18 WORKSHOP SUMMARY

Vijayalakshmi Atluri and David L. Spooner

The twelfth IFIP WG 11.3 Working Conference on Database Security was held at Porto Carras Complex, Chalkidiki, Greece, on July 15-17, 1998. Sushil Jajodia, the Program Chair, gave the opening remarks. The conference consisted of fourteen papers, two invited talks and a panel discussion.

The first session began with an invited talk "E-Commerce Security: No Silver Bullet," by Anup Ghosh, Reliable Software Technologies. Anup discussed several security issues in E-Commerce including security requirements in the E-Commerce environment, client and server vulnerabilities, security concerns of both merchants and consumers, various secure payment systems and protocols, and E-Commerce security today and tomorrow.

When Anup mentioned that most E-Commerce security protocols are based on encryption and are susceptible to a variety of common attacks, Sushil Jajodia questioned how realistic attacks such as man-in-the-middle are. Anup responded that the public might lose confidence if there is a single attack. When Anup mentioned that the system is only as secure as its weakest components, Sushil did not agree. Sushil suggested that there is a need for something like a reference monitor where one can have several untrusted components but the whole system can still be secure.

T.C. Ting questioned how secure is secure so that customers feel comfortable with electronic commerce just the same as customers trust a restaurant when giving a credit card. T.C. asked whether there is any notion of the degree of security that is acceptable to the public. Anup replied that there will be problems until businesses become aware of the problem and do something about it. Sushil commented that E-Commerce progress is slow because there is no customer confidence, and he suggested that there is a need for standards and

risk analysis of protocols. Anup replied that his company used risk analysis on its full system.

For Sushil's question on what certification of a software product means, Anup responded that a 3rd party certifier analyzes software for certain types of defects. T.C. asked about the technical basis for certifiers. Anup said that merchants have most of the risk and the most to lose. John Dobson commented that pipeline component testing will identify interesting research problems underneath.

For Thomas Keefe's questions on Trojan Horse detection and black box techniques, Anup responded that they look at the behavior of the product. For Sujeet Shenoi's question on how successful Trojan Horse detection is, Anup said that they have developed methodologies to detect Trojan Horses but they do not have any empirical results. For T.C.'s question of who are the potential customers, Anup replied that they are VISA and banks. For Sujeet's comment on the advertisement of secure E-Commerce servers by IBM, Anup commented that we trust them because they are from IBM.

During session 2, Anup continued his discussion and presented techniques to detect software vulnerabilities. For John's question on whether software flaws rather than configuration problems cause security violations, Anup responded that his company is now addressing configuration more from the software development point of view. Anup mentioned that current approaches first develop the software and then release patches to that software, which is not good. Sushil supported Anup by adding that this approach does not work because it may mean that the system has to be down for some time. This can be avoided by Anup's system since it analyzes software behavior and this enables software vendors to detect security flaws before they release the software. For T.C.'s question on what security value can be given to a system, Anup said that testing provides some level of confidence.

For John's question on whether there is any use of formal methods to decide if a flaw is a security flaw, Anup responded by saying that a flaw gives more privileges than it should. One does not need a well-defined security policy to observe this. There does not exist a formal method that is capable of doing this.

For Ehud Gudes' concern over the exponential number of states in a software system, Anup responded that they inject one fault at a time to identify the statement that causes a security violation. For Sushil's question on the size of code analyzed, Anup said that it is typically in the range of 10 - 20 thousand lines and it typically takes one person two weeks to develop a degree of confidence in the certification of a software component.

John questioned that since an analyst must write assertions about a security policy, how does the analyst know that all the required assertions are included, especially for non-intuitive things about causal relationships? There may be a mismatch in the level of expression of the security policy and a flaw. Anup replied that they map to a program, not to a flaw.

These two sessions on Security in Electronic Commerce generated interesting discussions among the conference participants. It was decided that the scope of future WG 11.3 conferences should be broadened to include such topics as security for E-Commerce, the WWW and Digital Libraries.

The third session was an invited talk by Joachim Biskup on "Technical Enforcement of Informational Assurances," and was chaired by David Spooner. Sushil asked the reason for using the word 'informational' rather than 'information'. Joachim said that it is a generalization of the word based on the German language. For John's question on whether a person can have multiple digital signatures under the German law, Joachim said yes. John was concerned about the presupposition of conflict resolution such that the intended purposes of a system are considered legitimate and consistent. When Joachim answered that one must relate it to prior law, John commented that this is very fluid as the law changes over time. Joachim said that periodic review of the security of a system is needed.

The last session on the first day of the conference was a panel discussion on "Privacy Issues in the WWW, Data Warehousing and Data Mining." Bhavani Thuraisingham chaired this session. The panelists, John Dobson, Sushil Jajodia, Martin Olivier and Pierangela Samarati, discussed issues such as anonymity versus accountability, data availability and access versus privacy, access control models for data warehouses, and conflicting and differing privacy policies in different countries. Ehud asked whether it is possible to have anonymous access to the web. Pierangela answered that anonymizers are available. Sujeet said Mike Reiter's work proves how anonymous anonymous is. Sushil asked whether we should trust the anonymizer. John responded that a decision has to be made about the risks involved and what information one is willing to share and not willing to share with others. T.C. asked what the borderline is between privacy and availability. Bhavani responded that the issues are more social than technical. Pierangela responded that availability is essential and more important than privacy in environments such as medical organizations.

For Anup's question on whether there are any technical solutions to protect user information collected by a web site, Sushil responded that clean policies and laws are needed and privacy issues need to be incorporated into access control. John responded by saying that technical solutions are not sufficient; the only solution is a method of recourse backed by law.

Bhavani concluded the panel by saying that the WWW Consortium is looking at security issues and asked whether anyone attending the conference knows what is going on there and how we can contribute. John responded that the current work of the consortium in the security area is flawed technology with no problem statement, and there is a need for a definition of security. The consensus was that the group should follow up with another panel session on WWW security at next year's conference in Seattle.

The second day of the conference started with a session on "Workflows," chaired by Tom Keefe. The first paper was "Analyzing the Safety of Workflow Authorization Models," by Huang, W.-K., and Atluri, V. This paper was

presented by Vijay Atluri. Vijay explained how the Workflow Authorization Model (WAM) can be extended to specify separation of duties constraints and showed how a safety analysis of WAM can be carried out using a Petri net based approach. Ehud asked how distributed authorizations can be checked. Vijay responded by saying that they are now using a centralized database and therefore everything can be determined from it. Tom added that a temporal part is not essential for enforcing separation of duties. Vijay said that they use a non-temporal projection of the authorization. The second paper in this session titled, "Rules and Patterns for Security in Workflow Systems," by Castano, S., and Fugini, M.G., was presented by Silvana Castano. She discussed how ECA rules are used to enforce authorization constraints in the Workflow Interactive Development Environment (WIDE) workflow management system.

T.C. Ting chaired the next session on "Policy Modeling." The first paper, "Security, Queries, and Autonomous Object Databases," by Gudes, E., and Olivier, M.S., was presented by Ehud Gudes. Ehud presented security policies to handle conflicts between local and global authorizations due to local autonomy. Sushil asked when data objects are replicated, how consistency of all the copies is ensured. Ehud said that they have not addressed this issue yet, but a version-based system may be appropriate. Karabulut asked how migration of object instances can be handled. Ehud said that global rules must be considered for moves. In addition, new local rules must be created. The original administrator loses control of the object instances.

The second paper titled, "Programmable Security for Object-Oriented Systems," by Hale, J., Papa, M., and Sheno, S., was presented by Sujeet Sheno. Sujeet showed how a primitive distributed object model can be used to support various types of decentralized authorization models by programming access control at the language level. Bhavani said that OMG has a standard object meta model and questioned the need for a new model. Sujeet said that it is part of a larger project that started before the OMG standard and that they can translate other meta models such as the OMG standard into their model. Ehud asked whether their model can handle a hierarchy of roles. Sujeet said that they have not looked at this yet, but are thinking that they should be able to do it. Bhavani suggested that they should look at the OMG standard and incorporate that in this work. Sujeet pointed out that it could be a problem because the OMG standard is a moving target. Tom asked what a token in the access control model is. Sujeet said that a token and a privilege together are needed to access an object and both are unforgeable. Karabulut asked about the relationship of their model to CORBA. Sujeet said that CORBA can be easily mapped into their model but they have not looked at this yet.

Sushil chaired the next session on "Mediation and Information Warfare Defense." The first paper, "Secure Mediation: Requirements and Design," by Biskup, J., Flegel, U., and Karabulut, Y. was presented by both Flegel and Karabulut. They first distinguished mediation from federation and presented approaches to secure interoperation. Bhavani asked if one needs to do mediation to do a federation. Flegel agreed that this is true but said that there are

differences between the two concepts that would become apparent. John asked whether they have considered the issue of requiring prior access to an information provider in order to establish a relationship with that provider, which also requires mediation. Karabulut said that they can extend their approach to handle this. John suggested that it would be useful to extend it into other types of relationships as well (anonymous, commercial, etc.).

The second paper, "Reconstructing the Database After Electronic Attacks," by Panda, B., and Giordano, J., was presented by Brijendra Panda. He presented algorithms to assess the damage after an attack and then to recover from the damage. Bhavani asked how the transaction that is causing the problem can be identified. Brijendra said that they assume an intrusion detection system that is capable of determining this. John asked how they can justify undoing operations based on false information resulting from previous intrusions. Brijendra said that they cannot handle situations where bad data is remembered outside the system and used in later transactions. Tom asked whether they can model data that leaves the system and notify users when a problem is discovered with it. Brijendra responded that he believes this can be done, but added that it might require maintaining a lot of extra data. Sushil said that external effects can be fixed outside the system in some other way. Sushil commented that this can be called data corruption detection, which is similar to storage jamming that was described at a previous WG 11.3 conference. Storage jamming also tries to detect corruption. Sushil added that a new research direction would be to look at what to do to recover after the detection. Pierangela asked whether they keep track of the conditions that lead to the updates. Redoing old operations from the log is not sufficient since the conditions may change and different operations should be done. Sushil added that the log doesn't make sense any more. Brijendra said that the entire transaction must be re-executed in the proper sequence. Ehud commented that it is not always possible to re-execute, e.g., ATM machine. Sushil said that there is a need to look deeper at the transaction before deciding what to do.

The last session on the second day was on "Multilevel Security," and was chaired by Bhavani. The first paper titled, "Version Management in the STAR MLS Database System," by Sripada, R., and Keefe, T., was presented by Tom Keefe. There were few questions regarding this paper.

The second paper, "SACADOS: a Support Tool to Manage Multilevel Documents," by Carrere, J., Cuppens, F., and Saurel, C., was presented by Jerome Carrere. Sushil asked when a new rule is applied, whether all the rules are recursively applied, and Jerome answered yes. Then Sushil questioned how conflicting rules are handled. Jerome replied that they use a resolution strategy that orders rules by priority. Sushil commented that all exceptions then need to be planned in advance to get the priorities correct. Joachim asked whether the previous work of their group that focused on complete and consistent assignment of labels is related to the present work. Jerome said no.

At the closing of this session, Bhavani asked whether anyone has comments on MLS. Sushil responded that we need to wait and see what happens with

existing commercial MLS products. He said that a new approach uses COTS and firewalls, but there are still interesting problems in MLS from a research point of view. A few people in the group said that they are still interested in working in this area. Bhavani said that no OODBMS vendor has picked up MLS ideas in a commercial product and noted that MLS aggregation and inference work transfers to data mining. Sushil said that only MLS systems are built with assurance in mind. Bhavani asked whether there are any agencies funding MLS research. Jerome said that in France there is support for MLS research and Sushil added that funding for MLS appears to be declining, but there is still some interest.

The first session on the third day was on "Role-based Access Controls and Mobile Databases" and was chaired by Silvana Castano. The first paper, "Using Role-Templates for Handling Recurring Role Structures" by Essmayr, W., Kapsammer, E., Wagner, R.R., and Tjoa, A.M. was presented by Wolfgang Essmayr. Bhavani asked whether the notion of 'agent' is similar to the notion of 'mediator'. Wolfgang said yes. Joachim commented that reuse of concepts is well known in programming languages and asked how this work is different. Wolfgang said that they mapped the concepts in programming languages to the concept of roles. Tom asked whether they need to modify applications to take advantage of role templates. Wolfgang said that they are not that far yet. Ehud asked whether they can specify different instances of roles to have different privileges. Wolfgang answered yes. Silvana asked how one can identify what templates are needed for roles. Wolfgang said that they can provide tools to do this analysis.

The second paper titled, "Security Capabilities and Potentials of Java" by Smarkusky, D.L., Demurjian, S.A.Sr., Bastarrica, M.C., and Ting, T.C., was presented by T.C. Ting. Ehud asked given roles, why are access control lists used. T.C. said that they provide additional functionality outside of roles and there is an access control list for each role that controls access to methods. Joachim asked whether translating roles to a class hierarchy using scope and visibility was enough to guarantee security. T.C. said that one can use public interfaces as in most OO systems and scope and visibility is one way to do it, but it may not be secure enough for all cases. Bhavani suggested that they need to work closely with the Java Security Group by making suggestions to them and learning from their work.

The third paper, "Security Issues in Mobile Database Access," by Lubinski, A. was presented by Astrid Lubinski. John asked what assumptions are made about the underlying network structure? Astrid said that she assumes a fixed network between base stations where only the first and last links can be mobile. Karabulut asked what minimal security means. Astrid said that this means the abstraction of the security rules to two or three main rules that must be satisfied and that often this takes the form of encryption. George Pangalos asked how the mobile component affects the security rules. Astrid said that it depends on the situation and there is no one answer. Bhavani asked whether there is any other work in this area. John responded that there has been a lot of classified

work in this area and the idea in this work is to separate the medium into a large number of segments so that one can have counter measures using different channels and introducing noise. T.C. asked whether packet switching can be a problem and added that time switching has more opportunities. Sushil added that this is the start of new work and more has to be done in this area.

The final session of the conference was on "Inference and Privacy," and was chaired by Ehud. The first paper, "Bayesian Methods Applied to the Database Inference Problem," by Chang, L., and Moskowitz, I. S., was presented by LiWu Chang. John asked whether they have any methods for estimating the confidence level. On the same note, Ehud asked what can be done as a defense for this approach. LiWu said that one might try spurious data and classifying more data. However, one does not want to undermine the usefulness of the database.

The second paper titled, "Inference Detection - A Data Level Approach," by Yip, R., and Levitt, K., was presented by Raymond Yip. Tom asked whether they used simulation or performance measurements in their study. Raymond said that they generated a database and queries and then measured the performance. Tom noted that one must consider the history, which gets larger and larger. Vijay added that changes to the database may invalidate the history. Raymond said that they consider changes as new information and can also search the history to identify problems. Sujeet asked how they handle collusion. Raymond said that they combine the queries of users together. Sushil noted that one can perform the analysis in data dependent or data independent mode depending on the goals. Ehud asked about the complexity of the approach. Raymond said that there is not much overlap between queries in general, so the complexity is manageable.

The last paper, "An Information-Flow Model for Privacy (InfoPriv)," by Dreyer, L.C.J., and Olivier, M.S., was presented by L. C. J. Dreyer. John asked how the assumptions about the environment are made. Tom said that one can trust certain users not to do certain things. John said that the only assumption one can make is that one cannot trust anyone, and added that serious breaches in the past have come from people who were trusted. He warned that the assumptions are too optimistic. Martin replied that their approach cannot catch all cases but will catch many. Sushil said that this is an important problem that we need to work on. John asked whether there is an assumption that people do not lie. Dreyer said that they assume that values are copied from entity to entity. But John said that in reality, people lie. Joachim noted that this is a very important problem, however, reducing privacy to information flow is like using agents to represent people and such systems have proven to be difficult to analyze. Ehud added that putting the user in the system allows one to include the user in the analysis. However, today firewalls control the flow between sites. Joachim said that firewalls do not consider the semantics of the information.