

# CONFERENCE REPORT

## National Computer Security Conference (NCSC)

Baltimore Convention Center, Maryland  
October 11-14, 1994.

**Dipankar Dasgupta, Ph.D**

Dept. of Computer Science

University of New Mexico

Albuquerque, NM 87131

dasgupta@cs.unm.edu

NCSC-94 was the 17th National Conference on Computer Security, which provided an update of research and development on various security technologies for the protection of rapidly evolving information infrastructures. The conference was organized by the National Security Agency/National Computer Security Center (NSA/NCSC) and the National Institute of Standards and Technology/Computer Systems Laboratory (NIST/CSL). It was for four days and the talks were presented in parallel sessions. The technical program was divided into tracks that addressed traditional information security concerns as well as security issues associated with the rapidly emerging information infrastructure. The track headings were *Research & Development, Architecture & Standards, Applications & Integration, and Tutorials & Presentations*. These tracks were designed to serve a wide range of interests from highly technical R&D projects to user-oriented management and administration topics. The opening and closing plenary sessions highlighted various dimensions of security challenges. There were ten high quality tutorials organized by expert tutors. The tutorial program offered experienced reports from companies and government agencies regarding up-to-date information on existing security measures, and how to bring new technology to practice. There were also 30 panel sessions which discussed different issues on emerging security technologies and practices.

After the opening plenary session on October 11th, I attended the "Intrusion Detection" session. The first speaker in this session was N. Puketza (UC, Davis), who talked on testing Intrusion Detection Systems (IDS). The author addressed the need for developing sound methodologies and tools for testing IDSs. He mentioned a software platform (using Unix expert and Tcl packages) for simulating various intrusion scenarios (like password-cracking, door knob rattling, network-hopping, etc.) to test the detection ability of different IDSs. Their IDS testing methodology included three phases: basic functional testing, variance testing, and stress testing. In the basic functional testing phase, each attack was simulated one at a time and the attacks were in their most straightforward form. The purpose of this phase was to check if the IDS, in ideal conditions, could detect each attack. During the variance testing phase, each attack was simulated several times, and each time some aspect of the attack was changed.

This determined any variation of an attack that the IDS could not detect, even though it could detect the most straightforward form of the attack. The stress testing phase examined IDSs response to the same attack under extreme conditions, to test its ability in a high level of system activity. Also by simulating several attacks at once, they examined whether the IDS could still be capable of detecting all of them. Their further goal is to create a benchmark suite to measure several aspects of IDSs. Particularly, the benchmark suite will monitor an IDS while it is running, and measure aspects of the IDS's performance such as the fraction of known intrusions it can identify, the false alarm rate, and the host system resource (memory, CPU load, I/O) consumption, etc. The information provided by the benchmark suite will help an organization to select an IDS that is suitable for their computer system.

The second speaker was S. Kumar (Purdue Uni), their paper on 'Pattern Matching model for misuse intrusion detection' received the outstanding student paper award. He described a pattern matching approach based on Colored Petri Nets for detection of system attacks. In this approach, knowledge about attacks was represented by specialized graphs. These graphs were an adaptation of Colored Petri Nets with guards representing signature context and vertices representing system states. He referred to each signature represented as an instantiation of a Colored Petri Automaton (CPA). The notion of one or more start states and a unique final state defined the set of strings matched by the CPA. According to him, matching begins with one token in each initial state and the pattern is considered to be matched for each token that reaches the final state. The model also supports specifying partial orders and subsumes matching of action sequences and regular expressions. This approach allows the user to design a generic misuse detector, and can be viewed as consisting of three basic abstraction layers: *The Information Layer* - This encapsulates the audit trail and provides a low-level data interface to the monitored computer system. *The Signature Layer* - This provides for a system-independent internal representation of signatures and a system-independent virtual machine to represent the signature context. *The matching Engine* - This encapsulates the method used to match the patterns. It makes the system independent of any particular choice of matching algorithms. It also allows simple substitution of newer or more powerful mechanisms as they become available. The model is generic and applicable to any well-defined format of input events such as audit trail records, network packets, or other abstractions. The paper experimented with UNIX audit trails examples as input to illustrate the usefulness and applicability of this approach in misuse detection.

The last talk of the session was by J. Frank (UC Davis), who received one of the best paper awards of the conference. His talk was on "Artificial Intelligence and Intrusion Detection: Current and Future Directions" which highlighted the use of AI methods in Intrusion Detection (ID). He provided a brief survey on AI-based Intrusion Detection systems and presented an illustration by using a feature selection technique to improve the classification of network connections. The improvement was achieved by minimizing the classification error rate and by reducing the number of features for connections classification. Specifically, he used the feature selection technique to reduce the amount of information required to make good predictions, and to improve the error rate of classifiers. This was accomplished by searching subsets of features, or information sources, and testing the ability of those features to classify the training instances. He showed that the feature selection method could improve the classification by

searching for the subset of features that best classify the training data. In his tests, features were derived from information sources used to detect intrusions, and training instances were derived from detected intrusion attempts as well as from normal behavior. He argued with some example applications that the method can be used to find features most indicative of misuse, or can be used to distinguish between types of misuse. In his paper, two types of experiments were performed: one selecting features which distinguished one type of connection from all others, and the other which classified all connection types. These experiments used seven features about each network connection (data collected using NSM, network Security Monitor). He analyzed three search algorithms (Backward sequential search, Beam search and Random Generation Plus Sequential Selection) for determining the best subset of features to classify connections and used decision trees to evaluate each set of features. But the search algorithms needed polynomial time and would be computationally expensive to handle large feature sets.

In the afternoon of Tuesday, I attended a panel-session on “Fuzzy Security: Formalizing Security as Risk Management”. There were three panelists who discussed different strategies for building flexibility into the formal aspects of computer security to produce more functional trusted systems. Panel’s view was that the acceptable security is basically concerned with risk management, though formal models in computer security ignore risk management and its fuzzy and subjective assessments. According to them, with current methods there is no way to measure the risk on leakage of secrets, while allowing particular information flows from the system. Panelists illustrated the motivation for using fuzzy logic and its implication to handle many possible degrees of security. It is possible to develop formal models for computer security in a fuzzy environment and to use fuzzy logic to establish provable security. Further combining ‘Fuzzy’ and ‘Crisp’ tools may lead to cleaner understanding of security ideals and security reality. They argued that fuzzy mathematics makes it possible to use verbal models for humanistic reasoning the way that mathematical models are used in physics. They also mentioned how fuzzy logic can be used to model fundamental computer security concepts, especially “real” world policies and policy interactions. This discussion include fuzzy generalization and issues involved multiple policies and resolving conflict among multiple policies.

On Wednesday morning, I attended a tutorial on “Trusted Networks” presented by R. K. Bauer (Arca Systems, Inc.). The tutorial focused on security issues in a network environment and highlighted network risk and trusted network criteria. The topics included in this tutorial were network security concerns and services, interpretation of trusted networks, trusted network components, evaluation classes, system composition and interconnection, and cascading.

At the afternoon session on *Management and Administration*, there were three paper presentations in the first half under session heading “Detecting and Detering Computer Crime” and a panel discussion on “Computer Crime on the Internet” in the second half of the session. The first speaker of the session was T. Phillips (Booz Allen & Hamilton Inc). His paper “The Electronic Intrusion Threats to National Security & Emergency Preparedness Telecommunications: An Awareness Document” addressed an assessment of the threat posed by individuals or groups (electronic intruders) who gain unauthorized access to elements of the nation’s public telecommunications infrastructure. He referred to reports which showed that the intruders could access key network elements, create denial-of-service problems, monitor communications, search data

bases, and modify and delete data base information. Though obtaining accurate information concerning the frequency of attacks on particular network elements is virtually impossible due, in part, to the vast majority of attacks not being reported, it is apparent that the number of electronic intruders is continually growing. Electronic intruders are developing advanced software techniques and making sophisticated programmed attacks motivated by financial gain from industrial espionage, foreign organizations, etc.

The second talk was by N. Kelem (Trusted Information Systems) on "Using Application Profiles to Detect Computer Misuse". Her talk focused on characterizing the behavior of application programs (rather than user behavior) by monitoring resource usage statistics captured in an audit log. In their experiments, audit records representing 'masquerades' were compared with application profiles to find whether the masquerades could be detected via examination of the resource usage statistics associated with application programs. She reported mixed results of their analysis - the analysis were more useful with individual application profiles than with group profiles or overall system profiles. She suggested that monitoring system usages to detect misuse remains a research topics.

The next speaker was S. Sherizen (Data Security Systems, Inc.). His paper on "Can Computer Crime be Deterred?" (received one of the best paper awards) was based on the promise that deterrence should be considered as a central concern in addition to the existing technical and managerial approaches to computer crime prevention. He emphasized that there is a need for personnel security officials to determine how best to change the existing perceptions of employees and outsiders regarding the risks of getting caught in computer crime activities as well as the perceived payoffs from such activities. He reviewed various concepts of making deterrence a computer crime prevention option, which include legislative changes, law enforcement changes, and organizational changes. He agreed that it will be difficult to be made deterrence effective with computer crimes, but it is important that the information security community, working with legislators and prosecutors, determine effective deterrent measures that can protect information. For deterring computer crime, he mentioned the need for improved detection techniques - investigation effectiveness - speedy and appropriate punishments - international cooperation.

The afternoon panel-session which I attended, *Computer Crime on the Internet*, addressed different computer crime issues related to internet connections from many angles to provide a practical standpoint in terms of risks. A federal computer systems manager (M. Pollitt) discussed specific computer security problems his agency experienced after permitting internet connections. He pointed out different roles and responsibilities of the victim organization, the investigator and the need for essential elements of an investigation to prevent Internet related crimes. A representative from the Computer Emergency Response Team (CERT) mentioned their role and initiatives in dealing with Internet crime.

On Thursday (October 13th), I attended the 14th **Intrusion-Detection Workshop** held in conjunction with the NCSC conference. The workshop was organized by Debra Anderson of *SRI International* and was attended by more than forty participants. There were eight short presentations and discussion sessions during the day. D. Anderson, in her opening talk, highlighted the progress of ongoing intrusion detection projects; particularly, she gave an update on

NIDES (Next Generation Intrusion Detection Expert System) software and mentioned about the NIDES training course to be offered by SRI International in November, 1994. C. Crowl (DISA-CISS) spoke on *Audit/Monitoring and Data Reduction System Specification* - its goal and functions. He stressed issues in auditing and different techniques for filtering information in audit data. J. Lister (Wollongong Uni) proposed a different approach on *Policy Formalization and Enforcement Tools*. He pointed out the needs for enforcing organization's policies and tools to assist in automating process of installing/managing security mechanisms for resources/services of system. M. Gross (NSA) told their experiences with the use of a intrusion detection system, NIDES. Currently they are using NIDES to flag any intrusive behavior in order to inform the system administrator for further analysis.

In the afternoon, S. Smaha's (Haystack Lab) talk on *Using Non-audit Data for Misuse Detection* addressed different features of an UNIX security software, **Stalker**. According to him, Stalker can automatically detect misuses and provides system accountability for security-conscious system managers, EDP auditors, and computer security professionals. D. Keirse (Hughes Research Lab) talked about his idea of using *Agent-based Intrusion Detection* in a distributed computing environment. In his system, agents in different machines are supposed to communicate with each other and monitor traffic looking for any possible intrusion. T. Lunt (SRI) emphasized aims and objectives of Intrusion Detection Systems. In her view, an ideal IDS should able to: detect a wide variety of intrusion types; easily extendable to detect new types; be highly reliable; run in real time; and operate in a network environment etc. Also the system should be scalable to support very large, heterogeneous networks.

The remaining talks of the workshop were by G. Gupta (James Cook Uni) on *Profiling Unix Users* and F. Lassmann (Tech. Uni. Munich) on *An Integration Concept for Audit Mechanisms in a Distributed System* (uses MIP to control audit trail). G. Gupta reported very interesting results on behavior of UNIX users' in using commands, his study was based on university students. His report showed that only a small percentage of students use more than 20 commands in their practice. He and his colleague also shown results on key strokes and mouse movements of users.

In the morning of Friday, I attended a panel-session which highlighted *new security paradigms '94 workshop*. This session was devoted to exploring new ways of viewing and thinking about computer security. The panel discussed issues ranging from multipolicy models: to use of object-oriented methods; to revision of traditional modes of designing and evaluating trusted systems. Talks I attended in this session included: Essin and Lincoln's paper on "Healthcare Information Architecture: Elements of a New Paradigm", which presented an architecture for multipurpose medical databases which could preserve atomicity, authenticity, and persistence of data related to healthcare. The talk by J. Dobson (Newcastle Uni) on "Communication, Information Security and Value" argued for a theory of information and associated security perspective which should be value and relevance-based. In his view, information security can be seen to be a value-adding or value-protecting process in the context of the objectives of the organization using the information. The talk on *Fuzzy Patterns in Data* by T. Y. Lin (SanJose State Uni) illustrated the use of fuzzy systems theory for auditing. He examined the repeatable patterns in audit data for formalizing signatures of user behavior.

The closing plenary was on "Security, Privacy, and Protection Issues in Emerging Information

Infrastructures” addressed a number of security issues for the present and for the future. They focused on the need for new technologies, since the existing tools are not adequate to protect changing infrastructures. Also they emphasized security awareness and global cooperation for Internet security.

There were exhibitions and demonstrations on computer security products in the conference premise. Other special sessions were also organized by many companies and agencies, including Trusted System Interoperability Group, Air Force, Defense Information Systems Agency, European Community, which I could not attend. Most of papers presented at different sessions (which I attended) covered different areas of computer and network security issues. However, this report reflects my personal and limited view of such a big conference with many parallel activities. I talked to many people during the conference on different topics and my feeling was that the information security issues will be one of the major area of research in coming years. On the whole, NCSC-94 was well organized conference. I would like to express my gratitude to Prof. Stephanie Forrest (my postdoc advisor) for funding to attend the conference.