Vol.2013-CSEC-63 No.5
2013/12/9

SecureComm2013・ATIS2013 参加報告

梶原　直也[1,3,a)]　松本　晋一[1,3,b)]　堀　良彰[2,3,c)]　櫻井　幸一[1,3,d)]

概要：本稿では，2013 年 9 月 25 から 27 日にオーストラリアのシドニー，Aerial UTS Function Centre にて開催された 9th International Conference on Security and Privacy in Communication Networks(SecureComm2013)，並びに同月 26 日に開催された併設ワークショップ 4th International Workshop on Applications and Techniques in Information Security(ATIS2013) に関し，その概要を報告する．

1. はじめに

本稿では，2013 年 9 月 25 から 27 日にオーストラリアのシドニー，Aerial UTS Function Centre にて開催された 9th International Conference on Security and Privacy in Communication Networks(SecureComm2013)[1]，並びに同月 26 日に開催された併設ワークショップ 4th International Workshop on Applications and Techniques in Information Security(ATIS2013)[2] に関して，その概要を報告する．

2. SecureComm2013 概要

9th International Conference on Security and Privacy in Communication Networks(以下，SecureComm2013 とする) は，EAI(European Alliance for Innovation) の主催による，ネットワークセキュリティに関する年次国際会議であり，今回の開催が 9 回目となる．スポンサーは，NSW Trade&Investment，テクニカルスポンサーが CREATE-NET，Charles Sturt University である．また，Excellence of Research in Australia (ERA) は，2010 年に本会議を最高評価である'A' にランク付けしている．

今年度は，オーストラリア，シドニーの Aerial UTS Function Centre にて 9 月 25 日から 27 日の三日間に渡り開催された．参加者は 30 人から 40 人程で，日本からの参加者は 2 名であった．発表会場の様子を写した写真を図 1 に示す．

図 1　SecureComm2013 会場の様子

2.1 運営体制

SecureComm2013 は，以下のメンバーにより運営された．

- General Chair
  Tanveer A Zia(Charles Sturt University, Australia)
  Albert Y Zomaya(University of Sydney, Australia)
- TPC Chairs
  Vijay Varadharajan(Macquarie University, Australia)
  Morley Mao(University of Michigan, USA)
- Local Chairs
  Junbin Gao(Charles Sturt University, Australia)
  Adel Al-Jumaily(University of Technology Sydney, Australia)
  Maumita Bhattacharya(Charles Sturt University, Australia)
- Publicity Chairs
  Salil Kanhere(University of New South Wales, Australia)
  Jianming Yong(University of Southern Queensland, Australia)

[1] 九州大学, Kyushu University
[2] 佐賀大学, Saga University
[3] （財）九州先端科学技術研究所, Institute of Systems, Information Technologies and Nanotechnologies (ISIT)
[a)] kajiwara@itslab.inf.kyushu-u.ac.jp
[b)] smatsumoto@isit.or.jp
[c)] horiyo@cc.saga-u.ac.jp
[d)] sakurai@csce.kyushu-u.ac.jp

Weili Han(Fudan University, China)

- Publication Chairs
  Aldar Chan Chun Fai(Institute for Infocomm Research (I2R), Singapore)
  Quazi Mamun(Charles Sturt University, Australia)
- Workshops Chairs
  Javed Taheri(University of Sydney, Australia)
  Md Rafiqul Islam(Charles Sturt University, Australia)
- Sponsorship Chair
  Sabih-ur Rehman(Charles Sturt University, Australia)
- Web Chair
  Saman Shafigh(Charles Sturt University, Australia)
- Conference Manager
  Erica Polini(European Alliance for Innovation (EAI))

2.2 Call for Papers

SecureComm2013 の Call for Papers では，セキュア通信とネットワークに関するあらゆる分野の研究を募集している．特に関係のあるトピックとして以下のものを挙げている．

- 有線，無線，ハイブリッド，センサ，アドホックネットワークにおけるセキュリティ&プライバシ
- ネットワーク侵入検知，侵入防止
- ファイアウォール，パケットフィルタ
- マルウェア
- ボットネット
- DDoS 攻撃
- 通信プライバシ，匿名性
- ネットワークフォレンジクス
- 公開鍵基盤，鍵管理
- セキュアルーティング
- ネーミング／アドレッシング
- ネットワーク管理
- ユビキタス・コンピューティングにおけるセキュリティ&プライバシ
- 先端技術に関するセキュリティ&プライバシ：VoIP，P2P，オーバーレイ・ネットワーク

2.3 投稿論文

General chair と TCP chair によると，SecureComm2013 には，15 を超える数の国から 70 本の論文が投稿され，その内採択されたのは 21 本であったと公表された．そのため，SecureComm2013 における採択率は 30%になる．採択された論文の発表者の国別内訳を見てみると，中国から 6 件，オーストラリアが 5 件，アメリカから 4 件と続き，ギリシャ，ベルギー，ニュージーランド，イギリス，フランスから 1 件ずつであった．また，発表は大学からのものがほとんどであった．

2.4 SecureComm2013 の構成

講演は 3 日間の会期においてシングルトラックで構成された．計 20 件の論文発表に加えて，4 件の基調講演が行われた．

表 1 に本年度を含めた過去 3 回のセッション構成を示す．各行の数字は，セッション内の発表論文件数を示す．

表 1 SecureComm におけるセッション変遷

2013 年度 [3]	
Security & Privacy in Mobile, Sensor, and Ad Hoc Networks	3
Malware, botnets, and Distributed Denial of Service	3
Security for emerging technologies: VoIP, peer-to-peer, and Cloud Computing	3
Encryption and Key Management	3
Security in Software and Machine Learning	2
Network and System Security Model	3
Security and Privacy in Pervasive and Ubiquitous Computing	3
2012 年度 [4]	
Crypto and Electronic Money	4
Wireless Security	3
Web Security	3
Intrusion Detection and Monitoring	4
Anonymity and Privacy	4
Miscellaneous	3
2011 年度 [5]	
Network Intrusion Detection	3
Anonymity and Privacy	6
Wireless Security	5
Systems Security	3
DNS and Routing Security	3
Key Management	3

過去 3 年間のセッション構成を比較すると，今年度は全体の発表数は若干減少していたが，モバイルセキュリティやクラウドセキュリティに関するセッションが新たに作成されており，それらの分野へ研究者の関心が集まっているように感じた．また，2011 年，2012 年とプライバシに関するセッション 1 つであったのが，今年度は関連する分野毎に 2 つのセッションに分けられており，サイバーセキュリティにおける様々な分野でプライバシ問題が拡大していると読み取れる．個別の発表に注目すると，2011 年，2012 年と 0 本であったスマートフォン関連の発表件数が今年度は 3 本に増えており，変化が顕著であった．

3. ATIS2013 概要

4th International Workshop on Applications and Tech-

図 2　ATIS2013 会場の様子

niques in Information Security(以下，ATIS2013 とする)[2] は，SecureComm2013 に併設された情報セキュリティに関する国際ワークショップである．2010 年から開催されており，今回の開催が 4 回目となる．

今年度は，SecureComm2013 会期中である 9 月 26 日に開催され，6 件の論文発表と 1 件の招待講演が行われた．発表会場の様子を写した写真を図 2 に示す．

3.1　運営体制

ATIS2013 は，以下のメンバーにより運営された．

- Steering Chair
  Lynn Batten(Deakin University, Australia)
  Jemal Abawajy(Deakin University, Australia)
- General Chair
  Rafiqul Islam(Charles Sturt University, Australia)
- Workshop Secretary
  Judy Chow(Deakin University, Australia)

3.2　Call for Papers

ATIS2013 の Call for Paper では，情報セキュリティに関するあらゆる分野の研究を募集している．特に関係のあるトピックとして以下のものを挙げている．

- アクセスコントロール
- アンチウイルス
- 認証
- クラウドセキュリティ
- コンピュータ・デジタルフォレンジクス
- データベースセキュリティ
- 分散システムセキュリティ
- 暗号セキュリティ
- 侵入検知
- マルウェア
- ネットワークセキュリティ
- OS セキュリティ
- プライバシ保護
- リスク評価
- モバイルセキュリティ
- スマートフォンセキュリティ

4.　SecureComm2013 における発表紹介

4.1　基調講演

SecureComm2013 において開催された基調講演の概略について以下に示す．

(1) Challenges in Cyber Security
[Mike Holm (Operations Manager, AusCERT)]
講演では，講演者が所属する AusCERT の例を元にして，近年のサイバーセキュリティに関する事例を紹介した．AusCERT はオーストラリアにおける CERT(Computer Emergency Response Team) で，アジア／太平洋地域における最大の CERT になる．講演者は，健康や産業の制御システムのような新しい産業へサイバー攻撃の標的が向く前に，それらの脅威を認知させていくことが重要であるとしている．今回の講演では，今年度初めに AusCERT が調査した Internet Census 2012 について紹介し，Carna Botnet から得られたデータが明らかにした，世界中に 120 万の脆弱性を持った端末が存在していた事例について語った．

(2) Data breach disclosure and other dinner party games
[James Turner (Chair AISA Advocacy Group)]
講演では，オーストラリアの IT セキュリティ産業に重大な影響を与えた出来事を紹介した．これらの出来事は技術的な分野から心理学，社会学の分野にまで及ぶ．講演者は，これらの分野を調査し，学術的な組織が産業に十分な援護をどのように行えるかについて議論した．

(3) Know thy Enemy
[Mark Goudie (Regional Manager ? Investigations, Dell SecureWorks)]
講演者は，近年の攻撃者を 3 つの異なるタイプに分類できるとした．攻撃者達はもはやステレオタイプな時間を持て余した若者だけではなく，サイバー攻撃者，社会的，政治的な主張を目的とした hacktivist，国から後援されているグループの混合になっている．そして，これらのグループはそれぞれ異なったツールや技術，そして目標を持っている．そのため，これらのグループの振る舞いや対象を知ることは，次の犠牲者になる可能性を最小限にするための準備となるだろう，と著者は述べた．また，講演では，これらのグループの動機についても議論し，それぞれのグループが狙う組織やデータ財産の種類も含めて彼らの技術にどのような影響を与えるか考察した．

(4) Cyber Security: from Bio-cryptography to Intrusion Detection

[Jiankun Hu (Australian Defence Force Academy, UNSW)]
この講演では，サイバーセキュリティは暗号に関する分野だという認識が存在しており，多くの資源が暗号分野に投入されてきたと述べられた．しかし，講演者は，サイバーセキュリティというのは「セキュリティの強さは最も弱い部分に依存する」というシステムコンセプトのことであり，ハッキングは必ずしも暗号に関係しないとしている．例えば，DoS 攻撃は暗号と何ら関係がない．残念なことに，近年そのような攻撃はより増加している．講演者は，そのような攻撃に対抗するための，アクセスコントロールと異常侵入検知に用いられるバイオ暗号学の最新の発展について紹介した．

4.2 SecureComm2013 における発表

SecureComm2013 における発表論文は 21 件であった．予稿集は USB メモリに収容された状態で配布された．以下に，各発表のタイトルを示す．

Session I: Security & Privacy in Mobile, Sensor, and Ad Hoc Networks

- [1a]Anomaly Detection in Beacon-Enabled IEEE 802.15.4 Wireless Sensor Networks [Eirini Karapistoli and Anastasios A. Economides(Department of Information Systems, University of Macedonia)]
- [1b]Secure and Verifiable Top-k Query in Two-tiered Sensor Networks [Ting Zhou, Yaping Lin, Wei Zhang, Sheng Xiao and Jinguo Li(Dept. of Information Science and Engineering, Hunan University)]
- [1c]CamTalk: A Bidirectional Light Communications Framework for Secure Communications On Smartphones [Mengjun Xie, Liang Hao, Kenji Yoshigoe and Jiang Bian(University of Arkansas at Little Rock, University of Arkansas for Medical Sciences)]

Session II: Malware, botnets, and Distributed Denial of Service

- [2a]Botnet Triple-Channel Model: Towards Resilient and Efficient Bidirectional Communication Botnets [Cui Xiang, Fang Binxing, Shi Jinqiao and Liu Chaoge(Institute of Computing Technology, Chinese Academy of Sciences, Beijing University of Posts and Telecommunications, Institute of Information Engineering, Chinese Academy of Sciences)]
- [2b]Contrasting Permission Patterns between Clean and Malicious Android Applications [Veelasha Moonsamy, Jia Rong, Shaowu Liu, Gang Li and Lynn Batten(School of Information Technology, Deakin University)]
- [2c]DroidAPIMiner: Mining API-Level Features for Robust Malware Detection in Android [Yousra Aafer, Wenliang Du and Heng Yin(Dept. of Electrical Engineering & Computer Science, Syracuse University)]

Session III: Security for emerging technologies: VoIP, peer-to-peer, and Cloud Computing

- [3a]Disabling a Computer by Exploiting Softphone Vulnerabilities: Threat and Mitigation [Ryan Farley and Xinyuan Wang(Department of Computer Science, George Mason University)]
- [3b]VCCBox: Practical Confinement of Untrusted Software in Virtual Cloud Computing [Jun Jiang, Meining Nie, Purui Su and Dengguo Feng(Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences)]
- [3c]Integrated Security Architecture for Virtual Machines [Vijay Varadharajan and Udaya Tupakula(Information and Networked Systems Security Research Faculty of Science, Macquarie University)]

Session IV: Encryption and Key Management

- [4a]Generic Mediated Encryption [Ibrahim Elashry, Yi Mu and Willy Susilo(Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong)]
- [4b]An Efficient Reconfigurable II-ONB Modular Multiplier [Li Miao, He Liangsheng, Gao Neng, Yang Tongjie and Liu Zongbin(Zhengzhou Information Science and Technology Institute, SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences)]
- [4c]Public-Key Encryption Resilient to Linear Related-Key Attacks [Hui Cui, Yi Mu and Man Ho Au(School of Computer Science and Software Engineering, University of Wollongong)]

Session V: Security in Software and Machine Learning

- [5a]Clonewise - Detecting Package-level Clones Using Machine Learning [Silvio Cesare, Yang Xiang and Jun Zhang(School of Information Technology, Deakin University)]
- [5b]Automatic Polymorphic Exploit Generation for Software Vulnerabilities [Minghua Wang, Purui Su, Qi Li, Lingyun Ying, Yi Yang and Dengguo Feng(Trusted Computing and Information Assurance

Laboratory, Institute of Software, Chinese Academy of Sciences, Institute of Information Security, ETH Zurich)]

Session VI: Network and System Security Model

- [6a]A Novel Web Tunnel Detection Method Based on Protocol Behaviors [Fei Wang, Liusheng Huang, Zhili Chen, Haibo Miao and Wei Yang(Department of Computer Science and Technology, Suzhou Institute for Advanced Study, University of Science and Technology of China)]
- [6b]Salus: Non-Hierarchical Memory Access Rights to Enforce the Principle of Least Privilege [Niels Avonds, Raoul Strackx, Pieter Agten and Frank Piessens(iMinds-DistriNet - KU Leuven)]
- [6c]Scalable Security Model Generation and Analysis using k-importance Measures [Jin B. Hong and Dong Seong Kim(Computer Science and Software Engineering, University of Canterbury)]

Session VII: Security and Privacy in Pervasive and Ubiquitous Computing

- [7a]The B-Side of Side Channel Leakage: Control Flow Security In Embedded Systems [Mehari Msgna, Konstantinos Markantonakis and Keith Mayes(Smart Card Centre, Information Security Group, Royal Holloway, University of London)]
- [7b]An e-payment architecture ensuring a high level of privacy protection [Aude Plateaux, Patrick Lacharme, Vincent Coquet, Sylvain Vernois, Kumar Murty and Christophe Rosenberger(ENSICAEN, BULL SAS, Department of Mathematics, 40 St. George Street, Toronto)]
- [7c]Unveiling Privacy Setting Breaches in Online Social Networks [Xin Ruan, Chuan Yue and Haining Wang(The College of William and Mary, University of Colorado Colorado Springs)]

SecureComm2013 で発表された論文の内，いくつかを以下に紹介する．

(1) [2c]DroidAPIMiner: Mining API-Level Features for Robust Malware Detection in Android [Yousra Aafer, Wenliang Du and Heng Yin(Dept. of Electrical Engineering & Computer Science, Syracuse University)]
本研究では，増加する Android マルウェアへの対策として，機械学習を用いた正規アプリとマルウェアの分類手法を提案している．
著者は，変化の激しい Android マルウェアに対して，長期的に使える手法を考案する必要があると述べた．提案手法では，まず正規アプリとマルウェアから特徴を抽出し，機械学習を行う．この際，使用するパラメータはロバスト性の高い特徴として，重要度の高い API コール，API を呼び出すパッケージ名，API が持つパラメータ，の 3 つを使用している．これらの特徴の抽出は，リバースエンジニアリングによって行われる．実験の結果，提案手法において kNN 分類法を用いた場合，99%程の精度と，2.2%程の false positive 率が表れた．

(2) [7c]Unveiling Privacy Setting Breaches in Online Social Networks [Xin Ruan, Chuan Yue and Haining Wang(The College of William and Mary, University of Colorado Colorado Springs)]
本研究では，オンラインソーシャルネットワーク (OSN) におけるプライバシ情報の流出について調査を行っている．
OSN においては，ユーザがプライバシに関する情報の公開範囲を設定できる．例えば，フェイスブックのユーザは，フレンドリストやプロフィール情報，投稿内容等の公開範囲を，一般公開・友人のみへの公開と言った粒度で変更できる．しかしながら，著者は，公開されている情報とユーザ間のつながりを用いることで，非公開の情報を推定することができる可能性があるとした．そこで，本研究では，フェイスブックのユーザ 30 万人を対象として，プライバシ情報を推定するためのスキームを実行し調査を行っている．提案されているスキームでは，対象となったあるユーザを起点として，公開されているユーザ間のつながりを元に公開情報を収集していく．最終的に，どのようなプライバシ公開設定に対しても高い確率で非公開の情報を推定することが可能であることを示した．

4.3 Best paper award

SecureComm2013 の会期最終日に，本会議の発表における Best paper が表彰された．表彰式では，SecureComm2013 で発表された以下の 2 つの研究が候補としてまず挙げられた．

- [3a]Disabling a Computer by Exploiting Softphone Vulnerabilities: Threat and Mitigation
  Ryan Farley and Xinyuan Wang(Department of Computer Science George Mason University)
- [1a]Anomaly Detection in Beacon-Enabled IEEE 802.15.4 Wireless Sensor Networks
  Eirini Karapistoli and Anastasios A. Economides(Department of Information Systems, University of Macedonia)

その後，次の発表が Best paper として表彰された．以

下にその概要を紹介する．

[3a]Disabling a Computer by Exploiting Softphone Vulnerabilities: Threat and Mitigation
Ryan Farley and Xinyuan Wang(Department of Computer Science George Mason University)

本研究は，VoIP ソフトフォンがホスト端末に課しているセキュリティ脅威や，その対策について調査を行っている．意図的に作られた SIP トラフィックは Vonage という VoIP ソフトフォンを動作させている Windows XP ホストを数分以内に動作不能にすることが分かった．そのような攻撃が閾値に基づいたフィルタリングによって効率的に緩和されるのに対して，stealthy attack が閾値に基づいたフィルタリングを通過し，対象とするソフトフォンに電話をかける事無く対象のコンピュータを動作不能にすることを示した．stealthy attack を緩和するために，著者らは，クライアントの代わりに SIP メッセージのインテンションを確かめるためにコンテキストと SIP プロトコル情報に影響を与える LCA(Limited Context Aware) フィルタリングを発展させた．正当な VoIP コールが通過するのを許可している間，LCA フィルタリングが効果的に stealthy attack を破ることを，著者らの実験は示した．

また，表彰候補となった次の論文についても概要を紹介する．

[1a]Anomaly Detection in Beacon-Enabled IEEE 802.15.4 Wireless Sensor Networks

本研究は，IEEE 802.15.4MAC プロトコルの beacon-enabled mode を安全にすることを目的とした新しい以上検知アルゴリズムを提案している．
発表者は，まずセンサネットワークにおけるセキュリティ上の制限として，リソースの制限や意図しないオペレーション，ブロードキャストの声質によるコミュニケーションの信頼性の低さについて述べた．次に，IEEE 802.15.4 MAC を対象とした攻撃として，PANId 衝突攻撃や，GTS 攻撃，False Data Injection などについて説明した．本研究では，そのような攻撃への対策として，異常検知アルゴリズムを提案した．また，ルールに基づく検知テクニックを用いた侵入の識別における提案アルゴリズムのパフォーマンスがシミュレーションの結果として示された．シミュレーションの結果は，提案手法がエネルギー消費のオーバーヘッドをかなり小さいレベルに維持しつつ，識別されているあらゆるタイプの攻撃に対して高い検知率を見せたことを示した．

5. ATIS2013 における発表紹介

5.1 招待講演

ATIS2013 において招待講演が開催された．

Revisiting Identity-based encryption towards no-escrow: Application and analysis of Embedding Secret Key Information in RSA moduli

[Professor Kouichi SAKURAI (Kyushu University and Institute of Systems & Information Technologies and Nanotechnologies)]

講演では，最初に公開鍵 $N = pq$ に基づく ID ベース暗号スキームの既存アプローチについて調査結果が報告された．また，講演者は，そのような ID ベース暗号に関連した鍵供託問題について議論し，この問題をどのように対策すべきか考察を行った．公開鍵における情報埋め込みの既存手法を発展させ，公開鍵オーナーのなりすますしを防ぐための新しい手法を発展させる．講演者らは，その手法を匿名暗号スキームに適用した．また，Lenstra らによる RSA モジュールに対する秘密情報の埋め込みアルゴリズムのさらなる解析について報告を行った．

5.2 ATIS2013 における発表

ATIS2013 では，6 件の研究発表が行われた．以下に各発表のタイトルを示す．

- [a]Detection of Android API Call Using Logging Mechanism within Android Framework [Yuuki Nishimoto, Naoya Kajiwara, Shinichi Matsumoto, Yoshiaki Hori and Kouichi Sakurai(Kyushu University, Institute of Systems, Information Technologies and Nanotechnologies, Saga University)]
- [b]Ensuring Data Integrity by Anomaly Node Detection during Data Gathering in WSNs [Quazi Mamun, Rafiqul Islam and Mohammed Kaosar(School of Computing and Mathematics, Charles Sturt University)]
- [c]Securing a Web-based Anti-counterfeit RFID System [Belal Chowdhury, Morshed Chowdhury and Jemal Abawajy(Melbourne Institute of Technology, Deakin University)]
- [d]Security concerns and remedy in a Cloud Based E-learning System [Md. Anwar Hossain Masud , Md. Rafiqul Islam and Jemal Abawajy(School of Computing and Mathematics, Charles Sturt University, School of Information Technology, Deakin University)]
- [e]Reversible Data Hiding Scheme based on 3-Least Significant Bits and Mix Column Transform [Wafaa

Abduallah, Abdul Monem S. Rahma and Al-Sakib Khan Pathan(Department of Computer Science, International Islamic University Malaysia, Department of Computer Science, University of Technology)]

- [f](k-n) Oblivious Transfer using Fully Homomorphic Encryption System [Mohammed Kaosar, Quazi Mamun, Rafiqul Islam and Xun Yi(School of Computing and Mathematics, Charles Sturt University, School of Engineering and Science, Victoria University)]

6. 次回開催について

SecureComm2013 の最終日に，SecureComm の次回開催についてアナウンスが行われた．次回の SecureComm は，2014 年 9 月 23 日から 26 日の 4 日間，中国の北京で開催される予定である．また，ATIS に関しては，現時点で次回の予定は発表されていない．

7. おわりに

本稿では，2013 年 9 月 25 から 27 日にオーストラリアのシドニー，Aerial UTS Function Centre にて開催された 9th International Conference on Security and Privacy in Communication Networks(SecureComm2013)，及び同月 26 日に開催された併設ワークショップ 4th International Workshop on Applications and Techniques in Information Security(ATIS2013) に関し，その概要を報告した．

謝辞 本研究の一部は，日本学術振興会 科学研究費補助金 基盤 B（課題番号 23300027）による補助のもとで行われた．また，本稿をまとめるにあたって，窪田歩氏，磯原隆将氏から支援を頂いた．

参考文献

[1] SECURECOMM 2013 - 9th International Conference on Security and Privacy in Communication Networks
http://securecomm.org/2013/show/home
[2] Cyberspace Security
http://www.deakin.edu.au/sebe/it/cyberspace-security/index.php
[3] SECURECOMM 2013 - Final Program in Full
http://securecomm.org/2013/show/program-final
[4] SECURECOMM 2012 - Final Program in Full
http://securecomm.org/2012/show/program-final
[5] SecureComm 2011 7th International ICST Conference on Security and Privacy in Communications Network
http://securecomm.org/2011/techprog.shtml