「IFIP WG 11.3 資料與應用安全年度會議」會議之出國報告

報告人：東吳大學資訊科學系 何煒華、鄭爲民

目　　錄

一、會議名稱

20th Annual IFIP WG11.3 Working Conference on Data and Application Security

二、參加會議目的及效益

IFIP (International Federation for Information Processing, IFIP)成立於 1960 年之資訊處理國際聯盟，該非營利組織聯盟與聯合國及其他非政府國際組織皆維持有良好關係；IFIP 於 1986 年成立 WG 11.3，本工作小組的目的在於促進資料安全研究與資料安全技術之應用，鼓勵有關資料安全需求的技術發展，使得設計與實現能滿足安全需求，並保證系統能滿足實際運作時的需求。WG 11.3 每年舉辦年度會議，本次目的除了聆聽論文發表之外，希望藉由專題演講(keynote speech)瞭解企業流程(business process)的安全議題。

此行趁此良好機會請教 Volkmar Lotz 有關 SAP 對於諸如引用或如何看待 ISO/IEC 等國際標準之現況，根據他及同僚的回答 SAP 對於國際標準是非常重視的，安全的技術發展會遵循既有的標準。該公司持續監視不同技術委員會之工作產品發展，也在適當機會以重要的軟體發展者身份提出建議，具體例子包括 metadata 等有關國際標準之制定及使用。因爲在企業之間的企業流程標準化是一大難題，因此實務上要考量安全議題更顯得複雜。此行最大的收穫，是聆聽到國際權威的商業資訊廠商，說明企業流程的安全議題，唯有安全的環境，才能促進電子商業的發展。

三、會議時間

2006 年 7 月 31 至 8 月 2 日

四、會議地點

Sophia Antipolis, France

五、會議摘要：會議議程及會議紀要

(一)、會議議程

本次會議一共收到 57 篇投稿論文，經審查後共接受 22 篇論文，多數均爲理論性之論文，作者來自歐亞美各洲，分別排入三天之議程加以發表。今年度發表的論文主要集中於存取控制(直接相關的論文共有九篇)，其它議題僅有零星的一兩篇論文，包括資料庫安全、資安政策、安全管理、入侵偵測與安全分析等議題，除了論文發表之外，大會於第一天安排邀請演講。詳細議程如下：

2006 年 7 月 31 日

9:00 Registration

9:30 - 10:30 Welcome and Keynote

Keynote Speech: Business Process Security Research directions.
Volkmar Lotz, Security & Trust Research Program Manager at SAP Research 11:00 - 13:00 Session 1: Privacy and Secrecy

Enhancing User Privacy through Data Handling Policies
Claudio Ardagna, Sabrina De Capitani di Vimercati, Pierangela Samarati

Efficient Enforcement of Security Policies based on Tracking of Mobile Users
Vijay Atluri, Heechang Shin

Information Theoretical Analysis of Two-Party Secret Computation
Da-Wei Wang, Churn-Jung Liau, Yi-Ting Chiang, Tsan-sheng Hsu

Detection and Resolution of Anomalies in Firewall Policy Rules
Muhammad Abedin, Syeda Nessa, Latifur Khan, Bhavani Thuraisingham

Interactive Analysis of Attack Graphs Using Relational
Lingyu Wang, Chao Yao, Anoop Singhal, Sushil Jajodia

13:00 Lunch at SAP / End of Conference

15:30 - 17:00 Session 2: Access Control for Coalitions and Business Processes

Consolidating the Access Control of Composite Applications and Workflows
Martin Wimmer, Alfons Kemper, Maarten Rits, Volkmar Lotz

A Distributed Coalition Service Registry for Ad-hoc Dynamic Coalitions: A Service-oriented Approach
Ravi Mukkamala, Vijay Atluri, Janice Warner, Ranjit Abbadasari

From Business Process Choreography to Authorization Policies
Philip Robinson, Florian Kerschbaum1, and Andreas Schaad

2006 年 8 月 1 日

9:30 - 11:00 Session 3: Flexible Access Control

Creating Objects in the Flexible Authorization Framework
Nicola Zannone, Sushil Jajodia, Duminda Wijesekera

A Framework for Flexible Access Control in Digital Library Systems
Indrajit Ray, Sudip Chakraborty

Authrule: A Generic Rule-Based Authorization Module
Sonke Busch, Bjorn Muschall, Gunther Pernul, Torsten Priebe

11:30 - 13:00 Session 4: Authentication, Integrity, and Inference Control

Aggregation Queries in the Database-As-a-Service Model
Einar Mykletun, Gene Tsudik

XML Streams Watermarking
Julien Lafaye, David Gross-Amblard

On Finding an Inference-Proof Complete Database for Controlled Query Evaluation

Joachim Biskup, Lena Wiese

13:00 Lunch at SAP

14:30 - 16:00 Session 5: Role-based Access Control

Resolving Information Flow Conflicts in RBAC Systems
Noa Tuval, Ehud gudes

Discretionary and Mandatory Controls for Role-Based Administration
Jason Crampton

Term Rewriting for Access Control
Steve Barker, Maribel Fernandez

2006 年 8 月 2 日

9:00 - 10:30　Session 6: Identity Management and Applications Security

Notarized Federated Identity Management for Web Services
Michael Goodrich, Roberto Tamassia, Danfeng Yao

Policy Transformations for Preventing Leakage of Sensitive Information in Email Systems
Saket Kaushik, William Winsborough, Duminda Wijesekera, Paul Ammann

Aspect-Oriented Risk Driven Development of Secure Applications
Geri Georg, Siv Hilde Houmb, and Indrakshi Ray

11:00 -- 12:00　Session 7: Secure Query Rewriting and Execution

Authenticating Multi-Dimensional Query Results in Data Publishing
Weiwei Cheng, HweeHwa Pang, Kian-Lee Tan

Policy Classes and Query Rewriting Algorithm for XML Security Views
Nataliya Rassadko, Gabriel Kuper, Fabio Massacci

(二)、會議紀要

本次 IFIP WG 11.3 資料與應用安全工作小組會議由名聞遐邇的 ERP 領導軟體廠商 SAP 主辦，地點位於法國南部 Sophia Antipolis 的 SAP 實驗室，大會主席由自稱海灘男孩的 Andreas Schaad 博士擔任，議程共同主席由來自賓州州立大學之 Peng Liu 博士一起負責做會議背景說明與介紹主講者。

爲闡明資料與應用安全對於諸如 ERP 軟體之影響及 SAP 在其上設計開發之理念，本次專題演講係邀請 SAP 在地之安全分析暨研發主管 Volkmar Lotz 擔任主講人，經由其個人之自我介紹，瞭解到他不僅關注安全需求工程、密碼學協定驗證、及行動編碼安全等具代表性之重要領域之研究，更參與智慧卡之處理器之正規安全模式之發展，也肩負德國政府贊助之行動內容系統之相關計畫，所以本次由他來擔任主講更加涵概理論研究與實務之雙重領域。

SAP 每年超過 85 億美元之營收及全球有超過五百萬以上之軟體發展者(請注

意不是使用者人數，使用者人數必當數倍於此)，Volkmar Lotz 從企業流程的角度分析安全的議題，IT 系統在 SAP 軟體的設計理念中扮演便利企業流程變革之功能，這項任務之完成需要包括企業標準化作業程序、聯合團隊之組織、便利變革進行之環境與企業流程平台。在 SAP 設計概念下更進一步將此分爲平台與應用的兩層架構，平台是包括如商業智慧(business intelligence)等可能加以行動化之層次，而應用層則是存在如顧客資源管理(CRM)與 Legacy 系統之 SAP 經常提供之典型軟體，也就是說整體設計由下而上分別是透過許多底層的企業流程組件，再利用服務的貯備處及最上層的複合應用提供顧客解決方案，使用對象則分成供應者、內部系統管理與購買者三者。

BPP (business process platform)則可分解成兩種不同平台，分別是應用平台與技術平台，有關安全的概念如下：

1. 由於安全機制在異質的系統環境上不是一個容易的工作，但是企業流程延伸至所有系統元件並形成一個整合的系統亦爲必須，故所有 IT 之從業人員不能將安全的解決方案視爲個別之技術解決方案，而是必須在整合的安全系統中透過 security building block 進行彈性建構及整合。
2. 在一個如 SAP 的標準化商業應用系統中，對使用者安全機制進行組態化通常是相當困難且容易出錯，SAP 的設計理念乃透過例如以 UML 語言爲基礎之 model-driven security 工具，對安全策略規則做自動化檢查，由於這種模組化的設計，對於標準化商業應用系統安全相關資源之組態管理工作較爲便利。
3. 在使用 SAP 相關之環境中皆存在有許多安全相關之限制，但同時顧客也想保有他們針對特定企業流程能加以發展之最大彈性(flexibility)，更必須對企業整合其他系統等需求提供 openness，這是不同於一般安全機制的考量，會是更大的挑戰。

故 SAP 之發展策略乃在於尋求可容忍的風險(tolerable risk)與企業需求(business need)之間可能的平衡，評估兼顧此兩大因素，並利用使用者或管理者

可觀察(observable)或可管理(manageable)的精神進行安全管制設計及措施，其目標乃在於以最小的管理成本達到管理跨組件軟體，並適合於不同企業間企業流程相異之需求。另外關於社會層面，主講人也提出如何建立服務的基礎建設，首先是要推動一個跨企業、國家、及社會的行動，並且也需要政府與社會對此有更多的約束控制，例如透過配套的法律框架等方為可行。

六、心得及建議

本次主辦單位 SAP 是國際性的資訊廠商，對於國際標準自是非常的重視，該公司持續監視不同技術委員會之工作產品發展，也在適當機會以重要軟體發展者身份提出建議，具體例子包括 metadata 等有關國際電子商務相關技術標準之制定及使用。SAP 是以企業流程出發，雖然企業之間流程很難標準化，但其軟體發展所採用的安全技術會遵循國際標準，足以作為國內相關業者在發展產品之借鏡。雖說本次專題演講不似典型的演講，提出一些近來理論發展回顧或演講者本人專精領域之概括介紹，但由全球首大電子商務軟體發展者之資訊安全部門主管以他的角度，分享其在融入資訊安全考量上的寶貴實務發展經驗，算是此行的一大收穫。

本次受限於主辦單位的場地，開始接受報名時才公布報名人數限制在四十人，原本還誤認為是在住宿旅館舉辦此次會議，扣除參與的論文作者，名額所剩無幾，這是很少見的情形。由於限制報名人數，影響經費的收入，另外其會議場地也不適合舉辦座談討論，因而本次會議未安排座談討論。本次大會直到七月才公布會議議程，議程的規劃與出國參訪規劃當時的評估是有落差的，成效不如當初所預期的好。受限於出國參訪的行政流程、預定機票、住宿等問題，因而未取消此次行程。本次出國特別規劃參加此會議，行前無法預估主辦單位的能力而產生預期的落差，主辦單位雖是國際的資訊廠商，但無法妥善安排議程與場地，擴大參與率殊為可惜。

七、附件

（一）、論文集編輯委員

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
University of Dortmund, Germany

Madhu Sudan
Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

MosheY. Vardi
Rice University, Houston, TX, USA

GerhardWeikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

（二）、論文摘要

1. Creating Objects in the Flexible Authorization Framework

Nicola Zannone, Sushil Jajodia, Duminda Wijesekera

Access control is a crucial concern to build secure IT systems and, more specifically, to protect the confidentiality of information. However, access control is necessary, but not sufficient. Actually, IT systems can manipulate data to provide services to users. The results of a data processing may disclose information concerning the objects used in the data processing itself. Therefore, the control of information flow results fundamental to guarantee data protection. In the last years many information flow control models have been proposed. However, these frameworks mainly focus on the detection and prevention of improper information leaks and do not provide support for the dynamical creation of new objects.

In this paper we extend our previous work to automatically support the dynamical creation of objects by verifying the conditions under which objects can be created and automatically associating an access control policy to them. Moreover, our proposal includes mechanisms tailored to control the usage of information once it has been accessed.

This material is based upon work supported by the National Science Foundation under grants IIS-0242237 and IIS-0430402. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. This work was partly supported by the projects RBNE0195K5 FIRB-ASTRO, 016004 IST-FP6-FET-IP-SENSORIA, 27587 IST-FP6-IP-SERENITY, 2003-S116-00018 PAT-MOSTRO.

2. Detection and Resolution of Anomalies in Firewall Policy Rules

Muhammad Abedin, Syeda Nessa, Latifur Khan,
Bhavani Thuraisingham

A firewall is a system acting as an interface of a network to one or more external networks. It implements the security policy of the network by deciding which packets to let through based on rules defined by the network administrator. Any error in defining the rules may compromise the system security by letting unwanted traffic pass or blocking desired traffic. Manual definition of rules often results in a set that contains conflicting, redundant or overshadowed rules, resulting in anomalies in the policy. Manually detecting and resolving these anomalies is a critical but tedious and error prone task. Existing research on this problem have been focused on the analysis and detection of the anomalies in firewall policy. Previous works define the possible

relations between rules and also define anomalies in terms of the relations and present algorithms to detect the anomalies by analyzing the rules. In this paper, we discuss some necessary modifications to the existing definitions of the relations. We present a new algorithm that will simultaneously detect and resolve any anomaly present in the policy rules by necessary reorder and split operations to generate a new anomaly free rule set. We also present proof of correctness of the algorithm. Then we present an algorithm to merge rules where possible in order to reduce the number of rules and hence increase efficiency of the firewall.

3. On Finding an Inference-Proof Complete Database for Controlled Query Evaluation

Joachim Biskup, Lena Wiese

Controlled Query Evaluation (CQE) offers a logical framework to prevent a user of a database from inadvertently gaining knowledge he is not allowed to know. By modeling the user's a priori knowledge in an appropriate way, a CQE system can control not only plain access to database entries but also inferences made by the user. A dynamic CQE system that enforces inference control at runtime has already been investigated. In this article, we pursue a static approach that constructs an inference-proof database in a preprocessing step. The inference-proof database can respond to any query without enabling the user to infer confidential information. We illustrate the semantics of the system by a comprehensive example and state the essential requirements for an inference-proof and highly available database. We present an algorithm that accomplishes the preprocessing by combining SAT solving and "Branch and Bound".

4. Consolidating the Access Control of Composite Applications and Workflows

Martin Wimmer, Alfons Kemper, Maarten Rits, Volkmar Lotz

The need for enterprise application integration projects leads to complex composite applications. For the sake of security and efficiency, consolidated access control policies for composite applications should be provided. Such a policy is based on the policies of the corresponding autonomous sub-applications and has the following properties: On the one hand, it needs to be as restrictive as possible to block requests which do not comply with the integrated sub-applications' policies. Thereby, unsuccessful executions of requests are prevented at an early stage. On the other hand, the composite policy must grant all necessary privileges in order to make the intended functionality available to legitimate users.

In this paper, we present our formal model and respective algorithmic solutions for consolidating the access control of composite applications. The generated policies

conform to the presented requirements of the least privileges paradigm and, thus, allow to revise and optimize the access control of composite applications. We demonstrate this by means of Web service workflows that constitute the state of the art for the realization of business processes.

5. Authenticating Multi-dimensional Query Results in Data Publishing

Weiwei Cheng, HweeHwa Pang, Kian-Lee Tan

In data publishing, the owner delegates the role of satisfying user queries to a third-party publisher. As the publisher may be untrusted or susceptible to attacks, it could produce incorrect query results. This paper introduces a mechanism for users to verify that their query answers on a *multi-dimensional dataset* are correct, in the sense of being complete (i.e., no qualifying data points are omitted) and authentic (i.e., all the result values originated from the owner). Our approach is to add authentication information into a spatial data structure, by constructing certified chains on the points within each partition, as well as on all the partitions in the data space. Given a query, we generate proof that every data point within those intervals of the certified chains that overlap the query window either is returned as a result value, or fails to meet some query condition. We study two instantiations of the approach: Verifiable KD-tree (VKDtree) that is based on space partitioning, and Verifiable R-tree (VRtree) that is based on data partitioning. The schemes are evaluated on window queries, and results show that VRtree is highly precise, meaning that few data points outside of a query result are disclosed in the course of proving its correctness.

6. XML Streams Watermarking

Julien Lafaye, David Gross-Amblard

XML streams are valuable, continuous, high-throughput sources of information whose owners must be protected against illegal redistributions. Watermarking is a known technique for hiding copyrights marks within documents, thus preventing redistributions. Here, we introduce a watermarking algorithm for XML streams so that (i) the watermark embedding and detection processes are done online and use only a constant memory, (ii) the stream distortion is controlled, (iii) the type of the stream is preserved and finally (iv) the detection procedure does not require the original stream. We also evaluate, analytically and experimentally, the robustness of the algorithm against watermark removal attempts.

Work supported by the ACI Sécurité & Informatique TADORNE grant (2004-2007).

7. Aggregation Queries in the Database-As-a-Service Model

Einar Mykletun, Gene Tsudik

In the Database-As-a-Service (DAS) model, clients store their database contents at servers belonging to potentially untrusted service providers. To maintain data confidentiality, clients need to outsource their data to servers in encrypted form. At the same time, clients must still be able to execute queries over encrypted data. One prominent and fairly effective technique for executing SQL-style range queries over encrypted data involves partitioning (or bucketization) of encrypted attributes.

However, executing aggregation-type queries over encrypted data is a notoriously difficult problem. One well-known cryptographic tool often utilized to support encrypted aggregation is homomorphic encryption; it enables arithmetic operations over encrypted data. One technique based on a specific homomorphic encryption function was recently proposed in the context of the DAS model. Unfortunately, as shown in this paper, this technique is insecure against ciphertext-only attacks. We propose a simple alternative for handling encrypted aggregation queries and describe its implementation. We also consider a different flavor of the DAS model which involves mixed databases, where some attributes are encrypted and some are left in the clear. We show how range queries can be executed in this model.

This work was supported by in part by NSF Awards 0331707 (ITR-DAS) and 0220069 (ITR-RESCUE).

8. Policy Classes and Query Rewriting Algorithm for XML Security Views

Nataliya Rassadko

Most state-of-the-art approaches of securing XML documents are based on a partial annotation of an XML tree with security labels which are later propagated to unlabeled nodes of the XML so that the resulting labeling is full (i.e. defined for every XML node). The first contribution of this paper is an investigation of possible alternatives for policy definition that lead to a fully annotated XML. We provide a classification of policies using different options of security label propagation and conflict resolution. Our second contribution is a generalized algorithm that constructs a full DTD annotation (from the the partial one) w.r.t. the policy classification. Finally, we discuss the query rewriting approach for our model of XML security views.

This work has been partially supported by MIUR under the project FIRB-ASTRO, by PAT under the project PAT-MOSTRO and by the EU Commission under the project EU-IST-IP-SERENITY.

9. Interactive Analysis of Attack Graphs Using Relational Queries

Lingyu Wang, Chao Yao, Anoop Singhal, Sushil Jajodia

Attack graph is important in defending against well-orchestrated network intrusions. However, the current analysis of attack graphs requires an algorithm to be developed and implemented, causing a delay in the availability of analysis. Such a delay is usually unacceptable because the needs for analyzing attack graphs may change rapidly in defending against network intrusions. An administrator may want to revise an analysis upon observing its outcome. Such an *interactive* analysis, similar to that in decision support systems, is difficult if at all possible with current approaches based on proprietary algorithms. This paper removes the above limitation and enables interactive analysis of attack graphs. We devise a relational model for representing necessary inputs including network configuration and domain knowledge. We generate the attack graph from those inputs as relational views. We then show that typical analyses of the attack graph can be realized as relational queries against the views. Our approach eliminates the needs for developing a proprietary algorithm for each different analysis, because an analysis is now simply a relational query. The interactive analysis of attack graphs is now possible, because relational queries can be dynamically constructed and revised at run time. Moreover, the mature optimization techniques in relational databases can also improve the performance of the analysis.

This material is based upon work supported by National Institute of Standards and Technology Computer Security Division; by Homeland Security Advanced Research Projects Agency under the contract FA8750-05-C-0212 administered by the Air Force Research Laboratory/Rome; by Army Research Office under grants DAAD19-03-1-0257 and W911NF-05-1-0374, by Federal Aviation Administration under the contract DTFAWA-04-P-00278/0001, and by the National Science Foundation under grants IIS-0242237 and IIS-0430402. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsoring organizations.

10. Notarized Federated Identity Management for Web Services

Michael T. Goodrich, Roberto Tamassia, Danfeng Yao

We propose a *notarized* federated identity management model that supports efficient user authentication when providers are unknown to each other. Our model introduces a notary service, owned by a trusted third-party, to dynamically notarize assertions generated by identity providers. An additional feature of our model is the avoidance of direct communications between identity providers and service providers, which provides improved privacy protection for users. We present an efficient implementation of our notarized federated identity management model based on the Secure Transaction Management System (STMS). We also give a practical solution for mitigating aspects of the identity theft problem and discuss its use in our notarized

federated identity management model. The unique feature of our cryptographic solution is that it enables one to proactively prevent the leaking of secret identity information.

This work was supported in part by the National Science Foundation under grants IIS–0324846, CCF–0311510 and CNS–0303577, and by IAM Technology, Inc. The work of the first author was done primarily as a consultant to Brown University.

11. Resolving Information Flow Conflicts in RBAC Systems

Noa Tuval, Ehud Gudes

Recently, Role Based Access Control (RBAC) model has taken place as a promising alternative to the conventional access control models, MAC and DAC. RBAC is more general than those traditional models as was shown by Osborn et al. [17], however, mapping a role based system to a valid MAC configuration is not always possible because certain combinations of permissions that are included in a role's effective privileges may cause information flow. Given a role-based graph where role's permissions refer to labeled data objects, Osborn et al. showed how to find conflicts that are resulted from information flow, but they have not suggested a solution for these conflicts and they have not handled user-role assignments, for the solved scheme. In this paper, we assume a more general model of permissions conflicts than MAC. We introduce an algorithm that handles information flow conflicts in a given role-based graph, corrects the Role-based graph if needed, and proposes a consistent users-roles assignment. As RBAC and information flow are becoming extremely important in Web based information systems, this algorithm becomes very relevant.

12. Policy Transformations for Preventing Leakage of Sensitive Information in Email Systems

Saket Kaushik, William Winsborough, Duminda Wijesekera, Paul Ammann

In this paper we identify an undesirable side-effect of combining different email-control mechanisms for protection from unwanted messages, namely, leakage of recipients' private information to message senders. The problem arises because some email-control mechanisms like bonds, graph-turing tests, *etc.*, inherently leak information, and without discontinuing their use, leakage channels cannot be closed. We formalize the capabilities of an attacker and show how she can launch guessing attacks on recipient's mail acceptance policy that utilizes leaky mechanism in an effort to avoid unwanted mail.

The attacker in our model guesses the contents of a recipient's private information. The recipients' use of leaky mechanisms allow the sender to verify her guess. We assume a constraint logic programming based policy language for specification and

evaluation of mail acceptance criteria and present two different program transformations that can prevent guessing attacks while allowing recipients to utilize any email-control mechanism in their policies.

13. Term Rewriting for Access Control

Steve Barker, Maribel Fern'andez

We demonstrate how access control models and policies can be represented by using term rewriting systems, and how rewriting may be used for evaluating access requests and for proving properties of an access control policy. We focus on two kinds of access control models: discretionary models, based on access control lists (ACLs), and role-based access control (RBAC) models. For RBAC models, we show that we can specify several variants, including models with role hierarchies, and constraints and support for security administrator review querying.

14. Discretionary and Mandatory Controls for Role-Based Administration

Jason Crampton

Role-based access control is an important way of limiting the access users have to computing resources. While the basic concepts of role-based access control are now well understood, there is no consensus on the best approach to managing role-based systems. In this paper, we introduce a new model for role-based administration, using the notions of discretionary and mandatory controls. Our model provides a number of important features that control the assignment of users and permissions to roles. This means that we can limit the damage that can be done by malicious administrative users. We compare our approach to a number of other models for role-based administration, and demonstrate that our model has several advantages.

15. A Distributed Coalition Service Registry for Ad-Hoc Dynamic Coalitions: A Service-Oriented Approach

Ravi Mukkamala, Vijayalakshmi Atluri, Janice Warner, Ranjit Abbadasari

It is often necessary for organizations to come together in a coalition to share services, without prior planning, to accomplish certain tasks. The *dynamic coalition-based access control* (DCBAC) model facilitates the formation of dynamic coalitions through the use of a registry service, where available services can be advertised by potential coalition members. The central component of the DCBAC model is the *distributed coalition service registry* (DCSR). Depending upon the levels of service needed by the service providers and requesters, DCSR provides different functionality. We define three levels of DCSR services: (i) Registry Service (ii)Authenticator Service, and (iii) Query Service. For the last service, DCSR answers a specific

question directly by using the information resources of service providers, when the requester has needed credentials. No direct interactions are needed between the coalition members in this level of service. In this paper, we describe our service-oriented approach to DCSR design and show the flexibility that it offers. The design features are tested through a prototype DCBAC system built using the .Net framework.

The work of Atluri and Warner is supported in part by the National Science Foundation under grant IIS-0306838.

16. Enhancing User Privacy Through Data Handling Policies

Claudio Ardagna, Sabrina De Capitani di Vimercati, Pierangela Samarati

The protection of privacy is an increasing concern in today's global infrastructure. One of the most important privacy protection principles states that personal information collected for one purpose may not be used for any other purpose without the specific *informed consent* of the person it concerns. Although users provide personal information for use in one specific context, they often have no idea on how such a personal information may be used subsequently.

In this paper, we introduce a new type of privacy policy, called *data handling policy*, which defines how the personal information release will be (or should be) dealt with at the receiving party. A data handling policy allows users to define simple and appropriate levels of control over who sees what information about them and under which circumstances.

17. Efficient Enforcement of Security Policies Based on Tracking of Mobile Users

Vijayalakshmi Atluri, Heechang Shin

Recent advances to mobile communication, Global Positioning System (GPS) and Radio Frequency Identification (RFID) technologies have propelled the growth of a number of mobile services. These require maintaining mobile object's location information and efficiently serving access requests on the *past, present* and *future* status of the moving objects. Moreover, these services raise a number of security and privacy challenges. To address this, security policies are specified to ensure controlled access to the mobile user's location and movement trajectories, their profile information, and stationary resources based on the mobile user's spatiotemporal information. Considering the basic authorization specification <subject, object, subject>, in a mobile environment, a moving object can be a subject, an object, or both. Serving an access request requires to search for the desired moving objects that satisfy the query, as well as enforce the security policies.

Often, enforcing security incurs overhead, and as a result may degrade the

performance of a system. To alleviate this problem, recently Atluri and Guo have proposed an unified index structure, ^{S}TPR-tree, to organize both the moving objects and authorizations specified over them. However, the ^{S}TPR-tree is not capable supporting security policies based on *tracking* of mobile users. In this paper, we present an index structure, called S^{PPF}-tree, which maintains past, present and future positions of the moving objects along with authorizations by employing *partial persistent storage*. We demonstrate how the S^{PPF}-tree can be constructed and maintained, and provide algorithms to process two types of access requests, including moving object requests by stationary subjects such as *locate* and *track*, and stationary object requests by moving subjects.

This work is supported in part by the National Science Foundation under grant IIS-0242415.

18. A Framework for Flexible Access Control in Digital Library Systems

Indrajit Ray, Sudip Chakraborty

Traditional access control models are often found to be inadequate for digital libraries. This is because the user population for digital libraries is very dynamic and not completely known in advance. In addition, the objects stored in a digital library are characterized by fine-grained behavioral interfaces and highly-contextualized access restrictions that require a user's access privileges to be updated dynamically. These motivate us to propose a trust-based authorization model for digital libraries. Access privileges can be associated with both objects and content classes. Trust levels associated with these specify the minimum acceptable level of trust needed of a user to allow access to the objects. We use a vector trust model to calculate the system's trust about a user. The model uses a number of different types of information about a user, for example, prior usage history, credentials, recommendations etc., to calculate the trust level in a dynamic manner and thus achieve a fine-grained access control.

This work was partially supported by the U.S. Air Force Research Laboratory (AFRL) and the Federal Aviation Administration (FAA) under contract F30602-03-1-0101 and by the National Science Foundation (NSF) of the USA under grant IIS-0242258. Any opinions, findings, and conclusions or recommendations expressed in this publication are solely those of the authors and do not necessarily represent those of the AFRL, the FAA, or the NSF.

19. Authrule: A Generic Rule-Based Authorization Module

Sonke Busch, Bjorn Muschall, Gunther Pernul, Torsten Priebe

As part of the access control process an authorization decision needs to be taken based on a certain authorization model. Depending on the environment different models are

applicable (e.g., RBAC in organizations, MAC in the military field). An authorization model contains all necessary elements needed for the decision (e.g., subjects, objects, and roles) as well as their relations. As these elements are usually inherent in the software architecture of an access control module, such modules limit themselves to the use of a certain specific authorization model. A later change of the model consequently results in a substantial effort for revising the software architecture of the given module. Rule-based systems are well suited to represent authorization models by mapping them to facts and rules, which can be modified in a flexible manner. In this paper we present a generic authorization module, which can take authorization decisions on the basis of arbitrary models utilizing rule-based technology. The implementation of the popular RBAC and ABAC (attribute-based access control) models is demonstrated

20. Aspect-Oriented Risk Driven Development of Secure Applications

Geri Georg, Siv Hilde Houmb, Indrakshi Ray

Security breaches seldom occur because of faulty security mechanisms. Often times, security mechanisms are incorrectly incorporated in an application which allows them to be bypassed resulting in a security breach. Methodologies are needed for incorporating security mechanisms in an application and assessing whether the resulting system is indeed secure. We propose one such methodology for designing secure applications. We begin by identifying the assets in the application that need protection. We then find the kinds of attacks that are typical for such applications. We show how to evaluate the application against such attacks. If the results are unacceptable, that is, they pose a high security risk, then some security mechanism must be incorporated into the application. We illustrate how this can be done and show how the resulting system can be evaluated to give assurance that it is resilient to the given attack.

21. From Business Process Choreography to Authorization Policies

Philip Robinson, Florian Kerschbaum, Andreas Schaad

A choreography specifies the interactions between the resources of multiple collaborating parties at design time. The runtime management of authorization policies in order to support such a specification is however tedious for administrators to manually handle. By compiling the choreography into enhanced authorization policies, we are able to automatically derive the minimal authorizations required for collaboration, as well as enable and disable the authorizations in a just-in-time manner that matches the control flow described in the choreography. We have evaluated the advantage of this utility in a collaborative engineering scenario.

22. Information Theoretical Analysis of Two-Party Secret Computation

Da-Wei Wang, Churn-Jung Liau, Yi-Ting Chiang, Tsan-sheng Hsu

Privacy protection has become one of the most important issues in the information era. Consequently, many protocols have been developed to achieve the goal of accomplishing a computational task cooperatively without revealing the participants' private data. Practical protocols, however, do not guarantee perfect privacy protection, as some degree of privacy leakage is allowed so that resources can be used efficiently, e.g., the number of random bits required and the computation time. A metric for measuring the degree of information leakage based on an information theoretical framework was proposed in [2]. Based on that formal framework, we present a lower bound of the scalar product problem in this paper, and show that to solve the problem without the help of a third party, approximately half the private information must be revealed. To better capture our intuition about the secrecy of various protocols, we propose two more measurements: *evenness* and *spread*. The first measures how evenly the information leakage is distributed among the participants' private inputs. The second measures the size of the smallest set an adversary could use to obtain the same ratio of leaked information that could be derived in the worst case scenario.

「2006 密碼硬體暨嵌入式系統國際會議，Workshop on Cryptographic Hardware & Embedded Systems」會議之出國報告

報告人：吳宗成 教授

台灣科技大學資訊管理系

中華民國資訊安全學會

目　　錄

一、會議名稱

2006 年密碼硬體暨嵌入式系統國際會議，Workshop on Cryptographic Hardware and Embedded Systems （CHES）、日本橫濱。

二、參加會議目的及效益

國際密碼研究協會(International Association for Cryptologic Research)簡稱**IACR**，該協會除了會在固定時間舉辦三大國際密碼會議：美洲密碼會議(**CRYPTO**，簡稱美密)、歐洲密碼學國際會議(**EUROCRYPT**，簡稱歐密)及亞洲密碼學會議(**AISACRYPT**，簡稱亞密)之外，還會定期地舉辦四種不同類型的會議：密碼硬體及嵌入式系統會議(**CHES**: Workshop on Cryptographic Hardware and Embedded Systems)、密碼理論會議(**TCC**: Theory of Cryptography Conference)、公開金鑰密碼學之實用暨理論會議(**PKC**: International Workshop on Practice and Theory in Public Key Cryptography)及快速軟體加密會議(**FSE**: Fast Software Encryption)來探討密碼技術在不同領域的應用及發展情形。

CHES 會議為全世界公認密碼技術應用於硬體設備領域中，水準最高且最重要的國際會議。自從 1999 年開始，每年都會在不同城市來舉辦密碼硬體及嵌入系統講習會，今年是在日本橫濱洲際飯店(Yokohama Grand Intercontinental Hotel)舉行第八屆 **CHES 2006** 會議，會議日期為 10 月 10 日至 10 月 13 日。

本次會議所發表論文以密碼模組硬體與嵌入式系統設備之攻擊分析為主流議題，尤其是 Power analysis。參加本次會議可以瞭解資安硬體及嵌入式系統之國際上最新驗證理論與實作結果，對我國推動資安模組安全檢測或驗證標準之研擬與未來政策規劃有所助益。

三、會議時間

1. 報到

大會報到時間為 10 月 10 日下午 6:00 至 8:00，地點為的會客廳，大會工作人員親切且禮貌地為與會人員辦理辦到手續。同時也舉行簡單的歡迎餐會，各國與會人員藉此機會認識，交換彼此的研究心得，或閒話家常。

2. 開幕

大會開幕時間定於 10 月 11 日上午 9:00 至 9:10，首先由大會主席報告，

報告本屆會議籌備過程與介紹相關籌劃人員。本屆會議參加人數約為250人。

3. 專題演講

(1) **“Integer Factoring Utilizing PC Cluster”**, 主講者為日本NTT公司的Kazumaro Aoki博士。

(2) **“The Outer Limits of RFID Security”**, 主講者為美國RSA實驗室的Ari Juels博士。

(3) **“Challenges for Trusted Computing”**主講人為德國Ruhr University Bochum的Ahmad-Reza Sadeghi 博士

四、會議地點

日本橫濱洲際飯店(Yokohama Grand Intercontinental Hotel)的 Pacific 會議廳，座位數約 280。

五、會議議程及會議紀要

本屆會議進行三場專題演講，分別是：

(1) **“Integer Factoring Utilizing PC Cluster”**, 主講者為日本NTT公司的Kazumaro Aoki博士。

Aoki 博士指出整數因子分解問題是最久且重要的問題，並且不易思考。由於這種問題在最差情況下無法在多項式時間內解決，所以著名的 RSA 利用這種因子分解的困難度提高安全性。因為現在的硬體科技一年比一年進步，因此分解 1024 bits 整數的時機已經成熟了。已經有多數的研究在分析 1024 bits 整數的可能性。以表一來說明目前各種演算法的發展情形：

表一:各種因數分解方法之時間複雜度比較表

Method	Complexity	Effective range
TD	$L_p[1; 1]$	$p \le 2^{28}$
ECM	$L_p[1/2; 1.414]$	$p \le 2^{130}$
MPQS	$L_N[1/2; 1.020]$	$N \le 2^{320}$
SNFS	$L_N[1/3; 1.526]$	$N > 2^{320}$
GNFS	$L_N[1/3; 1.923]$	$N > 2^{320}$
MPGNFS	$L_N[1/3; 1.902]$	$N > 2^{2000}$ (?)

Where: $L_x[s; c]=\exp((c + o(1))(\log x)^s(\log \log x)^{1-s})$

TD: Trial Division；

ECM: Elliptic Curve Method

MPQS: Multiple Polynomial Quadratic Sieve

NFS: Number Field Sieve

SNFS: Small Number Field Sieve

GNFS: Generation Number Field Sieve

但由於硬體設備的進步，一些研究希望用合理費用買到能夠在一年內能夠處理 1024 bits 整數的特殊目的的硬體設備。然而，整數因子分解的世界公開紀錄並非能以這種類型的電腦更新。超級電腦的確能在整數因子分解上有更好的紀錄，但是超級電腦的費用並不在合理範圍內。如果是在有限的預算下，電腦群組似乎是一個更好的選擇。事實上，最近的世界紀錄都是由電腦群組創下的。這結果帶領了利用電腦群組進行整數因子分解的方法。一個因子分解團隊可能需要寫數萬行的程式以及需要使用數百台的電腦,然後再花上幾個月才能完成。綜合其:針對GNFS、SNFS及 ECM 之相關研究成果整理至下表二至表四來說明：

表二:針對 GNFS 的紀錄

合成數	位元數	時間(年/月)	作者
RSA-200	663	05/05	Bonn et al.
RSA-640	640	05/11	Bonn et al.
c176 in $11^{281}+1$	582	05/05	NTT et al.
RSA-576	576	03/12	Bonn et al.
c164 in $2^{1826}+1$	545	03/12	NTT et al.
RSA-160	530	03/04	Bonn

表三:針對 SNFS 的紀錄

合成數	位元數	時間(年/月)	作者
c274 in 6^{353}-1	911(913)	06/01	NTT et al.
c248 in 2^{1642}+1	822	04/03	NTT et al.
2^{809}-1	809	03/01	Bonn
c244 in 5^{349}-1	809(811)	06/04	Kruppa+ Bonn
c239 in 2^{811}-1	793(811)	04/06	NFSNET
c234 in 3^{491}+1	777(779)	04/09	NFSNET+CWI
c227 in 2^{773}+1	774(753)	00/11	CWI et al.

表四:針對 ECM 的紀錄

合成數	Log_2 p	時間(年/月)	作者
c214 in 10^{381}+1	222	06/08	Dodson
c180 in 3^{466}+1	219	05/04	Dodson
c311 in 10^{311}-1	212	05/09	Aoki et al.
c175 in 3^{533}-1	209	05/11	Kruppa
c187 in 2^{2034}+1	205	05/04	Dodson
c162 in 2^{905}+1	201	06/09	Dodson
c242 in 2^{1099}+1	197	05/10	Dodson
c162 in 10^{233}-1	194	05/02	Dodson

雖然 Aoki 博士該團隊成果豐碩，但在這三年內所使用的設備(四十部伺服器，其中包括三十二部 2U P4[2.53GHz]等級的伺服器及其相關設施)損害情形也是不輕，損害情形說明如下:

- 大約有15%硬碟壞掉，但其中的90%是藉由壞軌自動定位系統來修復；
- 二部電力系統損毀；
- 四個記憶模組；
- 8 CPUs有時候會產生不正確的結果；
- 二部CPU的風扇故障；
- 1 of 4 HUBs損毀；
- 1 motherboard損毀。

(2) **“The Outer Limits of RFID Security”**, 主講者為美國 RSA 實驗室的 Ari Juels 博士。

Juels 博士指出隨著科技的進步，條碼的使用率變的非常地快速。使得條碼面臨不足使用的時限早日來臨。最有效解決此條碼不足問題的方法，乃是使用 RFID。但若將 RFID 安全及原本的隱私性視為加解密協定設計的問題，是很冒險的。我們應該想要在值得相信的方法上，將 RFID 標籤不但可以拿來驗證他們自己之外，也想要它去保護它們所持有者的身份及個人資料。因此若能將密碼學的原理應用到百萬或者幾十億個設備的 RFID 標籤環境及其所能使用的技能協議上，所以可藉由現有工具的使用讓我們能使用更多的標籤電路系統來滿足我們的需要。證據指出，RFID 裝置不僅是資訊的傳播器，而且它的實体特徵及操作的環境都會給現有的安全及工具提升風險並帶來挑戰。此外，本演講亦就 RFID 的外部限制安全研究題目作一說明，其中包括：

- 旁邊通道：如果 RFID 標籤在其他層不安全，最好的合乎邏輯層的協議也是徒勞無功的。作為 RFID 隱私性的一項驚人疑慮是最近的研究顯示出已經無用的標籤可被偵測的且甚至是在他們的 RF 簽章上是可分類的。什麼將會是這樣的資訊頻道上的(包含負面和正面)衝擊？
- 轉換通道: RFID 標籤也許可被輕率地看作是感測器。他們將會增加跟感測器一樣的動作，收集及傳送他們週遭環境的資料。有什麼比對於 RFID 偷偷摸摸的傳送資料來講，會有更大的風險？
- 人類可植入式 RFID 晶片: 現在的社會中，外科手上術可植入的 RFID 標籤用於醫學的辨認及存取控制都是具商業化的價值。在這樣的”生物醫學”上，什麼是安全及隱私的涵意？
- 提升安全: 可以藉由一問一答或者彼此認證的方式來保障其隱私權。但在莫爾定律或是晶片價錢的考量暨在所擁有的安全性需求之下，大量的提供提升 RFID 安全性的需求？
- 可合作的架構: 在 RFID 的領域中，一個有多元能力裝置的範圍是可以操控的。而怎樣才能夠讓多資源的裝置透過審核及摸擬來支援少資源的裝置呢？

(3) **“Challenges for Trusted Computing”**主講人為德國 Ruhr University

Bochum 的 Ahmad-Reza Sadeghi 博士。

Sadeghi 博士首先提到信任計算團隊(Trusted Computing Group: TCG)是擁有大量資訊技術(IT)企業成員的聯盟，它們對常見的電腦建立了一系列保密方法與安全防護的規格。其規格涉及了信任平台模組 (Trus ted Platform Module: TPM)，信任平台模組為計算平台信賴度的基礎且提供能更進一步瞭解安全防護服務的密碼原件(cryptographic primitives)。信任計算(Trusted Computing: TC)是一種新興的技術，現在針對建立在信任計算上值得信賴的 IT 系統進行重要研究和工業目標的研究。但目前仍有以下五個問題需要解決，值得大家去深思的地方：

- 信任平台模組複雜度問題：信任平台模組的規格包含了大量的指令和參數，所以信任平台模組難以操作。就算完全的對信任平台模組必要功能進行分析，仍然可能有遺失的地方。
- 信任平台模組承諾問題：最近報導顯示大多數市場上的信任平台模組與信任計算團隊規格不同。一般來說，信任計算團隊之平台使用者沒有有效的方法去測試他們的信任平台模組可靠度或一致性。
- 維護問題：回復密封資料與在改變平台設定和信任平台模組的轉移都需要更令人滿意的方式。
- 信任基礎建設問題：實際上分散式信任計算需要一種更合適的基礎架構來掌握其可靠度。
- 證明問題：現行的信任計算團隊的證明並不令人滿意。由於它公開系統設定增加了隱私的重要性。一般的觀念用屬性為基礎的證明需要證實電腦平台是否必須用安全屬性來代替信任計算團隊建議的二進制數。

本次會議共有 15 個國家，投稿論文篇總數為 112 篇，每篇論文至少由三位國際知名的學者專家進行審查，若為議程委員則至少有五位審查者。經初步審查後再經過約一個月的公開討論，每位議程委員均有權對每篇論文的審查意見發表自己的看法。審查委員評審，因此所發表的論文皆極具重要的研究價值與影響力。因此最後共有 32 篇論文發表，並分為 12 個場次(session)。每個場次之主題與主持人分別為：

場次	主題	主持人	論文數
1	Side Channels I	Marc Joye	3
2	Low Resources	Elena Trichina	1
3	Hardware Attacks and Countermeasures I	Pierre-Alain Fouque	3
4	Special Purpose Hardware	Tetsuya Izu	2
5	Efficient Algorithms for Embedded Processors	Berk Sunar	3
6	Side Channels II	Erkay Savas	4
7	Hardware Attacks and Countermeasures II	Ingrid Verbauwhede	3
8	Efficient Hardware I	Akashi Satoh	3
9	Trusted Computing	Shiho Moriai	1
10	Side Channels III	Katsuyuki Okeya	3
11	Hardware Attacks and Countermeasures III	Frederic Valette	3
12	Efficient Hardware II	Francois-Xavier Standaert	3

以下摘錄重要論文所提出的論點與貢獻：

(1) Template Attacks in Principal Subspaces

Authors: C. Archambeau (University of Southampton), E. Peeters, F.-X. Standaert and J.-J. Quisquater (Universite Catholique de Louvain)

本論文提到在進行設計演算法實做時，side channel 攻擊是一個非常令人擔心的理論。隱密性的資訊被還原是植基於能量的消耗、電磁的放射或是任何會使資訊洩漏的方法。而樣板攻擊(template attack)為一種高斯雜訊模式是屬於機率式攻擊。所以使用最大相似性理論來讓我們可獲得每一個紀錄集合中的秘密。但在實務應用上，重要的是：1.如何選出測試的插入點 2.如何在這些點中選出最小距離 3.在攻擊中所插入的點有多少是需要的。到目前為止，只有啟發式方法提供相關的資訊。在本論文中，作者們提出使用樣板攻擊作為攻擊主要的痕跡子空間模式。這種新型的攻擊著重在所有實際採用的原則和自動的方式，此方法對 RC4 串流加密認證而言是具有攻擊性的。本論文分析 FPGA 實做 Rijndael 抵擋樣板攻擊的結果。大致上，針對類似區塊加密器的攻擊，樣板攻擊所需要加密訊息比最佳報告關連式攻擊至少五倍。

(2) Templates vs. Stochastic Methods

Authors: Benedikt Gierlichs (Katholieke Universiteit Leuven and Ruhr

University Bochum), Kerstin Lemke-Rust and Christof Paar (Ruhr University Bochum)

本論文提到樣板攻擊和隨機模式是從數據圖表表示方式並利用”a-priori”的知識來提供作為 side channel 破密分析的進階辦法。本論文的作者們使用兩個原始不同的微控制器與安裝之量測資料，針對樣板攻擊和隨機模式這兩種方法做有條理式比較。其主要的貢獻是面對決定性的參數紀錄各方面的效能數值。此外，最佳化的技術是用於在評估上述兩者方法。尤其是在較低的數值測量和有雜訊樣本的情況下，使用”T - Test”為基底的演算法當作選擇恰當的瞬間值可以被引導到有意義的效能增益。經過實驗之主要結果是假若從數據圖表表示中可獲得較多的有效樣本時，”T - Test” 基底樣板是可以當作一個主要選擇方法。然而，針對從數據圖表表示中只能獲得少許的有效樣本之情況，隨機模式卻是在數據圖表表示及分類上獲得較好的效能。

(3) Towards Security Limits of Side-Channel Attacks

Authors: Francois-Xavier Standaert, Eric Peeters (Universite Catholique de Louvain), Cedric Archambeau (University of Southampton) and Jean-Jacques Quisquater (Universite Catholique de Louvain)

在這論文中，作者們探討到近期所提出的從一個理論的觀點來研究完全地可觀察實現的架構，這模型允許量化實際有關的洩漏功能與安全和資訊理論矩陣的結合之影響。更明確的，我們應用我們的評估方法到一個示範的區塊加密上。首先我們考慮一個漢明權重漏損函數和評估這兩個共有的調查對策(即是干擾和遮蔽)的功效；然後，作者們又證明出這提案的方法能夠獲得可靠的重要直覺，例如：有關這些有效的對策；最後，作者們比對和瞭解 side-channel 攻擊來評估合併矩陣的需要性。

(4) HIGHT: A New Block Cipher Suitable for Low-Resource Device

Authors: Deukjo Hong (CIST), Jaechul Sung (University of Seoul), Seokhie Hong, Jongin Lim, Sangjin Lee (CIST), Bon-Seok Koo (NSRI), Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Jongsung Kim (CIST) and Seongtaek Chee (NRSI)

這份論文提出一個新的區塊加密法”HIGHT”，其使用 64 位元及 128 位元的區塊長度。它主要是提供一個低資源硬體實體，那是個美國海軍或是 RFID 利用特有的普遍存在使用電腦裝置感應器。”HIGHT”不僅構成的極簡單運算，還有足夠的安全性當一個加密系統。最後，作者們利用硬體來實做”HIGHT”， 在 0.25μm 面積下，只需要 3048 個閘極。

(5) Optically Enhanced Area-Locked Power Analysis

Authors: Sergei Skorobogatov (University of Cambridge Computer Laboratory)

這篇論文介紹精確的積體電路電力分析攻擊。透過雷射照亮一特定晶片表面區域，電流通過一單獨的電晶體造成可見電路的電力追蹤。光電效應把光轉變成電流，電流通過一個封閉的電晶體。以這種方法，單一電晶體對全面供應電流的貢獻可以由光線調整。與標準電力分析攻擊相比，半侵略性的鎖住位置技術提出不僅存取 Hamming 權重，而且對單一位元的資料處理。這項技術證明同時揭露在 SRAM 陣列 PIC16F84 微控制器和記憶體被存取位置與其內容。

(6) Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations

Authors: Stefan Mangard (Graz University of Technology) and Kai Schramm (Ruhr University Bochum)

這篇論文從討論 3 種不同的遮蔽硬體實現 AES 攻擊開始。這些討論導致推論出假訊號在隱蔽電路對遮蔽硬體實現上造成大量威脅。透過這個事實，作者們精確的指出遮蔽那一部分的 AES S-boxes 會引起假訊號導致單邊通道洩漏。這個分析揭露這些假訊號起因於改變 XOR 的特性。遮蔽乘數的邏輯柵。大多數近來的提議對於遮蔽 AES S-boxes，遮蔽乘數是建立區塊的基礎。緊接著展示單邊通道洩漏遮蔽乘數可以由 3‧n XOR 邏輯柵在單一 AES S-boxes 上的每一個 GF(2")乘數時序限制被防止。最後作者們也簡短地提出 2 種方法，來說明這些時序限制如何被實現。

(7) A Generalized Method of Differential Fault Attack Against AES Cryptosystem

Authors: Amir Moradi, Mahmoud Salmasizadeh and Mohammad T. Manzuri Shalmani (Sharif University of Technology, Tehran)

這篇論文描述兩種差動攻擊技術作用在 AES 上。作者們為缺陷事件提出兩個模型；一種是透過使用它們其中之一或者僅利用 6 份有缺陷的密文來找到所有 128 位元的金鑰。大概需要 1500 份有缺陷的密文去找到有其他錯誤模型的鑰匙。結合這些模型覆蓋所有錯誤在 AES-128 密碼系統的第 9 輪加密演算法。其主要優勢提出缺陷模型是可以在任何 AES 加密開始 (在第一回合之前 AddRoundKey 有主要鑰匙) 到 MixColumns 運行 9 回合中利用其錯誤模型來塑造。而這些模型覆蓋所有狀態，所以造成差異，起因於互異的明文或密文可以假定錯誤並和我們的模型一起塑造。這些模型覆蓋所有狀態會造成差異之起因於互異的明文或密文。因此可建立一個新穎的技術去密碼分析 AES 而不用單一通道資訊。這個方法和先前的主要差

別在於假定錯誤模型，而其所推薦的錯誤模型使用相當常見且普遍的假設給位置和發生錯誤的值。

(8) Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker

Authors: Sandeep Kumar, Christof Paar, Jan Pelzl (Ruhr University Bochum), Gerd Pfeiffer and Manfred Schimmler (Christian-Albrechts-University of Kiel)

本論文提到對稱式及非對稱式的密碼解譯器所需要的計算能力是相當苛求的。因為安全的需求，(尤其是針對密碼學所需的金鑰長度)大多的加解密演算法都是選來防止電腦被攻擊，但太多都不適用。唯一一個有辦法能掌握住的現在加密方式，是去建立一個特別目的的硬體。驗證那些機器以用來加解密分析的任務，保留住顯著改善了成本效益，以致於商業加密器的破解很容易達成。這貢獻呈現了設計及真實的 COPACOBANA 機器，這是用來最佳化的執行加密演算法及能用少於美金 10,000 就可實現。它將會被顯示出，靠著實際的演算法，這架構能只用數個序列就能勝過傳統的電腦。COPACOBANA 擁有著 120 低成本的 FPGA 且它有能力去執行 DES 的暴力金鑰搜尋，而僅僅只花少於九天的時間。作為一個真實世界的應用，我們的架構能被用來攻擊機器可讀取的旅遊文件(E 護照)。COPACOBANA 傾向於，但非必要被限制在解決跟加解密相關的問題。這硬體架構可適用於平行計算的問題，且有著較低的溝通需求。這硬体可用來如，攻擊橢圓曲線加密系統及破解因數。就算是研解最大長度的 RSA(大於等於 1024 位元)或是橢圓曲線(大於等於 160 位元的 ECC)都卻不可由 COPACOBANA 來完成，它可被用來分析較小長度的加解密系統，以提供可靠的 RSA 及 ECC 的安全評估。

(9) Implementing the Elliptic Curve Method of Factoring in Reconfigurable Hardware

Authors: Kris Gaj, Soonhak Kwon, Patrick Baier, Paul Kohlbrenner, Hoang Le, Mohammed Khaleeluddin and Ramakrishna Bachimanchi (George Mason University)

本論文主要是來描述及分析一個新奇的可攜性硬体架構，植基於橢圓曲線的因數分解法，其包括在於關係集合應用上的設計及最佳化的 number field sieve 步驟的集合。一個用較早的觀念證明設計已經被 Pelzl 及 Simka 等人分別在於執行的時間及空間域之中，都有被確實的證明確有改善。如今 ECM (橢圓曲線法) 架構已經轉向跨於三個不同家族的 FPGA 裝置，是為了選擇有最低的成本效益表現的家族。有著高度最佳化的軟体時間效益的，GMP-EC M，已經被實作出來了。本文的結論指出，與相同的微處理

機的產生器相比的話，低成本的 FPGA 家族，像是 Xilinx Spartan 3 提供最少一個程度(order)以上之成本效益的改善。

(10) Implementing Cryptographic Pairings on Smartcards

Authors: Michael Scott, Neil Costigan and Wesam Abdulwahab (Dublin City University)

本論文提到橢圓曲線上的 Pairings 方法是最近幾年來密碼學上新的安全應用領域成長最快的一種方法。尤其是用來實現 IBE (Identity-Based Encryption)。在這篇論文中描述各種類型的 Pairing 方法應用到的 32 位元的智慧卡上，PhilipsHiPerSmart™ 是 MIPS-32 型的 SmartMIPS™ 架構智慧卡。如 Tate pairing、Ate pairing 及 ηT pairing 等三種不同種類的 pairing 都有討論到，首先是標準的 Tate pairing 在一個非 supersingular 曲線 $E(F_p)$，第二是 Ate pairing，也是一個非 supersingular 曲線 $E(F_p)$，最後是 ηT pairing 是一個 supersingular 曲線 $E(F_{2^m})$。最後作者們將這些 pairing 方法建構在這初始簡潔的架構下，只需要 0.15 秒計算時間就能有效率的將其值計算出來。

(11) SPA-resistant Scalar Multiplication on Hyperelliptic Curve Cryptosystems Combining Divisor Decomposition Technique and Joint Regular Form

Authors: Toru Akishita, Masanobu Katagi and Izuru Kitamura (Sony Corporation)

本論文提到與橢圓曲線加密系統作一比較，HECC (Hyperelliptic Curve Cryptosystems)在安全上及效率上仍較有競爭力的。雖然最近使用 theta 因數來有效率提昇乘法技巧已經被提出來了。然而他們的應用卻是侷限在當 theta 因數是用來當基本點(觀點)的情況之下。因此在這篇論文，作者們提出有效率的且是安全的延展乘法以用來產生在 $E(F_{2^m})$ 下的 HECC。這個被提出的方法，是基於兩個新奇的技巧。一個是因數分解技巧，一般因數是由兩個 theta 因數因式分解而來；另一個是 joint regular form，用一對整數，這整數是可變的有效率且安全同步的由兩個 theta 因數產生的延展乘法。這兩個技巧的有效促成跟標準方法相比較的話，兩者大約是 19%的效率改善，而且可避免不用任何破壞性操作的較小力量分析。

(12) Fast Generation of Prime Numbers on Portable Devices: An Update

Authors: Marc Joye and Pascal Paillier (Gemalto)

本論文提到一質數的產生是藉由加解密系統的公鑰所產生的，例如像是 RSA 金鑰對的產生。出乎意料的是，儘管是在質數測試的數學研究的急劇衰減及加速加解密學明顯進展，質數產生演算法依然是幾乎不加以研

究。作者們提出簡單的技巧，在本質上可以改善所有的之前所提出的(質數)演算法，或是從它們的演算法作一個延伸。並在可攜式的裝置上，推導出快速的實作方式，如同是在內建在加解密系統處理器上的 smart card 一樣。這可允許 RSA 金鑰的嵌入式產生器可以呈現出一個非常吸引人的處理時間。因此本論文的動機是來幫助傳送這任務，從到目前為止的終端上，會常常發生的操作—產生質數—使得可攜式裝置可以呈現更加的安全、可信任、及對於可延展式網路分配協定的承諾，如同是電子現金或者是行動會議。

(13) A Proposition for Correlation Power Analysis Enhancement

Authors: Thanh-Ha Le, Jessy Cledi`ere, Cecile Canovas (CEA/LETI), Christine Serviere, Jean-Louis Lacoume (INPG/LIS) and Bruno Robisson (CEA/LETI)

本論文提到最常用來破解密文的方法是 SPA(Simple Power Attack)、DPA (Differential Power Attack) 和 CPA (Correlation Power Attack)等三種。而它們主要的不同點在於：第一是 DPA 攻擊是包含針對單一位元和多個位元兩種模式；其次是 DPA 攻擊在多個位元模式下可以再衍生出 PPA (Partitioning Power Attack)攻擊模式；最後，本論文是著重在 CPA 攻擊模式，經過本論文的分析後，不但發現此種攻擊其實就是一種特別的 PPA 攻擊，而且我們也提出利用限制正規方式來防止此種 CPA 的攻擊。

(14) High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching

Authors: Naofumi Homma and Sei Nagashima and Yuichi Imai and Takafumi Aoki (Tohoku University) and Akashi Satoh (IBM Research, Tokyo Research Laboratory)

本論文提到 Side-channel attack 已有 SPA 跟 DPA 兩種攻擊被提出。它們是利用分析波形可以降低雜訊並取回密文資訊。然而這些波形資料通常是有包含位置測定之置換錯誤。如今本文的作者們是先將波形 DFT（discrete Fourier transforms）後，藉著高分辨率（high-resolution）將可以估計訊號波形之間的置換，來使 Side attack 的精確度增加。進而推論以 POC-base 方法的優點比較普通的 DPA 對於實驗性的 DPA 和 DEMA 不利於 DES。

(15) Cache-Collision Timing Attacks Against AES

Authors: Joseph Bonneau (Stanford University) and Ilya Mironov (Microsoft Research)

本論文提到目前許多 Timing Attacks(時序攻擊)是不利於利用傳統的 table-driven 方式來產生 AES 密文。所以在本文中，作者們藉由加密器在

完成加密動作時，是利用一個有順序的計算過程，而產生的快取碰撞之特性。因此用一快取預測時序變動的簡化模式來定義一個通用的攻擊策略。故這個攻擊是可以應用在大部份的 AES 系統和計算平台上。同時在 Pentium3, Pentium 4 Xeon, UltraSPARC 3+ 平台上來實現此種攻擊進而用它來對抗 OpenSSL v.0.9.8。結果發現在最理想的狀態下只要取 2^{13} 個時間樣本，以重新獲得 128-bit AES key。所以防護 AES 的工作來對抗時序攻擊是富有挑戰性。只要一個小的補釘就可以有效減少特定攻擊下的弱點。

(16) Provably Secure S-Box Implementation Based on Fourier Transform

Authors: Sebastien Aumonier, Christophe Giraud and Emmanuel Prouff (Oberthur Card Systems)

本論文提到當加密演算法在嵌入裝置實現時，就必須能抵擋像 DPA 一樣的 Side Channel Attacks。一種常用於對稱式加密法保護方式是利用遮罩的技術來保護以達到對抗 DPA 的方法。然而要用遮罩技術來保護像 S-Box 等具有非線性的特性加密器是有困難的。如今我們利用傅利葉轉換(Fourier Transform)特性，提出在一種新的解決方案應用於每一對稱式加密法的 S-Box 上來抵擋 DPA 攻擊。並進一步地將上述方法用在 FOX 和 AES 的 S-Boxes 上，經過測試後之結果指出這種開發方式是最有效率的一個。

(17) Instruction Set Extensions for Efficient AES Implementation on 32-bit Processors

Authors: Stefan Tillich and Johann Groszschaedl (Graz University of Technology)

本論文提到加密演算法使用在公開的網際網路通信領域中是很基本的應用。但大多數的加密演算法對個人數位輔助器(PDAs)、手機及節點感應器之類似的設備造成很大的負擔，因為在處理加密演算法上會消耗大量資源(錢、電源)。而在本論文中提出一種利用指令集擴展處理對稱演算法來增加32位元處理器的效率。我們提出許多慣用指令來支援AES加密標準。使用 SPARC V8-compatible Leon2 嵌入處理器來當作平台，來評估AES的擴展對性能的影響與指令大小、矽的面積的關係。結果發現適度的提高矽的面積，AES性能差不多能提升十分之一，而指令尺寸明顯著降低且保留住操作的靈活度。同時作者們也證明其所提的方法在更多數量的處理器中實作上有非常好的效果，不輸前人所提出的加密處理器和指令表擴展的性能。

(18) NanoCMOS Molecular Realization of Rijndael

Authors: Massoud Masoumi, Farshid Raissi and Mahmoud Ahmadian (K. N. Toosi University of Technology, Tehran)

這篇論文是描寫一個高階加密標準演算法 Rijndael 在一項新奈米技術(CMOL)裡的實作。這技術是由傳統 CMOS 閘道陣列與高密度奈米導線網路所組成。Rijndael 的基本模組是由 CMOL 所建構出來的。這樣的技術在容錯程度、執行速度、體積與能量需求與傳統 COMS 比起來都有相當的優勢。

(19) Improving SHA-2 Hardware Implementations

Authors: Ricardo Chaves, Georgi Kuzmanov, Leonel Sousa and Stamatis Vassiliadis (TUDelft)

這篇論文是介紹一個改進 Sha-2 雜湊演算法的方法。這技術主要是由重新編排執行程序與硬體有效重複使用，並允許當需求空間縮小時，關鍵路徑也跟著減少。SHA256 與 SHA512 雜湊方程式已經完成建構且做 VIRTEX II Pro 雛型技術測試。實驗結果與商業中心做比較，建議需要改善 50%以上的 SHA256 技術以及 70%以上的 SHA512 雜湊函數。最後在 XC2VP30-7 FPGA 中，SHA256 和 SHA512 可在 755 和 1667 的晶片上之速度分別可達到 1.4 Gbit/s 與 1.8 Gbit/s。

(20) Offline Hardware/Software Authentication for Reconfigurable Platforms

Authors: Eric Simpson and Patrick Schaumont (Virginia Tech)

本論文中提到在許多現場可程式化邏輯閘陣列(FPGA)的規劃上都是利用第三方的智慧財產權(IP)驗證，但在離線的狀態下使用就有很多問題。所以在這篇論文設計一個離線的 IP 驗證模組，來提供 IP 模組與硬體平台間的相互驗證。再經過與利用額外的軟硬體驗證平台來驗證，發現這篇論文所提供的方法更簡單，更能與現有的 FPGA 安全特性結合。

(21) Why One Should Also Secure RSA Public Key Elements

Authors: Eric Brier, Benoit Chevallier-Mames, Mathieu Ciet and Christophe Clavier (Gemalto)

本論文提到眾所周知的方法即是一個惡意的敵人希望能透過引起加密運算中的一個錯誤機制來獲得機密訊息。在 Seifert 提出 RSA 簽章驗証過程中的錯誤誘導方法之後，作者們在這篇文章中，針對簽章的抵檔部份做一探討：首先是介紹第一個錯誤攻擊用於標準模式的 RSA。透過只修改一個公鑰，其私有指數能恢復。事實上，類似于 Seifert 的攻擊，本論文所提的攻擊只是做了模數修改的動作而已；其次是本論文所提的攻擊是假設在可忽略在被引起錯誤的影響下，那麼絕對沒有錯誤行為的知識對於要達

到完全回復私有指數是必須的。在另一種模式下，則是基于一個所謂"字典"的錯誤模型定義中，攻擊的效率被改進和錯誤的數量被戲劇性降低。本論文所提的攻擊都是非常實際。注意到這些攻擊是可以攻擊有決定性(例如，RSA-FDH)或隨機(例如，RSA-PFDH)填補空白等方式的簽章，除非簽章是具有隨機性恢復(例如 RSA-PSS)特徵的情況才可避免。最後關於這篇文章提出的結果使我們斷定保護 RSA 的公眾參數以防錯誤攻擊也是義務的。

(22) Power Attack on Small RSA Public Exponent

Authors: Pierre-Alain Fouque (ENS), Sebastien Kunz-Jacques (DCSSI), Gwenaelle Martinet (DCSSI), Frederic Muller (HSBC) and Frederic Valette (DGA/CELAR)

在這論文裡，作者們對 RSA 加密機制提出新的攻擊模式，即是當公開金鑰長度是短的時候，例如 3 或者 2 的 16 次方+1，並且使用隨機的標準指數。這個攻擊對於即使是使用盲目的訊息也能用。 從簡單能量分析攻擊(SPA)中，作者們針對當由過程中不連續的位元洩漏而回復私鑰的問題做一研究。發現像這樣的訊息也可能從使用滑動窗口的傳輸中被獲得，是無法防止 SPA 攻擊。

(23) Unified Point Addition Formulae and Side-Channel Attacks

Authors: Douglas Stebila and Nicolas Theriault (University of Waterloo)

本論文提到關於這把密鑰的訊息可能是在像能量消耗、計時，或者電磁散發等另類的觀測中恢復，並造成促進曲線點運算共同公式的近代發展，並將此種 Side-channel attack 成功地應用在的橢圓曲線密碼系統攻擊上。在本篇論文裡，作者們改進由 Walter 所提出的一種攻擊並且針對 Brier、Dechene 和 Joye 的統一公式做攻擊。最後，作者們也提出算術領域中要如何做，才可避免更多這類型的攻擊。

(24) Read-Proof Hardware from Protective Coatings

Authors: Pim Tuyls, Geert-Jan Schrijen, Boris Skoric, Jan van Geloven, Nynke Verhaegh and Rob Wolters (Philips Research Laboratories)

本論文提到重要的資訊總是利用密碼來達到保護的功效，但是攻擊者還是可以利用一些非法的方式取得資訊。而在本論文的作者們是想要利用 Algorithmic Tamper Proof (ATP) security 來達到防止攻擊者行為。其中一個必要元件是 Read-Proof Hardware，此元件可以防止侵略性攻擊。其架構有 hardware 和 cryptographic part。Hardware 有一個許多不可預測性的 protective coating，cryptographic part 則有 Fuzzy Extractor 根據特徵取得密碼。最後根據實驗結果，侵略性攻擊僅能取得極少量的資訊。

(25) Path Swapping Method to Improve DPA resistance of Quasi Delay Insensitive Asynchronous circuits

Authors: F. Bouesse, G. Sicard and M. Renaudin (TIMA Laboratory)

此論文在討論利用 Path Swapping (PS)方式來提高 QDI (Quasi Delay Insensitive)的安全性抵抗能量分析(Power Analysis)攻擊。當攻擊者利用能量分析攻擊失敗時，PS 利用不同步 QDI 區塊的邏輯對稱，特別是資料路徑重複性來產生電波使用。更進一步，藉由隨機交換資料路徑來平衡每個區域的電波特徵。為了達成這個目標，我們必須採取一個正規的 QDI 模型。首先，為了能夠使用路徑交換方法，這個正規模型必須讓設計者能正式地定義所有路徑的對稱性。再來提供模型化不同步 QDI 電路之電波特徵的可能性。最後，在這個模型上使用 DPA 讓使用者評估，在設計的初期階段，電流的敏感度與這個方法的適宜度有關。最後在 DES 加密處理器上的模擬證實這個方法能有效阻擋 PA 攻擊。

(26) Automated Design of Cryptographic Devices Resistant to Multiple Side-Channel Attacks

Authors: Konrad Kulikowski, Alexander Smirnov and Alexander Taubin (Boston University)

本論文提到平衡動態的雙向閘道與非對稱的電流已經在前文中敘述，若能實做成功便可有效的抵抗 side-channel 攻擊。儘管上述方法在安全應用上有優秀之處，由於缺乏電子設計自動化支持以及其設計方法論不標準，所以它們無法成為通用且主要的設計方法。所以在本文中，作者們設計一個依遵循 QDI circuit 和 HDL 的規格並對那些限制定義的非對稱微型管線綜合方法論。

(27) Superscalar Coprocessor for High-speed Curve-based Cryptography

Authors: Kazuo Sakiyama, Lejla Batina, Bart Preneel and Ingrid Verbauwhede (Katholieke Universiteit Leuven)

在本論文中提出超純量處理器應用於高速曲線基底的密碼學，是藉由利用動態指令間的平行處理(ILP)和處理大量的指令來加快純量積的運算。該系統架構設計成能讓處理器可以充分地利用超純量的特性。在本論文的實驗結果顯示植基於 GF(2^163)橢圓曲線密碼學(ECC)的純量積、植基於 GF(2^83)超橢圓曲線密碼學(HECC)和植基於 GF((2 ^ 83)^ 2)兩種所合 ECC 等三種情形的橢圓曲線密碼系統，與單一純量結構做一比較，發現大約可分別改善 1.8、2.7 和 2.5。因此可藉由利用曲線基底的密碼學平行處理來完成加速。此處理器可處理使用在全部欄位之運算像是乘法和加法

的單一指令。此外，此指令只允許單點乘/除運算。而且，最後作者們也提供在這三種曲線基底的密碼學間做一簡單的公平比較。

(28) Hardware/Software Co-Design of Elliptic Curve Cryptography on an 8051 Microcontroller

Authors: Manuel Koschuch, Joachim Lechner, Andreas Weitzer, Johann Groszschaedl, Alexander Szekely, Stefan Tillich and Johannes Wolkerstorfer (Graz University of Technology)

本論文提到目前像 8051 的 8 位元微控制器在嵌入式系統市場和智慧卡的工業仍保有相當大的佔有率，而 8 位元微控制器要應用在公鑰密碼方面時，常常無法滿足其基本需求。在這篇論文中，作者們提出一種能使橢圓曲線密碼學能在 8051 微控制器運算的硬體加速器執行。由於硬體加速器和外部 RAM 間轉換運算所花費的時間是造成系統性能發生瓶頸的重要原因。因此若由少量直接存取記憶體(DMA)整合之裝置可充分利用硬體加速器的性能。所以作者們設計允許在 12MHz 時脈頻率下 118mse 完成 GF(2^191)純量積的運算。在考慮到實行和硬體成本的情況下，本系統是優於前相似的 8 位元工作平台。

(29) FPGA Implementation of Point Multiplication on Koblitz Curves Using Kleinian Integers

Authors: V.S. Dimitrov (University of Calgary), K. Jarvinen (Helsinki University of Technology), M.J. Jacobson, Jr , W.F. Chan and Z. Huang (University of Calgary)

本論文提到在 Koblitz 曲線上使用以 $k=\sum \pm r^a(\tau-1)^b$ 和 $k=\sum \pm r^a(\tau-1)^b(\tau^2-\tau-1)^c$ 作為複合式基底擴展的點積運算演算法來說明。作者們證明在後者之型態項目的數量是屬於次線性且其長度為 K 位元，藉此可延伸證明前者型態在 Koblitz 曲線之點積演算法為次線性。此外，就前者態而言，作者們推測項目的數量也為次線性，並且提供數據來證明項目的數量是相當少且小於擴展的 τ-adic non-adjacent。最後作者們也提出一創新的 FPGA 來實現此演算法，並用實驗的數據來證明所提的方法是有效率的。

除了正式議程外，遵循 IACR 所贊助會議的傳統，本次會議亦安排一個 Rump Session，提供為入選論文發表者或會議期間之最新發現來發表他們的結果。而 Rump Session 的投影片或論文也將公布於 CHES2006 網站，發表論文題目與作者如下所示：

(1) Tamper-Resistant Mobile Terminal(Hitachi SDL)

Author: Camille Vuillaume

(2) New Block Cipher for Ultra-Compact Hardware
Authors: A. Satoh (EyeBeeM), K. Aoki (MiKaKa)

(3) Brand-New Hash Function
Author: A. Satoh (EyeBeeM)

(4) RFID Authentication: Minimizing Tag Computation
Author: Jin Kwak (Kyushu University)

(5) Design of Key-Sharing System Based on a Unique Device
Author: Kenji Imamoto(Kyushu University)

(6) An Algorithm for the Eta_T pairing Calculation in Characteristic Three and Its Hardware Implementation
Authors: Masaai Shirase et al, (University Tsukuba, Future University Hakodate)

(7) A Success of an Integer Factorization by Using a Special-purpose Hardware
Authors: Tetsuya Izu Jun Kogure Takeshi Shimoyama (FUJITSU)

(8) Cryptanalysis of Chinese S-Boxes & Japanese L-Boxes
Author: Alexander A. Veith (Inst. of Social and Economic Development)

(9) Update on COPACOBANA
Author: Christof Paar (University Bochum)

(10) Power Analysis Attacks - The Book
Author: Stefan Mangard (Graz University)

(11) Template Attacks - Practical Results
Author: Lex Schoonen Brightsight (TNO ITSEF)

(12) Protocol-Level DPA Countermeasures
Author: Paul Kocher (Cryptographic Research)

(13) A First-Order DPA Hack on AES in Counter Mode with Unknown Initial Counter
Author: Josh Jaffe (Cryptography Research)

(14) A New DFA Attack Against the AES Key Schedule David Peacham
Author: Byron Thomas (SiVenture)

(15) Simple Branch Prediction Attacks (SBPA) - New Results
Author: Shay Gueron (Haifa University)

(16) Modified Cache Side Channel Attacks
Author: Joe Bonneau (Stanford University)

六、心得及建議

藉由出席本次 CHES2006 會議的機會，不僅獲得目前國際密碼技術應用在硬體設備暨嵌入系統之發展現況與趨勢的相關資訊。而藉由「**Integer Factoring Utilizing PC Cluster**」專題演講，從中了解日本在因數分解方法的發展現況，以及要成為世界研發之佼佼者除了要花費許多時間及金錢之外，尚需要有一群志同道合的夥伴才能達到的。再者，於會議期間，訪談各國密碼專家與研究學者，了解各國資通安全相關政策的制訂依據與發展趨勢，並可以了解各國學者對一些國際標準的看法，以供我國在相關政策研擬之重要參考。

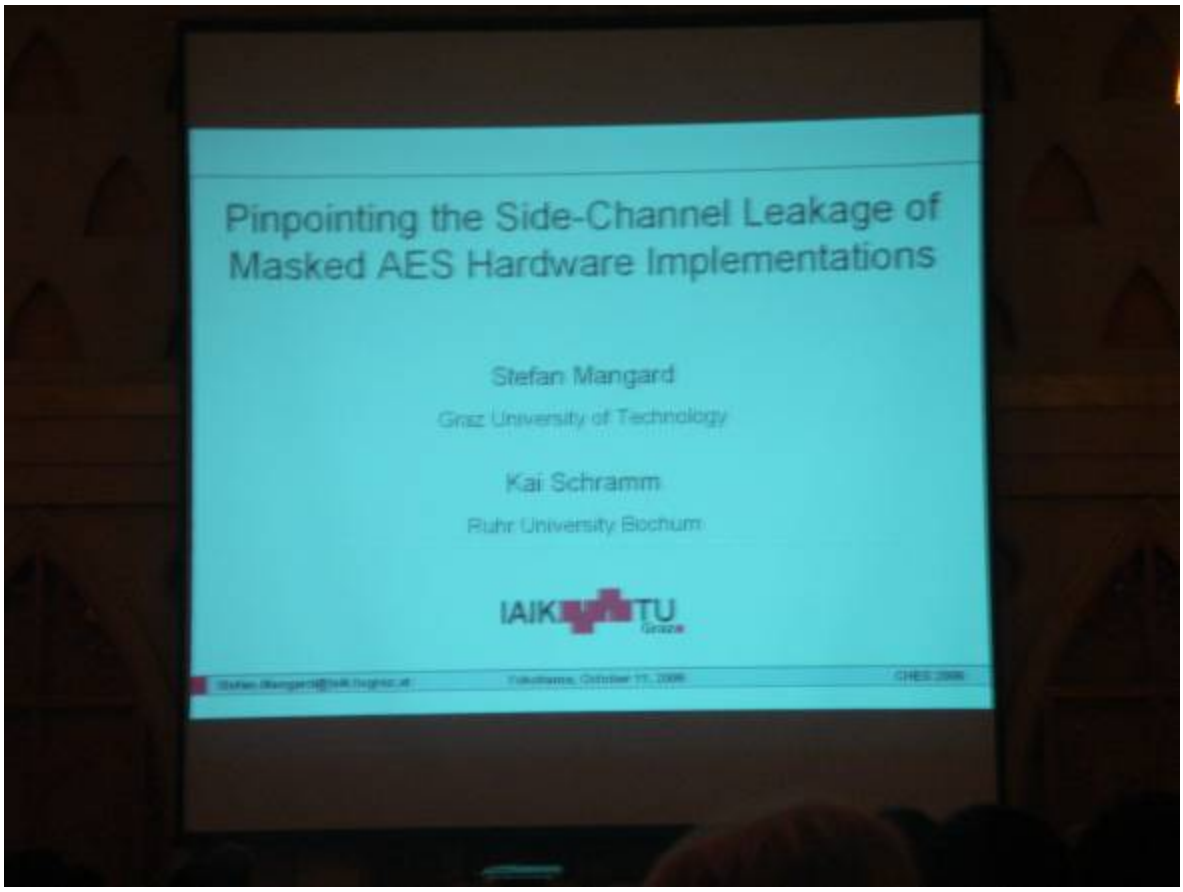
從本次 CHES2006 會議所接受的論文來看，發現該會議主要是針對當密碼技術應用在硬體設施時，可能因為其電磁輻射、計算時所散發出的熱量及計算所發的時間來探討秘密被洩露可能性及其相對的防護措施。尤其是針對目前最熱門的對稱式 AES 密碼系統中的 S-box、快取碰撞時間攻擊及對非對稱式的 RSA 密碼系統在使用較小的公開金鑰時的攻擊。而在此次會議接受的論文中，亞洲國家仍以日本及韓國為主，臺灣還是要再努力。不過這三天的會議中，發現我們可以發現以色列、日本、韓國、新加坡以及大陸等國家與會相當積極，藉由參加三大密碼會議以拓展研究視野，並感受世界一流學術研究氣氛。

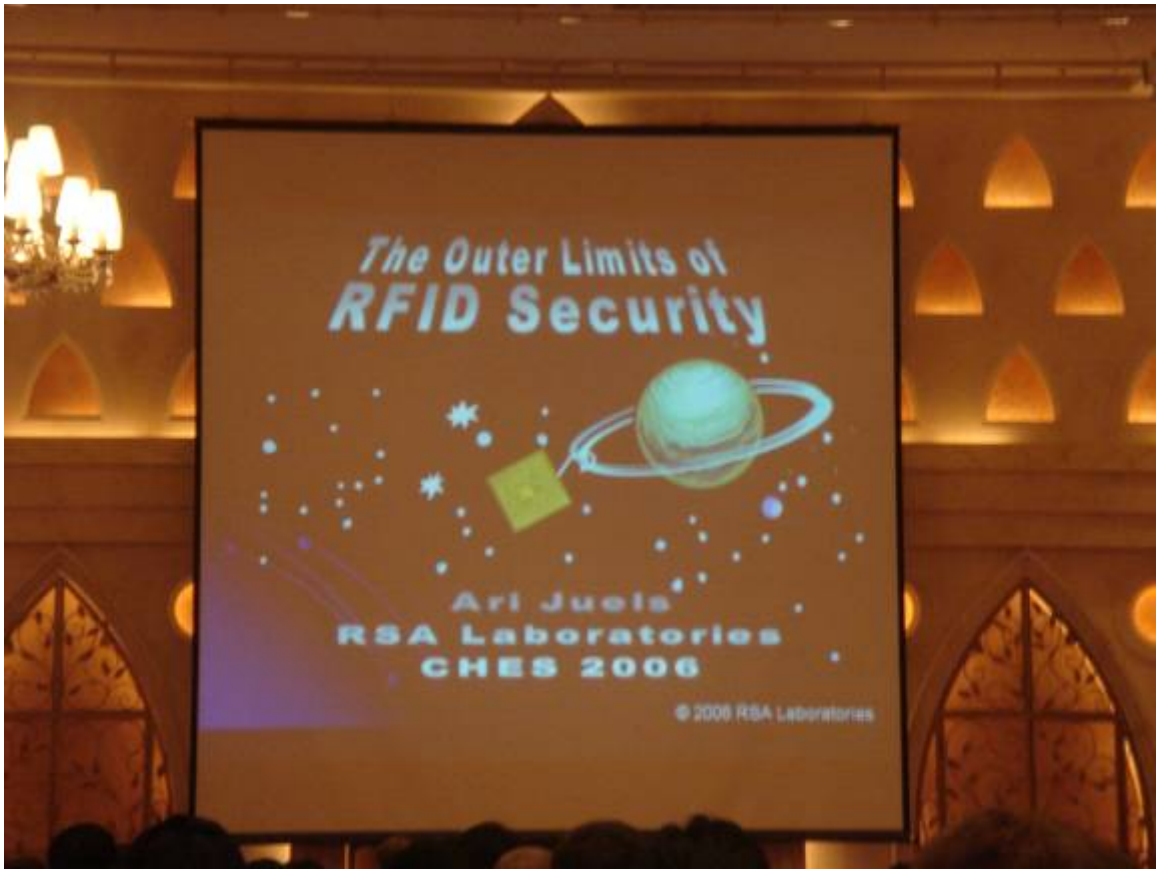
不過這些年來，政府也正在大力推動 E-Taiwan、M-Taiwan 及 IPv6 等與資訊相關基礎建設，高級或達世界水準的密碼學研究人才之需求更是急迫，或可建議各主管機構能多鼓勵與補助國內學術界(包括研究生)參與國際密碼研究協會所舉辦的各項大型國際密碼會議及講習會，相信定能為我國培育密碼學研究人才奠下契機。又，本次會議中發表論文仍是強調硬體及嵌入式系統模組驗證及安全防護（side channel），大會也特別安排邀請演講探討 RFID 相關安全議題。安全模組軟硬體驗證及 RFID 應用之相關安全標準，應持續觀察其發展趨勢。

（二）會議照片集錦


CHES
CHES


Integer Factoring Utilizing PC Cluster
Kazumaro Aoki
maro at isl.ntt.co.jp
NTT


Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations
Stefan Mangard
Graz University of Technology
Kai Schramm
Ruhr University Bochum
IAIK TU Graz


The Outer Limits of RFID Security
Ari Juels
RSA Laboratories
CHES 2006
© 2006 RSA Laboratories