person wanting access, or better still, those that scan the iris of the eye.

A Top Ten List for Intrusion – How to Plan, Procure, and Implement a Detection System.

Next, Ms. J. Wood (Dyncorp) discussed A Top Ten List for Intrusion – How to Plan, Procure, and Implement a Detection System. The first requirement, and the foundation of any security program, was to obtain the sanction of management. This involved having a plan to present to them specifying in detail the budget, scope, policies, and products needed to deal with the problem. A close second was to acknowledge that attacks could occur, even with security measures, so intrusion-detection systems and barriers on the network must be in place, remembering that inside threats may be more trouble than outside ones.

Then, she suggested developing rapport with vendors, and investing in training and technical support, asking for demonstrations of new technologies, and for automatic updates of the system. The best way is to start the detection-intrusion program is to keep it simple, monitoring initially with a default set policies, and then, with increasing familiarity, altering the program to meet particular specifications. Her fifth requirement was to have good situational awareness – realize that people are the weakest link, and educate them in maintaining the system's integrity and availability: Train people this way when they are first hired, and keep their commitment through briefings, broadcasts and posters.

There should be several layers of security, not just a firewall, with redundant equipment, and a detection system that will react to a challenge. An incident-response team should be created that will plan an alerting service, gauge the severity of attacks, and escalate the response, as needed. All procedures should be documented, including policies, auditing logs, and specifying the legal actions to be filed against intruders. A centralized monitoring process is preferable so that data from several sources can be normalized. Finally, a total security plan should be spelled out with people's roles and responsibilities, and separation of duties; it should incorporate the present configuration of the system for future comparisons.

Questions following the paper centered upon how much of the total budget should be spent upon security systems, especially for small organizations. Wood stated that this would depend upon the type of business, and the input from the staff. She named some helpful web sites.

Unauthorized Modem and FAX Misuse

Mr. G. White (SecureLogix) spoke next on Unauthorized Modem and FAX Misuse. He began by emphasizing the need to justify a security budget. A security system might be thought of an a necessary evil, so in planning it, thought should be given as to exactly how much to spend – as little as possible, and not too much. Often companies spend only three to six percent of their operating budget on information technology, out of which must come the funds for the security system, yet managers are reluctant to authorize funds because security is a non-tangible product. However, The system can save much money. He quoted examples from three corporations; in one, an inventory management system had helped double sales with no increase in personnel; in the second, the number of employees running a process had been drastically lowered; in the third, automation had reduced work time. Security might be looked upon as a Return on Investment (RIO) because its lack could result in real financial losses to a company. White listed several abuses and their costs from a 1999 Information Security survey. For 91 reporting companies, the average loss was $256,297. Similarly, the 2000 CSI/FBI Computer Crime and Security Survey showed an average loss of $972,857. Breaches of security and cases of unauthorized use are rising, with a concomitant monetary loss. Corporate officers can be held accountable for the failure to protect against loss, disclosure, and harassment. He mentioned the Health Insurance and Portability Act (HIPAA) that allows doctors to pull up a person's medical record; any transgressions of confidentiality may carry jail time and fines.

Facing a limited security budget, he considered next how the benefits could be maximized. He represented risk as being equal to the threat x vulnerability, divided by the countermeasures, and multiplied by value. Managers are not always convinced by calculations of risk, so that it is better to speak to them in terms of savings, and how security measures can enable business, calling this approach "how to close the big back door." He described, and showed slides of, several new technologies. Telephone bill reconciliation through an audit enabled Greyhound Buses to recover over one million dollars, illegally charged for 900 and 3rd party calls, and for services not requested. Toll fraud in the Unites States in 1999 accounted for losses of five billion dollars. He also suggested that forecasting and controlling the use for resources, such as fax lines, could generate savings. Overall, by having the institution to do something securely that it could not otherwise safely do, such as using on-line banking and brokers, savings would be made. Nevertheless, persuading managers of its value still could be an uphill battle.

Web Security – Scaling to the Global Enterprise; Cryptography and the Enterprise System

Web Security – Scaling to the Global Enterprise; Cryptography and the Enterprise System was the title of the next presentation by Mr. O. McCusker (Sonalyst).
His talk covered aspects of web architecture and Enterprise Architecture (EA), developing security models associated with web applications to identify risk, scaling such applications with global enterprises, and general security issues applied to EA. He discussed several security props: 1) Alice – that connects to a system and has Bob's

public key; 2) Bob – the entity of the host system with its private key; and 3) Eve – that has a lot of money and can crack 100 million keys/second. He began by describing how Web application boundaries have grown from single contained units to networks of varied systems tied together into single EAs. Security is the technology that protects the assets of information while allowing access to it, under the broad categories of authentication, authorization, privacy, non-repudiation, and integrity. Security and the EA are tightly coupled over all the developmental cycle, starting with the requirements for gathering information. The EA is best represented as a tier system of N layers, with the following basic ones: client tier; server tier; middleware tier; and, the data tier. Web-based architectures have grown over the past years to connect worldwide systems for sharing data. There may be geopolitical regions (GPRs) representing areas within which cryptographic constraints are shared (such as laws, standards, and rules). Security for these global systems is modeled by having security cells (functional units), or systems and subsystems within the GPR, each with its own Level of Penetration (LOP). All are given a security profile that describes how they can be both compromised and monitored. McCusker showed slides illustrating this; first, there was a table listing security measures from the time the cell is accessed to an entity leaving the cell, and then a diagram of an entire system with its LOPs. He suggested repackaging messages at GPR boundaries, establishing security audits between GRPs, monitoring the use of log files within the firewalls of cells, and having the ability to trace information to its source. Cryptographic algorithms (i.e., ciphers) are used to encrypt and decrypt messages between parties. Previously, restricted ciphers were used, but modern cryptographic systems are key-based. Symmetric keys use the same key to encrypt and decrypt. A combination of a public key may be used for encryption together with a private key for decryption. The “key” is the only number that will decrypt the data. Its length is important: symmetric keys are usually 56 to 128 bits, and public keys are 384 to 2304 bits. There are security issues involved in managing keys that concern their creation, distribution, and destruction, and their expiration and verification.

McCusker next touched upon the controls on the export of cryptography which were recently relaxed in several countries, including the United States; however, France has its own laws applicable to GRPs which differ from those of other countries. In conclusion, he stated that security starts with an analysis of requirements, moves on to developing a model of the global enterprise, and then gaining an understanding of where and how security should be applied within the global enterprise to reach the desired level of security. In doing this, the architects of the system must determine the geo-political constraints upon it.

Sandia’s Classified Network Integrity: StatepointPlus

After a short break,Mr. D. Patrick (Sandia National Laboratory) spoke on Sandia’s Classified Network Integrity: StatepointPlus. He began by describing the work of his group in designing classified- and unclassified- networks, and defense of security measures. The most important tasks are designing the security plan and system, evolving a test plan, and then testing the security measures to ensure that they are satisfactory. These actions increase customers’ confidence and the organization’s credibility. Sandia

Laboratory had adopted this approach for many years, and has a mandatory configuration document (CRUD) for all systems on their network. Thus, the group can be pro-active, and the system audited properly. Initially, their response to hackers was a reactive one and they found that even when all systems were in place and all users trained, still they overlooked loopholes. The group at Sandia was concerned about how to tell when the system was being attacked, and how to measure the attacks and their effects. Therefore, they met with representatives from Westinghouse who had a security tool, StatePointPlus, and reached a memorandum of agreement to convert it into a measuring tool.

StatePointPlus runs on NT-Unix and Lenox version. It measures hardware and software configurations and has features that query changes. It incorporates a strategic console wherein the computer will measure its configuration against a template and identify all the changes that were made. The system promptly presents a comprehensive view of all computers, or any within a selected set, classifying the depth of any changes. Thus, any problems are highlighted on-line, and their source can be separated. StatePointPlus diagnoses integrity at the product level, unlike other tools that monitor at the directory level.

Patrick suggested several ways in which the IAEA might benefit from adopting StatePointPlus. Thus, currently the Agency pulls out data from computers, stores it, and then looks through this archived material for trends within its system's architecture. StatePointPlus can rollout hundreds of nodes very rapidly without users noticing, even from isolated computers. It can complete audits, track logs, condense the data and analyze it. Its monitoring functions can be customized, and its rollout capacity automated, giving unprecedented control and efficient management of a diverse system. If the Agency formulated a security plan, and incorporated StatePointPlus, it would have a very solid system.

Securing Web-based Applications via Oblix Net Point

Mr. S. Talcott (Aquila Technologies) gave his second talk at this International Workshop entitled Securing Web-based Applications via Oblix Net Point. Aquila established a partnership with Oblix to produce this application of Net Point because of their problems with insuring security. They are satisfied with Net Point and believe that it might be of interest to the Agency. Net Point offers the first unified solution for managing user- and policy- security. It has rich and comprehensive features for managing both intra- and extra-net applications, and can create centralized security policies, while delegating their administration. Net Point includes several methods of authentication (one or more can be selected and assigned different strengths), and business-level and security-level auditing. The user interface has many intuitive features, and the system can be personalized to deliver personalized experience to users via a portal. There is a single sign-on for access across many web applications. No passwords are required for individual web servers. Resource domains are based on URLs.

Aquila Technologies found that the system is highly reliable, incorporating many redundant servers and directions. It scales easily to large and small networks. Using encrypted cookies ensures security. The centralized administration allows the sharing of secrets. They particularly favored its user self-registration, which allows services to be customized, and also, its delegated identity administration.

Using ISO15408 as the Basis for Security Assessments

The following speaker, Ms. L.Ambuel (Decisive Analytics) explained the advantages of Using ISO15408 as the Basis for Security Assessments. ISO15408 is the Common Criteria for Information Technology Security Evaluation (CC), an 800-page, three-part catalogue of criteria and a set of tools for constructing requirements. It uses internationally agreed-upon specifications language for functionality and assurance measures, and is endorsed by a Recognition Arrangement among thirteen nations, based of the results of assessments. CC started as a replacement for the Department of Defense's so-called Orange Book, and was written over seven years, the various drafts being merged in 1999. Canada, France, Germany, The Netherlands, U.K., the United States, and Australia sponsor it. Another six nations have signed on as "consumers", i.e., they use the information but do not generate evaluations. Russia and Poland are replacing their national criteria with CC, and it is being translated for the Czech republic and Korea who are considering its use. Japan, Israel, and Sweden also are interested.

The CC is invaluable because it contains guidelines for evaluating information technology (IT) security, using a standard language for communication among consumers, developers, and assessors. It offers a means for accepting the results of security assessments from different countries so that users can understand what has been done, and if it is applicable to their situation (so avoiding duplication of work). Among its tools there are guidelines for developing and procuring products with IT security features, and for evaluating them. In other words, it provides a sound framework for defining the security environment, and the objectives of a chosen security stance, the Protection Profile. Then, it shows users how to refine those objectives into requirements, and finally to assess any security product against a defined set of criteria, the Security Target.

Ambuel pointed out that using CC would help to build confidence in the security of any operation. By understanding the problems facing an organization, choosing the appropriate solutions and vendors, and deciding how much confidence is required in particular security features, then CC can offer simple means to assess, establish, and maintain a secure system. Several nations are making security assessments that might be useful in aiding the IAEA in defining their security problems.

Unauthorized Modem and Fax Misuse

Mr. G. White, SecureLogix Corporation, turned next to troubles with Unauthorized Modem and Fax Misuse. To date, security has primarily been focused upon the TCP/IP network. White proposed that the weak link is the phone network, and all efforts to secure systems will be of no avail unless the telephone lines are secure. In contrast to the TCP/IP network with its one high-speed pipe and thousands of connections, the telephone system has very many slow-speed lines. He was particularly concerned about the potential threats when staff, working from their modems at home, dial in to the organization via the public telephone lines. Hackers can break in through these lines, so negating any security systems installed to protect the computer network.

White offered several solutions. Institutes may establish a policy forbidding such modem connections, though often 2 to 4% of employees use them, and sometimes as many as 9%. Scanning could be an answer, but the window of visibility will show only those modems in use. Employees may transmit material during the day and disconnect the modem at night, and there may be problems in designating a person to deal promptly with the reports from the scans.

Resolution may be to install a telecom firewall on the public telephone network and restrict access based upon parameters such as area codes, specific numbers, and type of call. The scalability of the firewall is important. The system will log incoming- and outgoing-traffic, generate audits, and block access. Although this firewall seemed to offer a solution to closing this security "back door", managers were not eager to purchase it. However, they were persuaded on the basis of the monetary savings that could be realized. Thus, the logs can be consolidated, so enabling a company to see who is using phones and faxes after work hours. Reconciliation of telephone bills with these records also will reveal illegal usage.

Securing Web Applications via PKI

The next contribution, Securing Web Applications via PKI was given by Mr. J. Rome (Oak Ridge National Laboratory). His work upon Public Key Infrastructure (PKI) began from a remote scientific collaboration on materials mischaracterization and involved five sites and many electron microscopes. The advantages of this collaboration were the savings in travel time and expenses, and the convenience of not wasting time if a microscope broke down. Indeed, with appropriate software programs, microscopes in the laboratory can be controlled and run from home.

There were several challenges in establishing this remote collaboration. (1) It is hard to establish scientific trust over distances; (2) the network must support all remote environments and platforms; (3) the information must penetrate firewalls; (4) the networking must be fast and have a low-latency; and, (5) the network must be secure. Nevertheless, PKI is good for such small teams and can be supported by modem browsers and web servers, and by features such authentication. Rome found problems in using Certificate Authorities (CAs) for browsers, primarily centering on whether to put more trust in the standard CAs that can be applied for, or the CAs already in the browser. He mentioned that it was difficult to select a certificate in Internet Explorer, but Netscape allows users to give the certificate a name.

Rome mentioned that he was not satisfied with the Internet Explorer (IE) which the Internet Information Server (IIS) uses for security, since both browser and server were intertwined. He suggested leaving on ActiveX so that IE could download patches for the server and operating system. He believes that the best approach is to issue one's own certificates with a single sign-on, and base them on authentication, role-based access, and audits. He also mentioned that good tools for PKI have become available, seventeen years after its invention. Servlets allow all codes and resources to be placed on the server. The servlet's engine intercepts every request, and can encrypt messages.

He discussed, and showed slides of, the Oak Ridge National Laboratory's E-lab Notebook. IT is written in Practical Extraction and Reporting Language (PERL) and used at hundreds of sites. It conforms to Microsoft Management Control (MMC) requirements, to which the user adds encryption, access by certificates, and remote control of the notebook. The pages are dynamic - Rome has the ability to restrict access from particular people and countries. Importantly, for his research, the notebook can acquire experimental images.

*Commercial Example of Continuous Risk Reductio*n

Mr. Potter (ICSA.net) continued the presentations with an overview of Commercial Example of Continuous Risk Reduction. Some ten years ago, the National Computer Security Association (NCSA) evolved into the International Computer Security Association (ICAS). The ICAS is a private, for-profit, company and is not part of any governmental organization. The company is active in three main areas: (1) As a media group, publishing a free information-security magazine; (2) as a consulting service, advising people on security; and, (3) as a laboratory, researching products. ICAS sets up consortiums, establishing them when there is a critical mass of a certain product, such as systems for cryptography, intrusion detection, and ISP security. The consortiums have a life cycle, beginning by surveying the equipment, and buyer's guides, testing the products, and finally certifying them. Vendors fund the consortiums. ICAS does not rank the various products, but their certificates show publicly the features upon which the product was certified. (They do not touch the beta-level code in patches; however, the patches must be available to the public).

Potter listed some of their achievements. They founded consortiums for assessing anti-virus systems in 1991 and began testing them in 1993. So far, they have examined 100 products; failures are published (28%) as well as those that pass their scrutiny. There is a graded rating system from 1 to3. Successful systems must be able to detect 90% of known viruses, including 100% of those on the so-called wild list and the ICSA's list of Common Infectors, and 90% from the "zoo" of viruses. Five years ago they began to study the security of firewalls, which resulted in an 86% failure rate by their criteria. They have begun to re-certify them, including enterprise firewall certification, always on the public network so that they can learn of any new problems that arise.

The speaker then gave a brief overview of their work on Internet Protocol Security (IPSec) that arose when motor-manufacturing companies wanted to move from leased lines to the Internet, but wanted security. They certify the products, which must be interoperable (tested against a reference set) and have good cryptographic features. Twenty-six have been certified from among 40 participating. The data have been published. In this area, as in other certifications, the criteria are evolving and becoming more stringent, thereby pushing industry to better its products. Finally, Potter described ICAS's developing program to certify cryptographic products. So far, they can detect poor implementations, but cannot give assurances that the product is satisfactory. The company plans to test other technologies, including PC firewalls, and PKIs.

Friday Morning, October 27.

Session 4. Closing Plenary and Round Table Discussion

Securing the Infocosm

B. Malik, Gartner Group, opened the session with Securing the Infocosm a talk that proffered a model for information security, suggesting the steps that are required to put in place an effective security program. He first discussed the extent of risk, illustrating it with a graph showing the projected reduction from 1999 to 2004. The goal of a security team is not to make risk minimal but to properly ensure risk is at a level that an organization wants. He pointed out that good technology is never a substitute for good management, though the reverse may hold. He discussed the enormous changes in business that have occurred since 1994, when one could not even send e-mail, to the situation today when companies are being restructured to take advantage of information technology, either Internet-enabled or Internet-centric. He contrasted the advantages of changing an infrastructure, or starting afresh, preferring the latter option. With a new start, security must be changed. Security is a function of the design of the system, and must be built-in from the beginning. The Y2K problem gave a breathing space to look at security systems available, and there is a comprehensive list.

He turned to threats. Only two threats from over 500 that had a financial outcome did not involve insiders. Further, he quoted examples showing that uncovering threats may not only require technical skills but a sound knowledge of business practices and cultures. His slide of information-security problems linking the supplier and the customer revealed a loss of information or issues of privacy, all the way through, from the design stages to shipping the product. In the present era of monitoring mainframes, a “due care” security exposure has been adopted; however, security is failing as people move from PCs to Java that is unsecured.

Malik stressed the importance of the “Art of the Long View” propounded in Peter Schwartz’s book. Security teams should try to think about, and group, everything that could impact future plans, from allowing full access to restricting it. He illustrated this in eight slides projecting the needed changes, from now to the year 2004, for firewalls, intrusion detection, malicious-code detection, vulnerability assessments, and so forth. He next posed some critical security questions about outsourcing, and contracts, cautioning that if outsiders establish the security system, then all the contracts should be examined in detail as vendors may phrase them to limit legal liability. He touched upon the lack of security in present-day cellular phones: their security score now is only 0.063 but is expected to climb to 0.5 by the year 2004.

Malik’s solution to security problems was a six-step security hierarchy: At its basis is Information Security Policy and Standards that should be simple and short, reflecting the organization’s culture and ethics. The second step is setting up administratively the information-security architecture and processes; this will encompass access control, authorizations, encryption, and their strengths that will depend upon the amount of risk that the company can shoulder. Awareness and training are step three, and must be thorough. Step four involves selecting the technology that fits the architecture, followed by its auditing, monitoring, and testing. The final step, validation is an on-going process employed whenever there is any change in the systems from people to functions – then, the process starts again from step 1. He finished by going over issues of outsourcing, market relationships, and the costs of the security system.

Malik invited questions on issues raised in his presentation. Suski asked for his view on how to get the IAEA's senior managers and staff to support such security measures. She pointed out again that the Agency could lose not only monies but also its reputation if compromised. With their limited resources, how might they set priorities? Malik's advice was to find a senior individual who would support them and with that person discuss 50 to 50 scenarios from which needs could be identified and grouped. Farnitano highlighted the value of giving the IAEA a roadmap with specific milestones, rather than disjointed information. Seits said that the IAEA had secured confidential material on the mainframe, but the problem remained of securing highly sensitive information. She proposed access control and encryption, but the Agency's management was not certain that this was adequate. Malik again stressed the dependence of security upon the managers' day-to-day decisions and upon the organization's culture, rather than upon technology per se.

In moving from sensitive information from paper-based security to electronic security, as the Agency is doing, Malik suggested that the measures used for the former could be modified for the latter. New staff should sign an agreement of privacy that was reviewed annually, to ensure its legality. Training courses should inform staff about security. He advocated preparations for a breach of security, especially as the worse risks are unidentified ones. The essence of the policies could be written on 3 x 5 inch cards, or as a participant aptly put it, formulated as "…series of newspaper headlines of possible scenarios of doom."

Round Table Discussion

After a short break, Mr. Malik led off the roundtable discussion on the architecture of security systems. He stated that the costs of a fully secured system are prohibitive, and so an acceptable default level must be chosen. Therefore, it may be useful to designate a security architect who would describe all aspects of the security environment, including who participates, and what has happened. This person would closely consider the trade-off between accountability, reliability, and ease of audit on the one hand, against reduced performance, reduced flexibility, and reduced ease of use on the other. Malik's suggested initial step would be to write a policy and show managers how this can keep data confidential, and yet be audited. The control architecture in that policy would describe the technology in neutral terms while the security implementation guidelines would describe the application of controls to each specific platform. (Control architecture is not needed if all computers are alike, nor if they are different but unconnected; it is only needed when different ones are wired together because then there are gaps at the interfaces). Controls are exercised by roles and responsibilities, as well as by functions and departments. Control processes for acquiring new technology should meet the checklist. Also, there should be provisions about what to do if a different type of computer is added.

Malik moved on to discuss technology-enforced implementation guidelines with their baseline controls for authentication, authorization, tracking, detecting, recovery, administration and assurance, and physical security backup. He showed diagrams of baseline control matrices (from some insurance companies); for example, companies may require that each person have a unique I.D, and may check automatically every five minutes to see that there have been no changes. He mentioned the importance of a "match to the market", i.e., looking at the security controls of the vendors, as well as their ability to manage the system. He believes that business groups may contract out for their security architecture to a web host company. Along with this, he expects costs to rise from about 2% to about 15%, as networks become more complex. The value of security architecture to businesses is in demonstrating that data are secure. This business process has matured from having nobody on staff to respond to a virus, to having a rudimentary response team, to documenting procedure and policies, to experiencing the first major problem, and finally, to having full feedback and a thorough knowledge of the network's defects.

Malik answered questions about the risk of outsourcing; he suggested that if two products are available, one perfect but which cannot be audited, and the other flawed but able to be audited, then a buyer should take the latter and modify it; audibility is the key to establishing trust. In considering the security policy proposed to the IAEA by Ms. Seits, he suggested developing an incident-response protocol, and consolidating the help-desk with one telephone number (a problem is "owned" by the person who first responds to the caller). Meaningful reports should be generated describing what the network contains and what it needs. According to Dr. Chitumbo the proposed policy from the Safeguards Department would cover the entire Agency because it is the most stringent one. The audience discussed whether the security system could be established in-house rather than hiring a company to do it. Malik thought that in-house implementation was feasible provided that not too many people are involved because it is a very rigorous undertaking. A small group (a best-practices group) could best define acceptable risk and brainstorm possible scenarios.

. Chitumbo, IAEA, drew the meeting to a close. He said that the staff did not come to the meeting seeking answers and solutions, since participants were not fully cognizant with the Agency's computer environment. Rather, they wanted to talk to experts to help them understand the Agency's problems, many of which are the same of those in other organizations. He and his colleagues had learnt a lot and were happy to learn that they already were aware of many of the problems discussed. Now, they were wrestling with how to implement the measure and build up confidence between the Agency and the member countries. The Agency recognized that they must demonstrate that the IAEA's processes can be audited; accountability is particularly vital for the Safeguards Division. Any breaches found will be closed. Also, the system must be transparent and clear so that they will know where any leaks come from. The Director will be accountable.

Chitumbo then spoke about the IAEA's view on outsourcing, and for which parts of the system it could be use. Member states might be upset because they want central control. The Agency, therefore, must set out s strong case for any such measures to keep members' trust and satisfaction.

Chitumbo stated that he was comfortable that he now saw a light at the end of the tunnel. He wished that representatives from the member states could have been present at the meeting so that they too could have gained this understanding. He also would have liked the Director of Operations to be present. Previously, there was no focus on security, nor a security budget: Ms. Seits had highlighted it for the Agency only within the last two years. He hoped that there would be more such meetings to which he could bring other people from the Operations Division.

On behalf of the IAEA, Dr. Chitumbo expressed his gratitude to the organizers. They, in turn, thanked the participants and those who had given talks. Mr. Farnitano stated that the SSTS was keen to help and receptive to budgetary requests and also to queries about what could be accomplished on an extra-budgetary basis.