Vol.2010-CSEC-50 No.34
2010/7/2

ACM WISEC 2010 会議 参加報告

江藤文治[†]　　櫻井幸一[†,††]

2010 年 3 月 22 日から 3 月 24 日の間､米国ニュージャージー州ホボケン(Hoboken)で開催された第 3 回 WISEC 2010 (Third ACM Conference on Wireless Network Security に関して報告する。

ACM WISEC 2010 report

Fumiharu Etoh[†]　and　Kouichi Sakurai[†,††]

This paper reports on the Third ACM Conference on Wireless Network Security (Wisec '10), held on March 22 to March 24, 2010, at Stevens Institute of Technology, Hoboken, NJ, U.S.A.

1. はじめに

本稿では､2010 年 3 月 22 日から同月 24 日の間に米国ニュージャージー州ホボケン(Hoboken)で開催された第 3 回 ACM WISEC 2010 (Third ACM Conference on Wireless Network Security (Wisec '10)) [1]に関して報告する。

2. ACM WISEC 2010 の概要

ACM Conference on Wireless Network Security（以下、WISECとする）はACM SIGSAC (Special Interest Group on Security, Audit and Control)が主催する年次コンファレンスのひとつである。その名の通り無線ネットワークにおけるセキュリティに関する話題を取扱い、無線ネットワークへの攻撃とその防御方法の研究を目的としている。
尚、WISECは以下の3つの組織によって開催される毎年恒例の合同会議である。

- ESAS：European Workshop on the Security of Ad Hoc and Sensor Networks
- SASN：ACM Workshop on the Security of Ad Hoc and Sensor Networks
- WiSe：ACM Workshop on Wireless Security

2008 年に初めて開催され、2010 年の開催で 3 回目である。2008 年は米国バージニア州アレクサンドリア市、2009 年はスイスのチューリッヒ州にて開催され、今年度は米国ニュージャージー州ホボケン市のスティーブンス工科大学（Stevens Institute of Technology）にて開催された。本会議は月曜日から水曜日の 3 日間の開催である。併設ワークショップの開催は行われていないが、初日と二日目の昼食後に、ポスターセッションの時間が設けられている。

表1 に、今年度を含む過去3カ年（2008年から2010年）の投稿論文数、採択論文数、採択率[2]を示す。まだ2008から2010年の3カ年だけであるが、毎年100件前後の投稿があり、2009年は107件（WISECの過去最高）で、2010年はそれに次ぐ99件の投稿があり、この分野における関心の高さが伺われる。

表 1　ACM WISES 2008～2010 の投稿採択状況

	投稿数	採択数	採択率
WISEC 2008	**96**	**26**	**27.0%**
WISEC 2009	**107**	**28**	**26.2%**
WISEC 2010	**99**	**21**	**21.2%**

[†] （財）九州先端科学技術研究所
Institute of Systems, Information Technologies and Nanotechnologies (ISIT)
[††] 九州大学大学院システム情報科学研究院　情報学部門（数理情報）
Department of Informatics, Kyushu University

2010年の会議では、欧米及びアジア各国からの99件の論文の投稿のうち、21件の論文が採択された。内、9件がfull paper、12件がshort paperとしての採択である。論文採択率は21.2%で、過去2年と比較しても下がる傾向にあり、低い採択率であると言える。

WISEC2010 本会議の会議録は、会場では冊子版のみが配布された(CD-ROM 版の配布は無かった)。例年と同様に WISEC2010 本会議の会議録は ACM デジタルライブラリ[a]により参照可能である。

WISEC2010 のプログラムは、6 つの研究発表セッション、2 つのキーノートセッション及び 2 つのポスターセッションから構成された。2008 年度のプログラムでは、”**RFID Security and Privacy: Long-term Research or Short-term Tinkering?”** [3]のテーマでパネルディスカッションが行われているが、昨年と同様に今年は設定されなかった。

WISEC2010 は 6 つのセッションにより構成された。各セッションには、ローマ数字で 1 から 6 が割り当てられており、セッション内容を意味するような名称は特に明記されていない。しかし、過去 2 年はセッション毎に名称が以下のように明記されている。2008 年度[4]及び 2009 年度[5]におけるセッション名称を以下に示す。尚、セッション名の後の“(2)”は 2 つのセッションから構成されていたことを示す。

2008 年度：
- Authentication in Wireless Networks
- Device Identification and Privacy
- Sensor Network Security
- Key Management
- RFID and Embedded Sensors
- Multi-hop Applications and Mal-packets
- Defensive Techniques

2009 年度：
- Sensor Network Security (2)
- RFID security
- Attacks
- Ad Hoc Networks
- WiFi and Mesh Network Security
- Jamming/Anti-jamming
- Secure Localization and Time synchronization

a) ACM Digital Library, http://portal.acm. org/dl.cfm

WISEC2010 の 6 つのセッションの概要、又は、傾向を表すために、各セッションの発表論文の内容、及び、過去 2 年のキーワードを参考に、筆者が今年度のセッションに名称をつけるとすると、以下のようになる。
- Attacks
- Defensive Techniques
- RFID security and Ad Hoc Networks
- Device Identification and Privacy
- Sensor Network Security
- Secure Localization

2009 年度に 2 件が発表された WiFi のように、スポット的な分野は見受けられない。発表論文名に”RFID”を含む論文が 4 件、”Sensor Network”を含む論文が 3 件あり、センサーネットワーク関連の関心が高いように思われる。

WISEC2010 ではキーノートセッションとして 2 のセッションが設けられ、キーノートが 2 件企画された。これらのタイトル及び概要を次に示す。行頭の記号 K-#は基調講演を表す。

K-1. Providing security with insecure systems (Andrew Odlyzko, Professor in the School of Mathematics at the University of Minnesota)

Odlyzko教授はルーセントテクノロジーの出身。新しい脆弱性の発見とセキュリティ漏洩の報道により、政府・産業界ではICTシステムの設計及び運用の再検討を呼び掛けている、とセキュリティの弱さを指摘する。これに対し、到達不能なレベルを求めるのではなく、完全なセキュリティは無いことを認識し、システム設計原理を変えることと過去から学ぶことを提案する。異質なエレメントによるメッシュ構造やソフトウェアの難読化等、基礎設計哲学に反しているがうまく動作した例のように、システム設計哲学を変えて、ICTの進化に対して受容可能なセキュリティを実現しよう、呼び掛けていた。

K-2. To Be Announced (Philip R. Zimmermann, the creator of Pretty Good Privacy)

Zimmermann氏は、PGP(Pretty Good Privacy)の開発者である。特に講演タイトルはなく、前半は携帯電話上でのPGPや鍵交換方式に関する内容で、後半は聴講者とのQ&Aの対話形式であった。Facebookに関する情報保護レベルの質問に対し、「データマイニングの力は想像されているよりも強い。複数の情報から特定の情報が見えることがある。利便性は認めるが、セキュリティの面から私は使わない。」との回答があり、セキュリティに対する意識の強さが感じられた。

WISEC2010の参加者は、欧州、北米、アジアから全体で70名程であった。
6つの発表セッションにおける聴講者は各々40～65名程度であった。また、日本からの参加者は4名であった。

3. ポスターセッション

WISEC2010 では前述の通り、初日と二日目の昼食後に、ポスターセッションの時間が設けられた。本会議会場及びその隣室において、以下の 14 件の展示と希望者への説明、デモ及び質疑応答が行われた。尚、行頭の記号 P-#はポスターを表す。

P-1. Testbed Design For Facilitating Simultaneous WiMAX Experiments (Rutgers University)
P-2. Regulating Applications in Ad hoc networks using Law Governed Interaction (Rutgers University)
P-3. Detecting Wormholes in Wireless Sensor Networks ACM Conference on Wireless Network Security (WiSec) (Athens Information Tech.)
P-4. Enhancing Unlinkability on IPv6 Receiver Address with Distributed Relay Service (Takushoku University)
P-5. Secret Handshakes or Oh, It's You Again! (Stevens Institute of Technology)
P-6. Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks (UCL Crypto Group)
P-7. The Indiana Jones Attack: An Initial Evaluation of RSS Authentication (Rutgers University)
P-8. An Efficient Security Framework for Mobile WiMAX (Rutgers University)
P-9. appoint – A Distributed Privacy-Preserving iPhone Application (Stevens Institute of Technology)
P-10. Strongly Secure Pairing of Wireless Devices within Physical Proximity (Rutgers University)
P-11. Mobile Ad-hoc Routing Secruity (Stevens Institute of Technology)
P-12. Demo:Rapid prototyping of a "Denial of Service Radio" using the GENI OCRP Kit (Rutgers University)
P-13. Discovering Wormhole Attacks in Delay Tolerant Networks via Forbidden Topology Structure Identification (Stevens Institute of Technology)
P-14. Coping with Frequency-based Attacks to Secure Distributed Data Storage in Wireless Networks (Stevens Institute of Technology)

開催場所であるスティーブンス工科大学(Stevens Institute of Technology から 4 件、同じくニュージャージー州のラトガース大学(Rutgers University)から 5 件が展示された。日本からは 1 件(P-4)が出展されていた。

4. WISEC2010 本会議における発表

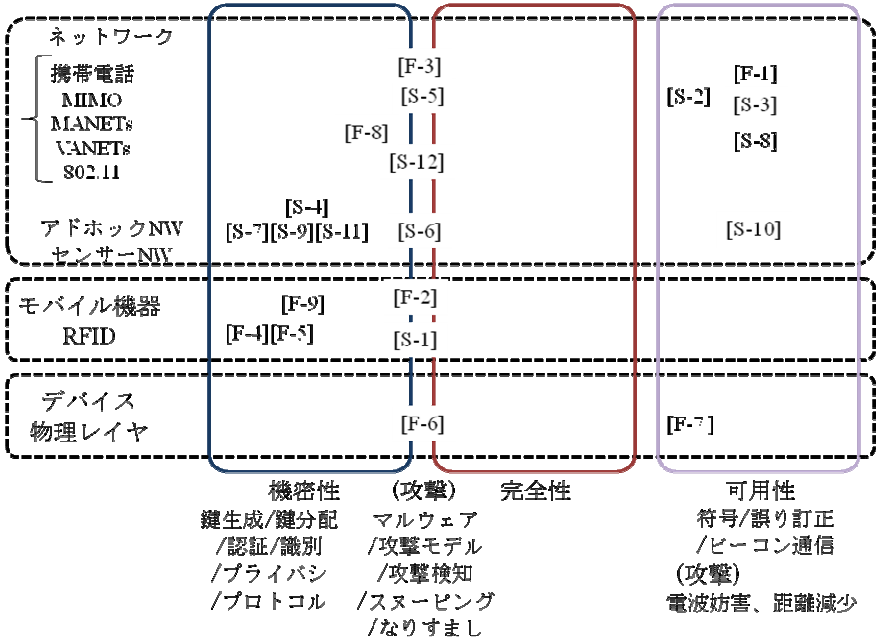
WISEC2010 発表された full paper 及び short paper を以下に示す。
行頭の記号 F-#は full paper, S-#は short paper を表す。(発表順)

F-1. Timing-based Localization of In-Band Wormhole Tunnels in MANETs
Jinsub Kim (Cornell University) et al.
S-1. RFID Survivability Quantification and Attack Modeling
Yanjun Zuo (University of North Dakota)
S-2. Subverting MIMO Wireless Systems by Jamming the Channel Estimation Procedure
Rob aMiller, Wade Trappe (Rutgers University)
F-2. Preventing Multi-query Attack in Location-based Services
Nilothpal Talukder (Purdue University) et al.
F-3. pBMDS: A Behavior-based Malware Detection System for Cellphone Devices
Liang Xie (The Pennsylvania State University) et al.
S-3. Efficient Compromising Resilient Authentication Schemes for Large Scale Wireless Sensor Networks
Hao Chen (East China Normal University)
F-4. Low-Cost Untraceable Authentication Protocols for RFID
Yong Ki Lee (University of California, Los Angeles) et al.
F-5. A Secure and Scalable Identification for Hash-based RFID Systems Using Updatable Pre-computation
Yasunobu Nohara (Kyushu University), Sozo Inoue (Kyushu Institute of Technology)
S-4. On the Tradeoff between Trust and Privacy in Wireless Ad Hoc Networks
Maxim Raya, Reza Shokri, Jean-Pierre Hubaux (EPFL)
S-5. Automating the Injection of Believable Decoys to Detect Snooping
Brian M.Bowen, Vasileios P.Kemerlis et al. (Columbia University)
F-6. Attacks on Physical-layer Identification
Boris Danev, Heinrich Luecken, Srdjan Capkun (ETH Zurich) et al.
S-6. Zeroing-In on Network Metric Minima for Sink Location Determination
Zhenhua Liu, Wenyuan Xu (University of South Carolina)
S-7. Privacy-Preserving Computation of Benchmarks on Item-Level Data Using RFID
Florian Kerschbaum, Nina Oertel et al. (SAP Research)
S-8. On the Efficiency of Secure Beaconing in VANETs
ZElmar Schoch (Ulm University), Frank Kargl (University of Twente)
F-7. Effectiveness of Distance-decreasing Attacks Against Impulse Radio Ranging
Manuel Flury, Marcin Poturalski et al. (EPFL)

Vol.2010-CSEC-50 No.34
2010/7/2

F-8. honeyM: A Framework for Implementing Virtual Honeyclients for Mobile Devices
TJ O'Connor, Ben Sangster (United States Military Academy)
S-9. Secret Keys from Entangled Sensor Motes: Implementation and Analysis
Matthias Wilhelm, Ivan Martinovic, Jens B. Schmitt (TU Kaiserslautern)
S-10. Efficient Code Diversification for Network Reprogramming in Sensor Networks
Qijun Gu (Texas State University-San Marcos)
F-9. Mobile User Location-specific Encryption (MULE): Using Your Office as Your Password
Ahren Studer, Adrian Perrig (Carnegie Melon University)
S-11. Secure Walking GPS: A Secure Localization and Key Distribution Scheme for Wireless Sensor Networks
Qi Mi, John A. Stankovic (University of Vierginia), et al.
S-12. On the Reliability of Wireless Fingerprinting using Clock Skews
Chrisil Arackaparambil, Sergey Bratus et al. (Dartmouth College)

図 1　WISEC 2010 における発表論文の分類



採択率21.2%で選ばれた各論文は、いずれも興味深い内容であった。研究の対象分野と情報セキュリティの3要件(技術要素)でマッピングすると図1のように分類できる。図1に示すように取り扱われるトピックは無線ネットワークの多岐にわたっていることが判る。特に、RFIDやモバイル機器、及び、各種無線ネットワークにおける機密性保持と攻撃に関する研究が多いと言える。本稿では、無線ネットワーク運用におけるセキュリティの実現に関し、実用性と有効性の観点から筆者が興味を持った4つの論文を紹介する。

F-3. pBMDS: A Behavior-based Malware Detection System for Cellphone Devices
[Liang Xie (The Pennsylvania State University) et al.]

携帯電話(特に、スマートフォン)上のイベント動作からユーザ操作による動作かマルウェア処理による動作かを識別し、確率的アプローチによりマルウェア検出を実現する研究である。検出の仕組みは、training phase と real-time detection phase の 2 つのフェーズで構成される。training phase では、まず行動解析(Behavior Analyzer)として、該携帯電話端末の正規ユーザのキー操作や LCD 画面操作によって記録されるイベントログから時間情報を利用して入力イベントと出力イベントのペアを作成し、その操作を Behavior Graph 呼ぶ OS のシステムコール(ex. open(), socket() etc.)のプロセス動作のデータに変換する。さらに、学習機能(Learning Engine)として、上述の Behavior Graph における測定により、ユーザ特有の操作パターン(キー入力間隔、キー入力時間、スクリーンタッチの強さ)とプロセス状態遷移の間の関係を抽出し、ユーザプロファイルとしてカーネル部に保存する。real-time detection phase では、Systemcall Monitor により、プロセス動作をリアルタイムでモニタし、Malware Detection Engine がユーザプロファイルと検出ポリシーに従い、該動作がユーザ操作による動作かマルウェア処理による動作かを判断する。尚、Malware Detection Engine においては、限られた数のモニタ情報でプロセス状態と関連付ける為に"隠れマルコフモデル(HMM:Hidden Markov Model)"を導入しており、数多くのシステムコール、及び、プロセス状態とその複雑性の軽減を図っている。

評価実験においては、一般的なユーザ操作ではなく、特定の個人ユーザ操作を学習して実験を実施している。SMS/MMS//Email/Bluetooth の各サービスにおいて、マルウェア検出率は 92.1~96.4%であり、誤検出も False Positive が 2.8~6.3%、False Negative が 0.6~1.6%と報告されている。また、将来的には、上述の"隠れマルコフモデル"を学習機能(Learning Engine)におけるユーザ特有の操作パターンの学習やユーザプロファイル生成へ利用することにより、より精巧なマルウェアへの対応も検討されている。

iPhone をはじめとするスマートフォンの利用は、各キャリアからのスマートフォン端末の提供と SIM ロックの解除の可能性等により、日本国内においても拡大が見込まれている。その拡大に伴い、新たなセキュリティインシデントの発生も予測される。

よって、高検出率で、特定 OS に依存せず、比較的軽い検出方法とする本研究は、実運用において有益な内容であると考える。

(1) **F-4. Low-Cost Untraceable Authentication Protocols for RFID**

[Yong Ki Lee (University of California, Los Angeles) et al.]

講演者のLeeらは、RFIDネットワークにおけるトラッキング攻撃(tracking attack)に関し、 EC-RAC(Elliptic Curve Based Randomized Access Control)プロトコルの研究[b]を行っている。既存のEC-RACプロトコルに対して中間者攻撃(man-in-middle the middle attack)に対する耐性を有する3つの改良プロトコルを提案している。New ID-Transfer SchemeはRFIDタグIDをサーバへ通知するプロトコルであるID-Transfer Schemeの改良である。認証時にサーバで生成された乱数に対して楕円曲線を利用する非線形処理を実施する(non-linearity by reusing EC operatoinsと表現)。具体的には、サーバで生成された乱数をそのままID情報の計算に使用するのではなく、サーバで生成した乱数を用いてタグのx座標にマッピングする計算により得た値を、ID情報の計算に利用している。サーバとタグの双方でこの計算を実施することにより、暗号処理の為のハードウェア追加をすることなく、中間者攻撃への耐性を実現している。さらに、上述のID-Transer Schemeとパスワードを転送するPwd-Transfer Schemeの機能を同時に提供するID&Pwd-Transfer Schemeに関し、1stと2ndの2つのプロトコルを提案している。いずれのプロトコルにおいても上述の認証時にサーバで生成された乱数に対して楕円曲線を利用する非線形処理を実施している。しかし、1stプロトコルにおいては、IDとPwdの双方に対して共通の乱数を使用していることから、脆弱性(privacy wide-weak)を指摘している。2ndプロトコルにおいては、Randomized Schnorr Protocol[c]を応用して、2つの乱数を使用することにより耐性を高めて(privacy wide-strong)いる。また、特定タグのサーチプロトコルや、提案プロトコルの実現可能性を示すためのRFID Processor Architectureを提案している。提案アーキテクチャにおける評価実験の結果、既存研究より24%の性能向上と消費電力の大幅な削減が報告されている。RFIDの利用用途は今後も拡大が予想されており、セキュアかつ低コストの運用技術として、有益な研究であると考える。

(2) **F-5. A Secure and Scalable Identification for Hash-based RFID Systems Using**

[Yasunobu Nohara (Kyushu University), Sozo Inoue (Kyusyu Institute of Technology)**]**

RFID (Radie Frequency Identification)を用いた通信の RFID からサーバへの送信内容の盗聴によるロケーションプライバシ問題に関する、防御技術であるハッシュチェーン方式における高速識別方法、d-left ハッシュテーブルの研究である。RFID の出力情報関し、ID 情報に対する位置情報を時系列でモニタすることにより、その ID を有する RFID の位置追跡が可能である。該 RFID の ID が個人を識別可能の場合、個人の位置を追跡するロケーションプライバシ問題となる。RFID が出力する情報がどの ID の情報であるかを識別不可能とするリンク不能性を実現する方法として、ハッシュチェーン方式が提案されている。これは、サーバ側において、2 つの異なる一方向性ハッシュ関数を用いて、どの RFID の何番目の出力であるかを示す出力対象情報を事前に計算してハッシュテーブルで管理しておく。各 RFID が出力時に同様に算出して付与した出力情報を、サーバが事前計算したハッシュテーブルを検索することにより、出力元の RFID の ID を識別する方法である。しかし、既存方式においては、計算量が多い(逐次検索)、メモリ量が多い(Look Up Table 検索)、ハッシュテーブルの動的更新が困難等の問題があり、大規模システムへの適用が困難であるという。これを解決するため、d 個のハッシュ関数を用いて予め RFID の出力対象情報を d-left ハッシュテーブルで管理することにより、検索時間と計算量を削減する。さらに、使用済みの順番までの出力対象情報を削除し、その分だけ新たな出力対象情報を追加することで、出力対象情報のハッシュテーブルを動的更新してメモリ量を制限する、というセキュアかつスケーラブルで動的な RFID のハッシュチェーン方式を提案している。実験結果である他の方式と比較では、使用メモリ量、計算速度、及び、SRI(Successful Rate of Identification)のいずれにおいても、高性能の結果が報告されている。ユビキタス分野において RFID は有望かつ低コストのデバイスと予想され、実用的な面で有益な研究であると考える。

(3) **F-9. Mobile User Location-specific Encryption (MULE): Using Your Office as Your Password**

[Ahren Studer, Adrian Perrig (Carnegie Melon University)**]**

極秘ファイルを参照する場所をオフィス等の信頼できる場所に限定されることを想定し、暗号化時は、信頼できる場所に設置される TLD(Trusted Location Device)において生成される乱数(location-specific information)を用いて、それを受信した PC 上で対象の極秘ファイルを暗号化する。復号時は、同じく信頼できる場所において TLD が生成する上述の乱数を用いて、それを受信した PC 上で復号する。但し、信頼できる場所以外で極秘ファイルにアクセスする場合には、位置情報に依存しない第二のパスワードを入力することにより、極秘ファイルの参照を許容する、MULE(Mobile User Location-specific Encryption)に関する研究である。TLD は MULE において、鍵情報を生成し、信頼できる場所内の PC に送信する機能を有する機器であり、信頼できる場所内に設置されることを前提としている。さらに、TLD が鍵を分配する対象は、予めホワイトリストに登録された ID を所有する PC(又は、ブラックリストに登録されている ID を所有しない PC)を前提としている。極秘ファイルは、予め TLD 内のホワイト

b) Y. K. Lee, L. Batina, and I. Verbauwhede. Untraceable RFID Atuthetication Ptrotocols: Revising of EC-RAC. In IEEE International Conference on RFID, pages 178-185. IEEE, 2009

c) J.Bringer, H. Chabannel, and T. Icart. Cryptanalysis of EC-RAC, a RFID Identification Protocol. In International Conference on Cryptology and Network Security-CANS'08, Lecture Notes in Computer Science. Springer-Verlag 2008.

リストに登録されている信頼される場所に位置する PC において新規作成し、TLD より受信する位置情報に基づく暗号鍵によって暗号化されており、信頼される場所内において予め登録された PC のみが TLD から復号鍵を受信することにより復号することが可能となる。会社のような同一の組織内においては、異なる場所であっても同一のポリシーの下で信頼できる場所に設置される TLD の管理下においては、極秘ファイルの暗号化と復号が可能となる。攻撃者が TLD を設置された信頼できる場所から成りすまし攻撃を試みても、ホワイトリスト上の登録 ID の確認により鍵情報を入手することはできず、万一、PC が盗難にあった場合は、ホワイトリストから ID を削除することにより、情報漏洩の防止が可能となる。また、評価実験において、復号鍵の配信と復号に要する時間は 5 秒未満と報告されている。
極秘ファイルのような重要ファイルへのアクセスするビジネス環境に着目し、信頼できる場所内において、ID 登録された PC と TLD 間での認証情報及び鍵情報を自動的に送受信することにより、ユーザ負担なくセキュアな極秘ファイルアクセス環境を実現している点が実用面で有益な研究であると考える。
尚、本論文は、WISEC 2010 の最優秀アワードを受賞している。

5. WISEC2011 について

来春に開催される WISEC 2011 は、ドイツでの開催予定と会議終了時にアナウンスされた。
会期、会議場及び研究発表講演を行うための論文の投稿〆切等の募集要項の詳細については、未だ公表されていない(2010 年 5 月末日現在)。

6. おわりに

本稿では、2010 年 3 月 22 日から同月 24 日の間に米国ニュージャージー州ホボケンで開催された第 3 回 ACM WISEC 2010 (Third ACM Conference on Wireless Network Security (Wisec '10))に関して、その概要を紹介した。さらに、WISEC 2010 本会議で発表された無線ネットワークセキュリティに関するいくつかの研究について概要を示した。

参考文献

1 Third ACM Conference on Wireless Network Security (Wisec '10).
http://www.sigsac.org/wisec/WiSec2010/
2 WISEC: Papers Acceptance Statistics.
http://portal.acm.org/browse_dl.cfm?linked=1&part=series&idx=SERIES11635&coll=portal&dl=ACM
3 2008 ACM Conference on Wireless Network Security (WiSec'08) PANEL:
http://sconce.ics.uci.edu/wisec08-rfid-panel/
4 First ACM Conference on Wireless Network Security (WiSec'08)
http://www.sigsac.org/wisec/WiSec2008/program.html
5 Second ACM Conference on Wireless Network Security (WiSec'09)
http://www.sigsac.org/wisec/WiSec2009/program.html