2005－CSEC－31（5）
2005／12／9

Information Security Conference (ISC)/International Workshop for Applied PKI (IWAP)/Secure Mobile Ad-hoc Networks and Sensors (MADNES) 参加報告

長野 文昭 ∗　　上繁 義史 †　　櫻井 幸一 ‡

∗ 九州大学大学院システム情報科学府
812-8581 福岡市東区箱崎 6-10-1
{nagano,tatara}@itslab.csce.kyushu-u.ac.jp

†（財）九州システム情報技術研究所
814-0001 福岡市早良区百道浜 2-1-22 福岡 SRP センタービル 7 階
ueshige@isit.or.jp

‡ 九州大学大学院システム情報科学研究院
812-8581 福岡市東区箱崎 6-10-1
sakurai@csce.kyushu-u.ac.jp

あらまし

本稿では，今年 9 月 21 日から 23 日にシンガポールのセントーサにて開催された Information Security Conference (ISC)，International Workshop for Applied PKI (IWAP)，Secure Mobile Ad-hoc Networks and Sensors (MADNES) について，その概要を報告する．

A Report on Information Security Conference (ISC)/International Workshop for Applied PKI (IWAP)/Secure Mobile Ad-hoc Networks and Sensors (MADNES)

Fumiaki NAGANO∗　　Yoshifumi Ueshige†　　Kouichi SAKURAI†

∗ Graduate School of Information Science and Electrical Engineering, Kyushu University
6-10-1 Hakozaki, Higashiku Fukuoka, 812-8581
nagano@itslab.csce.kyushu-u.ac.jp

†Institute of Systems & Information Technologies/ KYUSHU
Fukuoka SRP Center Building 7F, 2-1-22,
Momochihama Sawara-ku, Fukuoka City 814-0001
ueshige@isit.or.jp

‡Faculty of Information Science and Electrical Engineering, Kyushu University
6-10-1 Hakozaki, Higashiku Fukuoka, 812-8581
sakurai@csce.kyushu-u.ac.jp

Abstract

This paper reports Information Security Conference (ISC), International Workshop for Applied PKI (IWAP), and Secure Mobile Ad-hoc Networks and Sensors (MADNES) held on September 20-23, 2005 at Sentosa, Singapore.

1. はじめに

本稿では，今年 9 月 21 日から 23 日にシンガポールのセントーサにて合同開催された Information Security Conference (ISC) [1]，International Workshop for Applied PKI (IWAP) [2]，Secure Mobile Ad-hoc Networks and Sensors (MADNES) [3] について，その概要を報告する．

2. ワークショップの概要

2.1 ISC'05

ISC は情報セキュリティの研究を目的とした会議として，1997 年に第一回会議が開催され本年で 8 回目となる．本会議は情報セキュリティの技術的なものの全てを扱う．Call For Paper によると，ISC'05 では以下のテーマについて扱う．

- Access Control
- Ad Hoc & Sensor Network Security
- Applied Cryptography
- Authentication and Non-repudiation
- Cryptographic Protocols
- Denial of Service
- E-Commerce Security
- Identity and Trust Management
- Information Hiding
- Insider Threats and Countermeasures
- Intrusion Detection & Prevention
- Network & Wireless Security
- Peer-to-Peer Security
- Privacy and Anonymity
- Security Analysis Methodologies
- Security in Software Outsourcing
- Systems and Data Security
- Ubiquitous Computing Security

昨年と比較して，Authentication and Non-repudiation と Systems and Data Security が追加された．今年の会議へは 271 件の投稿があり，このうち 38 件が採録された．このうち 5 件は student paper である．通常採用の発表には 30 分，student paper で採用された発表には 20 分が与えられ，論文は通常採用の論文は最大 15 ページ、student paper は 8 ページであった．Invited Talk は 2 件であった．昨年の会議は 106 件の投稿があり，そのうち 36 件が採用された．また、proceeding が LNCS3650 となっている。

また、来年は 8 月 30 日から 9 月 2 日まで、ギリシャの Samos での開催が決定している。詳細は、Web [4] にて確認できる。

2.2 IWAP'05

IWAP は PKI に焦点を当てた会議として，2001 年に第一回会議が開催され本年で 4 回目となる．Call For Paper によると，IWAP'05 では以下のテーマについて扱う．

- Authentication & Verification
- Bio-PKI & Mobile PKI
- Case Studies
- Certificate and its Revocation
- Cross Certification
- Design & Implementation
- Interoperability & Standards
- Key Management & Recovery
- Legal Issues, Policies & Regulations
- Modeling & Architecture
- Privilege Management Infrastructure
- Protocols & Applications
- Reliability & Fault-Tolerance
- Risk Management & Analysis
- Security Analysis & Testing
- Signature Validation
- Time Stamping
- Trust & Privacy

昨年と比較して，Trust & Privacy，Signature Validation Authentication and Non-repudiation ，Systems and Data Security などが追加された．今年の会議へは 43 件の投稿があり，このうち 15 件が採録された．通常採用の発表には 30 分が与えられ，論文は最大 18 ページであった．Invited Talk は 1 件であった．なお、Proceeding は出版されている。(4th International Workshop: IWAP 2005 Volume 128 Frontiers in Artificial Intelligence and Applications Edited by: J. Zhou, M.-C. Kang, F. Bao and H.-H. Pang September 2005, approx. 280 pp., hardcover ISBN: 1-58603-550-9 Price: US$108 / .90 / £62)

2.3 MADNES'05

MADNES は実際のアドホックネットワークでのモバイル技術に焦点をあてた会議であり，今年がはじめての開催となる．Call For Paper によると，MADNES'05 では以下のテーマについて扱う．

- Security and fault tolerance
- Privacy issues
- Security & privacy applications of mobile agents and intelligent autonomous systems
- Distributed denial of service attacks and defenses
- Mobile code security and verification
- Key management and trust infrastructures
- Security, privacy and efficiency trade-offs
- Secure distributed algorithms

- Secure & private protocols for dynamic group applications
- Secure location, discovery and authentication of neighbors
- Secure timing and synchronization
- Secure/private data collection and aggregation
- Secure self-configuration
- Secure routing
- Analysis and simulation of security and privacy properties
- Case Studies
- Energy efficient cryptography

12 件の発表があり，発表には 30 分が与えられ，論文は最大 16 ページであった．Keynote Speaker は 4 件であった．また、Proceeding が LNCS になる予定である。

3. 発表内容

3.1 ISC'05

A Dynamic Mechanism for Recovering from Buffer Overflow Attacks *Stelios Sidiroglou, Giannis Giovanidis, and Angelos D. Keromytis*

スタック，ヒープのオーバフロー，アンダーフローを検知するための仕組みの提案．攻撃が起こった際にも，関数をトランザクションのようにアボート可能であるという仮定を起き，効率的な仕組みを提案した．Apache 利用したベンチマークの結果，full-protection モードでは 20%のコストアップ，selective protection モードでは 1.2%のコストアップとなった．

Time-based Release of Confidential Information in Hierarchical Settings *D. Nali, C. Adams, and A. Miri*

指定された時間まで情報の機密性を確保するための暗号化法に関する提案．具体的には，BBGs Methodology+NAM-HIBE による方法 HTIP を提案．これは，木構造による ID の設定をし，生成のタイミングに独立な鍵情報を生成するというもの．効率について EGG fsHIBE と比較して，Setup では提案法が高コストとなるが，暗号化復号化はほぼ同等であった．

Trust Engineering: From Requirements to System Design and Maintenance – A Working National Lottery System Experience *Elisavet Konstantinou, Vasiliki Liagkou, Paul Spirakis, Yannis Stamatiou, and Moti Yung*

情報レベルで「信頼」を確立するための方法についての発表．システムの初期化，信頼の要件と詳細化，信頼設計のコンポーネント，Trust Component の構築とテスト，オペレーションとメンテナンスによりシステムの生成する。実用的な信頼を確立するためにシステムを，

科学的健全性 ⊂ 実装健全性 ⊂ 内部操作健全性 ⊂ 外部から可視な操作の健全性のような包含関係を伴うレイヤに分けるアーキテクチャを提案している

Certificateless Public Key Encryption without Pairing *Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo*

公開鍵暗号と ID ベース暗号を組み合わせることにより証明書なし公開鍵暗号（CLPKE）を構成することができるという方式の提案．本発表ではペアリングの計算を省くことにより効率的な CLPKE を構築する方法を提案している．提案法は CDH 問題に基づく安全性が保証されている．

Tracing-by-Linking Group Signatures *Victor K. Wei*

Tracing-by-Linking グループ署名の提案．この署名方式は、もし，グループメンバーが一度しか署名をしない場合は，署名者の匿名性は変更できないが，グループメンバーが二度署名をした場合は，トレースが可能となるという特徴を持つ．

Keynote: Security in Sensor Webs *Doug Tygar*

Sensor Web や RFID は将来もっと普及すると考えられる．その際ブロードキャスト認証が重要になってくる．そこで，ブロードキャスト認証の方式として利用する TESLA の発表．TESLA は時間同期と MAC を利用してブロードキャスト認証を行う．また，Polution Attack に対応するためには Merkle Hash Trees と accumulator を利用してパケットロスも許容した認証方式を利用する．

Building a Cryptovirus Using Microsoft's Cryptographic API *Adam L. Young*

マイクロソフトの API を利用して cryptovirus を作成する方法の実装の論文．crpytovirus とは，感染先のデータを公開鍵暗号方式を利用して暗号化し，それを人質として感染先のホストに脅威をあたえるウイルスの事．実装の結果，8 個の API のタイプと 72 行の ANSI C により実現することができた．

Integrity Improvements to an RFID Privacy Protec-

tion Protocol for Anti-Counterfeiting *Xiaolan Zhang and Brian King*

RFID プロトコルにおける完全性モデルの提案．2003 年 Juels らによって提案された Squezling Euros protocol を用いて検証を行い、既存の方式より優れたプロトコルを提案することができた．

3.2 IWAP'05

PKI Challenges: An Industry Analysis *Geraint Price*

PKI の実証実験について特徴の解析，安全性の問題点についての指摘を行った．技術面では、PMI のサポートは鍵ではあるが PMI をアウトソーシングする困難さはサービスに影響する、という問題点と、PKI は再利用が重要と考えられているが実際には可能ではないという問題点がある。法的側面，規約作りの面では、ディジタル署名に法的根拠が必要である。管理，運営の面では、失効モデルの選択が最大の論点となる．また、技術，法整備，管理・運営，経済，利用者の視点から PKI のもつ課題とそれに対する発表者の意見として、PKI はセキュリティサービスとして販売されており，ビジネスプロセスへのサポートを含むべきである、リスクマネジメントはクライアントが実行できる、というものがあった。

On Automatically Detecting Malicious Imposter Emails *Erhan J. Kartaltepe and Shouhuai Xu*

悪意ある詐称者からの E-mail を阻止するための Multi-server Authentication User DEtection(MAUDE）の提案．MAUDE はメールサーバから送信されるメールについて受信側のメールサーバに接続されている MAUDE と共に検証する．環境（CPU，接続されているネットワークの通信速度など）の異なるシステムについて実証実験を行い，Incoming の遅延，MAUDE の検出精度についてのデータが紹介された．

A Generic Protocol for Controlling Access to Mobile Services *Shuhong Wang, Yingjiu Li, Bo Zhu, and Nan Hu*

モバイルサービスのアクセスをコントロールするための一般的なプロトコルの提案．本方式は，暗号アルゴリズム，サービスモデルに依存しないという特徴を持つ．また，さまざまなモバイルサービスへの攻撃に対しても耐性を持つ．楕円カーブデジタル署名アルゴリズムに基づくプロトコルの実装オプションについても提案した．

On Universal Composable Security of Time-Stamping Protocols *Toshihiko Matsuo and Shin'ichiro Matsuo*

タイムスタンプの偽造による Back-dating Attack, Forward-dating Attack を防止するためのプロトコルの提案．タイムスタンプのセキュリティ要件を定義して Universal Composability Framework を導入するメリットを紹介し，タイムスタンプの機能の 3 つのケース（Cannetti の方法，ディジタル署名ベース，トークン発行）を紹介している，

A Lightweight Delegated Privileges Revocation Scheme Based on Coding *M. Francisca Hinarejos and Jordi Forne*

検証者は証明書のチェーンに属するそれぞれの証明書を検証する必要があることを問題点としている．PMI における権限の委譲モデルでは権限のチェーン長が限られることと，Attribute 証明書の失効状況を検証できないことが問題となる．これを改善するためにコードワードを用いて Attribute 証明書の識別情報を符号化する方法を提案している，具体的には，トップの AttributeAuthority からツリー構造に基づいてパスの情報に当たるコードワードを生成している．

Generic Fair Non-Repudiation Protocols with Transparent Off-line TTP *Guilin Wang*

Fair exchange protocol におけるディジタルアイテムの生成，交換，検証における否認防止についての提案．このプロトコルでは TTP 無し，オンライン TTP，オフライン TTP によるプロトコルが考えられる．どの署名アルゴリズムでも適用可能な Generic Construction, Tranparent TTP, Offline TTP について提案し，Fairness, Timeliness，High Performance を実現している．

3.3 MADNES'05

A Novel Pairwise Key Predistribution scheme for Ubiquitous Sensor Network *Mohammed Sadi*, Jong Sou Park, Dong Seong Kim, Young Deog Song*

センサーネットワークにおいて，ノード間で鍵を交換しておく方式についての提案．既存の方式と比較し利点があることを示した．具体的には，既存の方式より少量のメモリですみ，またオーバーヘッドも削減することができた．

Towards a Standards-based Authorization Framework for Mobile Agents *Guillermo Navarro*, Joan*

Borrell

モバイルエージェント XMAS（XML-based Mobile Agent Authorization System を用いた RBAC ポリシー，権限譲渡を含んだ認証フレームワークに関する発表．モバイルエージェントはコードのハッシュ値にて識別される．XMAS の構成要素として以下の 5 つの要素がある．

- Role Manager
- Authorization Manager
- Resource Controller
- Delegation Assertion Repository Manager
- Authorization Decision Engine

Keynote: Enhancing Intrusion Detection in Future Wireless and Mobile Networks *Evangelos Kranakis*

本講義では，ワイヤレスセキュリティについてとワイヤレスセキュリティIDS についての講演があった．ワイヤレスの難しさとして，リソースが限られているという点があり，ワイヤレスネットワークの難しさとしては，信頼できるサーバ確立の難しさがあげられる．それらの難しさより，いろいろな脅威が存在するがそれらの対策を行なう必要がある．その対策案として Radio Frequency Fingerprinting を提案．これは，機器によって異なる Radio Frequency を DNA としてセキュリティに利用する．これにより一意に機器を識別することができるようになるというものである。

Non-Group Cellular Automata based One Time Password Authentication Scheme in Wireless Networks *Jun-Cheol Jeon, Kee-Won Kim, Kee-Young Yoo*

計算能力の低いプロセッサでも処理可能な Cellular Automata based One Time Password についてのプロトコルの提案．提案方式の最適な運用のためのパラメータの設定，パスワード類推攻撃，リプレイ攻撃等の攻撃に対する安全性を議論している．

Kyenote: Efficient Cryptographic Techniques for Mobile Ad-Hoc Networks *Yuliang Zheng*

本講演ではモバイルレベルのネットワークにおける暗号がもつべき特徴，実際のアルゴリズムに関する紹介が行われた．近年，ユビキタスネットワークにおけるハードウェア的な制約（バッテリ，CPU の計算能力，メモリの容量）を考慮して安全性を確保するためのシステムの研究が進んでいる．これらのシステムはより高いフレキシビリティを持つ必要がある．

最適な暗号アルゴリズムを考えるとき，セキュリティのゴールを満足するのに過不足のない方式を選ぶことと，効率的なアルゴリズム（高速，最小のデータ展開，小さいコードサイズ，短い鍵，実装の容易さ）を選ぶことが必要である．

Identity Base の手法（ペアリング技術）は PKI を単純化することが可能だが，標準化や実装経験，新しい要件（Trust な鍵生成，秘密鍵の配布等）などの課題を持つ．鍵事前配布の方式は高速で計算可能で情報理論的安全性が保証されているが，標準化や新しい要件の追加などの課題を持つ．署名暗号化（Signcryption）は高速演算が可能で実装が容易，多数のバリエーションを持ち PKI と等価であるという特徴を持つ．楕円曲線を用いたときの実行時間を DSS+ElGamal の方法と比較すると，Signcryption は DSS+El Gamal の約 60 %の時間で計算される事が分かる．秘密鍵暗号のアルゴリズムについては，ブロック暗号は AES が勧告されている．またストリーム暗号では理想的な候補はないが ECRYPT が有望である．ハッシュについては SHA-1 の問題が浮上しており，新しい主導的なハッシュアルゴリズムが必要となっている．MAC を適用する試みがある．MAC には情報理論的安全性が保証されており，高速に計算できる良い候補が多数ある．

ARMS: An Authenticated Routing Message in Sensor Networks *Yoon-Hwa Choi, Suk-Bok Lee*

センサーノードのルーティングメッセージのブロードキャスト認証のプロトコルの提案．本方式は，ノード間の時間同期が必要でなく，遅延もない．また，パケットロスに対しても耐性がある．

4. 終わりに

本稿では，Information Security Conference (ISC), International Workshop for Applied PKI (IWAP), Secure Mobile Ad-hoc Networks and Sensors (MADNES) の開催概要について報告した．

文　献

[1] The 8th information security conference (isc'05) 20-23 september 2005 singapore. http://isc05.i2r.a-star.edu.sg/.

[2] The 4th international workshop for applied pki (iwap'05) 21-23 september 2005 singapore. http://iwap05.i2r.a-star.edu.sg/.

[3] Secure mobile ad-hoc networks and sensors (madnes) 20-22 september 2005 singapore. http://www.sait.fsu.edu/conferences/2005/madnes/home.shtml.

[4] Information security conference. http://www.icsd.aegean.gr/ISC06/s_index.htm.