Vol.2012-CSEC-57 No.8
Vol.2012-IOT17 No.8
2012/5/10

ESSoS(セキュアソフトウェアおよびシステム工学) 12 参加報告

松本晋一[†]　櫻井幸一[†,††]

本稿は, 2012 年 2 月 16 日から 17 日に, オランダのアイントホーフェン工科大学 (Technische Universiteit Eindhoven) にて開催された，第 4 回 International Symposium on Engineering Secure Software and Systems (ESSoS 12)に関して，その内容を報告する.

ESSoS(Engineering Secure Software and Systems) 12 symposium report

SHINICHI MATSUMOTO[†]　KOUICHI SAKURAI[†,††]

This paper reports on the 4th International Symposium on Engineering Secure Software and System (ESSoS 12), held on February 16 to 17, 2012,　at Technische Universiteit Eindhoven, Netherlands.

1. はじめに

本稿では，2012 年 2 月 16 日と 17 日の両日，オランダのアイントホーフェン工科大学(Technische Universiteit Eindhoven) にて開催された，第 4 回 ESSoS (International Symposium on Engineering Secure Software and Systems 12)[1]に関し，その内容を報告する.

2. シンポジウム概要

International Symposium on Engineering Secure Software and Systems(以下, ESSoS とする)は, ACM SIGSAC (the ACM interest group in security)と同 SIGSOFT(the ACM interest group in software engineering), および IEEE Computer Society の共同技術スポンサーシップによる年次コンファレンスであり，ソフトウェアとコンピュータシステムのセキュリティに関する話題を取扱う.

本年はオランダ，北ブラバント州アイントホーフェンのアイントホーフェン工科大学にて 2 月 16 日から 17 日の二日間に渡り開催され, 欧州を中心とした各国から 40 名余りが参加した．日本からの参加者は，発表者一名のみであった.

2.1 運営体制

本会議は以下のメンバーにより運営された.

- General Chair
  Sandro Etalle(Technical University of Eindhoven)
- Program Co-chairs
  Gilles Barthe(IMDEA Software Institute)
  Ben Livshits(Microsoft Research)
- Publication Chair
  Riccardo Scandariato(Katholieke Universiteit Leuven)
- Publicity Chair
  Pieter Philippaerts(Katholieke Universiteit Leuven)
- Local Arrangements Co-chairs
  Jerry den Hartog(Eindhoven University of Technology)
  Jolande Matthijsse(Eindhoven University of Technology)

また，開催にあたっては EU の NESSOS (Network of Excellence on Engineering Secure Future Internet Software Services and Systems)，およびオランダ国内の NWO (Netherlandse Organisatie voor Wetenschappelijk Onderzoek), 並びに NWO/Jacquard (Joint Academic and Commercial Quality Research & Development)のセキュリティプログラムによりスポンサードされている.

また本会の講演録は，Springer LNCS 7159[2]として刊行されている.

2.2 Call for Paper

ESSoS の趣旨について, 論文募集の要項より抜粋すると，「Internet のようなネットワーク接続された環境においては, ソフトウェアの脆弱性はあらゆる所から攻撃されうる. これに対処するためには，暗号処理コンポネントといった高品質なセキュリティビルディングブロックが不可欠ではあるが, これだけでは十分ではない. セキュアなソフトウェアの構築には課題が多く，これは現代のアプリケーションの複雑さ，セキュリティ要求が厳密さを増してきていること，利用可能なソフトウェア技術の多さ，攻撃ベクタの進化のためである．課題解決のためのスケーラビリティのあ

[†]（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
Department of Informatics, Kyushu University

る技術が必要とされている」という現状認識のもと,「研究者と実務者の双方に，セキュアなソフトウェアエンジニアリングにおける最新の技術とプラクティスを促進すること」を目的としている．

この目的に沿った形で，以下のようなテーマの投稿が呼びかけられた．

- 脅威のモデリングと，脆弱性解析のためのスケーラブルな技法
- セキュリティ要求とポリシイの策定と管理
- ソフトウェアとシステムのセキュリティアーキテクチャおよび設計
- セキュリティのためのモデル検査
- セキュリティ成果物の形式的規定
- セキュリティプロパティの検証技法
- セキュリティベストプラクティスのシステマティックなサポート
- セキュリティテスティング
- セキュリティアシュアランスケース
- セキュリティのためのプログラミングパラダイム、モデルおよび DSL
- プログラムのリライティング技法
- セキュアなソフトウェア/システムの開発のプロセス
- セキュリティ指向なソフトウェアの再構築と進化
- セキュリティの測定(measurement)
- 開発の自動化
- セキュリティとその他非機能要求間のトレードオフ
- アシュアランス，サティフィケーション，アクレディテーションのサポート

2.3 投稿論文

論文募集に対しては 53 本の論文が寄せられた．この内 7 本が Full Paper として採択されたことから，採択率は 13%となる．また残りの論文の内，7 本が Idea Paper として採用された．Idea Paper としては,「研究/開発の初期段階にはあるが，興味深く新しいアイデアの crisp exposition を与えるもの」が選出されている．

採用された論文の，発表者の国別の内訳は(Full Paper と Idea Paper を合算), ドイツが 4 本, フランスが 2 本であり，残りはイギリス，イタリア，スペイン，スウェーデン，ノルウェー，ギリシャ，アメリカ合衆国，シンガポールから各 1 本ずつであった．

また大学/企業の内訳は，大学からのものが 12 本，企業からが 2 本と，大学からのものが大多数であった．

2.4 ESSoS 12 の構成

講演は 2 日間の会期のシングルトラックで構成された．セッションの構成は，表 1 の通りである．各行の数字は，各セッション内の発表件数を表す(Full Paper，および Idea Paper を合算).

表 1 ESSoS 12 における，セッション構成
Table1 Sessions in ESSoS 12.

ESSoS 2012(開催地: Eindhoven, Netherlands)	
Formal Methods	3
Mobile Devices	3
Trust	2
Models and Policies	3
Applied Cryptography	3

計 14 本の論文発表に加えて，各開催日の最初に，基調講演が 2 本行われた．

なお，会期の前日には Doctoral Symposium が開催され，12 本の論文が発表された．その他のチュートリアルやワークショップ類の併催，またポスターセッションなどはなかった．

2.5 ESSoS の変遷

ESSoS は 2009 年の開催から数えて，本年の開催で 4 回目を数える．この間の内容の変遷について，セッションのタイトルとその構成から辿ると，表 2 のようになる．各行の数字は，各セッション内の発表件数を表わす．

表 2 ESSoS における，セッション構成の変遷
Table2 Changes in ESSoS programs.

ESSoS 2009(開催地 Leven, Belgium)[3]	
Attack analysis and prevention	3
Policy verification and enforcement	3
Refinement and transformation	4
Testing and faults	4
Secure system development	4
ESSoS 2010(開催地: Pisa, Italy)[4]	
Policy verification and enforcement I	3
Secure system and software development I	3
Attack analysis and prevention	3
Secure system and software development Ⅱ	3
Policy verification and enforcement Ⅱ	3
Attack analysis and prevention Ⅱ	3
ESSoS 2011(開催地: Madrid, Spain)[5]	
Model-based Security Ⅰ	3
Tools and Mechanisms	3
Web Security	3
Model-based security Ⅱ	3
Ideas	3
Security Requirements Engineering	3
Authorization	3

3. ESSoS 12 における発表

3.1 初日基調講演

(1) **Improving Software Reliability and Security via Symbolic Execution**

[Cristian Cadar(Imperial College)]

シンボリック実行によるソフトウェアの検証技術と，当該技術を用いたソフトウェアの脆弱性発見に関し，講演者らが開発したツール EGT, EXE, KLEE の概要を紹介した．

シンボリック実行による検証を実用的なものにするためには，パス探索を最適化し，検証時間を実用的なものに抑える必要がある．パスの削除(静的なパスのマージ, Phi-node folding)，Irrelevant Constraint Elimination と Caching の組合せが効果があることを示した．

一方，ソフトウェア検証において意味論的バグの検査は困難であるが，これは検証のためのアサーションの記述に関する問題に起因する．即ち，

- ソフトウェア仕様のアサーションでの記述に要する工数の問題．
- ソフトウェア仕様が，アサーションに正しく記述されているかの証明の問題．

これらの問題に対して，講演者はクロスチェックによる検証という考え方を示した．クロスチェックとは，ここでは同一のソフトウェア仕様に基づく複数の実装間での動作の差異の検証を指す．

この場合，ソフトウェア仕様に基づいてアサーションの記述を行う必要がなく，またその故に，ソフトウェア仕様とアサーションとの差異も生じない．

講演者らはこの考えに基づき，次に示す各実装についてクロスチェックによる検証を行い，その有効性を示した．

- BusyBox と，GNU Coreutils の内の BusyBox 相当機能の双方の振る舞い．
- Zeroconf 仕様のオープンソース実装である，Avahi と Bonjour の振る舞い．
- OpenCV のリファレンス実装と，同じく OpenCV の SIMD 最適化コードの振る舞い．

3.2 セッション Formal methods

座長: Cristian Cadar (Imperial College)

(1) Runtime Enforcement of Information Flow Security in Tree Manipulating Processes

[Máté Kovács and Helmut Seidl (共に Technische Universität München)]

現代のワークフロー言語において実装されている，Web サービスやビジネスプロセスといった XML 文書のツリー操作処理における，情報フローポリシイの強制を実現するための，ランタイムモニタ方式の提案．

著者らはまずツリー操作のための最低限の仕様のみを持つプログラミング言語を設計した．次にアプリケーションの例として，論文の投稿およびレビューの支援システムを仮定し，情報フローポリシイに基づくモニタリングが必要な状況の例について述べた．次にランタイムモニタの形式的表現について述べ，当該モニタにより実現される保証を明らかにしている．

最後に他の関連研究との比較を行い，ツリー操作に基づく本方式が，変数やノード単体のテインティングに着目する他の研究よりも，高い精度での判断が可能であると結論付けている．

(2) Formalisation and Implementation of a Standard Access Control Mechanism for Web Services

[Massimiliano Masi(Tiani “Spirit” GmbH/Università degli Studi di Firenze), Rosario Pugliese(Università degli Studi di Firenze) and Francesco Tiezzi(IMT Advanced Studies Lucca]

Policy Based Access Control(PBAC)記述のための言語として eXtensible Access Control Markup Language(XACML)があるが，当該言語は XML ベースであることから，

- 一般的なテキストエディタでは，編集が困難．
- XACML ポリシイの記述における一貫性の保持が困難であり，エラーを防ぎにくい

という問題をかかえている．著者らはこれに対処するため，本稿において，より形式的なアクセス制御記述言語を実装している．

また当該言語のエディタ，および当該言語から XACML へのコンバータを備えたツールを実装している．実装言語としては Java を，パーサとしては ANTLR を用いている．

著者らの実装したツールは，Web 上で公開されている[6].

(3) Hunting Application-Level Logical Errors (Idea Paper)

[George Stergiopoulos, Bill Tsoumas and Dimitris Gritzalis (共に Athens University of Economics and Business)]

著者らは，ビジネスアプリケーション内へのビジネスロジック組込みにおける技術的な脆弱性検証(バッファオーバーフローや SQL インジェクション等)についてはこれまで研究が進められてきたが，アプリケーションレベルの論理的脆弱性(LV: Logic Vulnerability)についてはあまり関心が払われてこなかったと指摘，解析のためのフレームワーク”App_LogGIC”を提案している．

当該フレームワークは，以下のコンポネント，

- IBM(Invariant-Based Analysis Method): Daikon による動的解析と，Java PathFinder による静的解析を組合せ，解析対象となるアプリケーションのビジネスロジックを抽出する．
- IEM(Information Extraction Method): IBM からの情報

と，ソースコードから生成した抽象構文木，さらに入力ベクタのエントリポイントを解析し，LV に関する情報を精緻化する．出力のフィルタに必要な情報を抽出する．

に基づき構成されている．既に LV の存在が確認されているスタンドアロンの Java GUI アプリケーションをサンプルに，当該フレームワークによる LV 解析を行い，全ての LV が検出されることを示した．

3.3 セッション Mobile devices

座長: Wouter Joosen(KU Leuven – DistriNet research group)

(1) Challenges in Implementing End-to-End Secure Protocol for Java ME-Based Mobile Data Collection in Low-Budget Settings (Idea Paper)

[Samson Gejibo, Federico Mancini, Khalid A.Mughal, Remi Valvik, and Jørn Klungsøyr (共に University of Bergen)]

MDCS(Mobile Data Collection Systems)システムにおける，モバイルデバイス側の実装のための，Java ME 上へのセキュアな通信プロトコルの実装方法に関する発表．

Java ME 上での実装に関する課題として以下を挙げ，それぞれ対策を述べている．

- 暗号処理 API の選択，あるいは新規実装

  初期の Java ME は暗号処理 API を備えていない．Security and Trust Services API(SATSA)が後に Java ME のオプショナルパッケージとなったが，これを実際にサポートする携帯電話は数少ない．

  一方，オープンソースの暗号処理 API である Bouncy Castle 実装は，外部 API であることからメモリオーバヘッドが多大である．

  著者らは暗号処理 API のインタフェースのみを提供し，実装として SATSA と Bouncy Castle を選択可能なアーキテクチャを採用した．
- 鍵の生成

  携帯電話は十分なエントロピー源を持たず，J2ME には適切なライブラリもないことから，サーバ上で乱数を生成し，端末に送信する方式を採っている．
- データのセキュアなアップロード/ダウンロード

  HTTPS と，著者らのオリジナルのプロトコルを選択可能な API を実装している．
- セキュアなストレージ

  複数ユーザが同一端末を用いることを可能とするため，ユーザ認証に基づき，MIDP の Record Management System との間で暗号化されたデータを読み書きする API を実装している．

これらの設計指針に基づき，当該実装の，Java ME を搭載したローエンドの携帯電話上での性能評価を行った結果を示し，十分な性能を得た旨を報告している．

(2) Application-Replay Attack on Java Cards: When the Garbage Collector Gets Confused

[Guillaume Barbu (Institut Telecom/Télécom ParisTech, Parq Scientifique), Philippe Hoogvorst and Guillaume Due(共に Institut Telecom/ Télécom ParisTech)]

Java Card 仕様の新版である 3.0 版では，旧版からの拡張として，組込み Web サーバやマルチスレッディングサポートなどの仕様と共に，自動ガーベッジコレクションが盛り込まれている．

しかし著者らは，Java Card 仕様の 2.2.2 版と 3.0 版では，アプリケーションインスタンスの削除に関する挙動の規定が変更されていることに着目し，アプリケーションインスタンスが削除されたものの，そのアプリケーションに属するオブジェクトが削除されない状況が形成されうることを示す．

また，この状況を意図的に作り出し，更に著者らがリファレンス予測と呼ぶ手法を用いることで，アプリケーションファイアウォールを回避した攻撃が成立しうることを示した．

(3) Plagiarizing Smartphone Applications: Attack Strategies and Defense Techniques

[Rahul Potharaju, Andrew Newell, Christina Nita-Rotaru, and Xingyu Zhang (共に Purdue University)]

著者らは，スマートフォンにおけるアプリケーションの剽窃は，多くがマルウェアの偽装の手段として行われていることから，マルウェア検出にはアプリケーションの剽窃行為の判定が重要であることを主張し，このような剽窃アプリケーション判定のための手法を提案している．

当該方式ではアプリケーションのバイナリ(DEX 形式)から，メソッドレベルで AST(抽象構文木)を構築し，シンボルカバレッジ，AST 距離，AST カバレッジの手法を用い判定を行う．

本手法に基づく検証システムの実装を評価し，評価対象のアプリケーション群の中から，剽窃版アプリケーションの全てを検出し，偽陽性率 0.5%の結果を得たこと，また判定処理の処理速度として十分実用的な結果を得たことを報告している．

3.4 セッション Trust

座長: Sandro Etalle(TU Eindhoven)

(1) A Task Ordering Approach for Automatic Trust Establishment

[Francisco Moyano, Carman Fernandez-Gago, and Javier Lopez (共に University of Malaga)]

アクセス制御の判断プロセスにおいて必要となる信頼度の定量化(Trust metric)に関する研究．

信頼度の定量化のために，複数エンティティ間の，あるタスクに対して信頼度の順序付けを行う(トラストを，重み付双方向グラフで表現する．タスクについての重ね合わせで重み付き多重グラフを構築することで，信頼度の定量化を実現する．

ケーススタディとして，e-health システムへの適用が説明された．実装は今後の課題とのことだった．

(2) Optimal Trust Mining and Computing on Keyed MapReduce(Idea Paper)

[Huafei Zhu(A*STAR) and Hong Xial(AFEU, Xi'An)]

Keyed MapReduce を用いたトラストマイニングに関する研究．ネットワーク上の (掲示板上の投稿や Web ページの内容，何らかの reputation サービス上の評価などといった) 情報を収集し，蓄積した中から，Keyed MapReduce を用いてトラストマイニングを行うステップと，この結果からスコアを計算するステップからなる．

なお当該論文は，予稿集には掲載されているが，発表自体はキャンセルされた．

3.5 二日目基調講演

(1) **An Overview of Modern Security Threats**

[Thorsten Holz(Ruhr-Universität Bochum)]

講演者は，近年のセキュリティ上の脅威の特徴として，APT: Advanced Persistent Threat を挙げた．これは，特定のターゲットに対し継続して，かつ様々な手法を駆使して攻撃(スパイ行為や妨害行為)を行うものである．

このような攻撃の例として，クラッカー集団 LulzSec と Sony の暗闘を紹介し，APT は多くの企業をリスクにさらしかねない脅威であることを示した．

しかしその一方で，攻撃手段は技術的には洗練されているとは限らず，その脅威は幾分誇張気味に騒がれすぎているとも述べた．

講演者はその他 Stuxnet や SPAM の問題についても述べ，最後にまとめとして，攻撃者は金銭的なモチベーションに基づき行動することが多いことを手掛かりに，攻撃側の経済的インセンティブについて検討を加える事が重要であると結論付け，ワークショップ Workshop on the Economics of Information Security(WEIS)[7]の開催を案内した．

3.6 セッション Models and policies

座長: Thorsten Holz(Ruhr-Universität Bochum)

(1) Supporting the Development and Documentation of ISO 27001 Information Security Management Systems Through Security Requirements Engineering Approaches (Idea Paper)

[Kristian Beckers, Stephan Faßbender, Maritta Heisel, (University of Duisburg-Essen), Jan-Christoph Küster (Fraunhofer Institut for Software and Systems Engineering) and Holger Schmidt(University of Duisburg-Essen)]

筆者らは，ISO27001 に準拠する情報セキュリティマネジメントシステム(ISMS: Information Security Management System)構築の困難さは，これをサポートするシステム開発やドキュメントの乏しさにあると指摘し，その上で，セキュリティ要求工学(SRE: Security Requirement Engineering)のアプローチを，セキュリティ要件の抽出と分析に留まらず，ISO27001 準拠の ISMS 構築に適用することを提案した．

著者らは SRE によって異なる表現，用語のばらつきを吸収するため，Fabian らの概念フレームワーク(CF: Conceptual Framework)による SRE メソッドの分類を活用する．

著者らは，これにより ISO 27001 準拠のシステム開発および文書化に既存の SRE メソッドの再利用を可能とし，ISO 27001 の実現をサポートすることが可能と結論付けている．

(2) An Independent Validation of Vulnerabilities Discovery Models (Idea Paper)

[Viet Hung Nguyen and Fabio Massacci (共に University of Trento)]

複数の脆弱性発見モデル(VDM: Vulnerabilities Discovery Model)を，3 種類の Web ブラウザ(Firefox, Google Chrome, Microsoft Internet Explorer)の複数のバージョンに対して適用し，比較を行った．比較対象となった VDM は，

- Rescolar Quadratic(RQ)
- Rescolar Exponential(RE)
- Alhazmi-Malaiya Logistic(AML)
- Anderson Thermodynamic(AT)
- Linear model(LN)
- Logarithmic Poisson(LP): Musa-Okumoto Model

の 6 種類であり，各モデルの NIST の NVD (National Vulnerability Database)との適合度を求めることで比較を行っている．

(3) Transversal Policy Conflict Detection

[Matteo Maria Casalino, Henrik Plate, and Slim Trabelsi (共に SAP Labs France)]

これまでのポリシイ解析のアプローチは，多くが単一のクラス(アクセス制御，フィルタリング，データ保護など)を対象としてきた．

これに対し，異なるクラスに属し，異なる言語で表現された複数のセキュリティポリシイを組み合わせる際に横断的なポリシイ衝突(Transversal Policy Conflict)が発生する恐れがある．

当該論文では，このような衝突がセキュリティ上の脆弱性や，コンプライアンス違反を引き起こし，なおかつ問題の特定や修整にコストを要すると指摘，衝突を事前に検出

するためのフレームワークを提案している．

フレームワークは以下から構成される

- ドメイン記述モデル(DDM: Domain Description Model)
  管理対象となるドメインを記述し，クラス間の相互依存関係をモデル化する．
- クラス固有ポリシイモデル(CSPM: Class-Specific Policy Model)
  クラスに属するポリシイの形式的表現によるモデル．
- 衝突規定モデル(CSM: Conflict Specification Model)
  検出対象となる，横断的衝突を定義する．

これらを組合せ，検出対象となる横断的衝突は，SAT(充足可能性問題)として解決されることを示した．

3.7 セッション Applied cryptography

座長: Gilles Barthe(IMDEA Software)

(1) Typed Assembler for a Crypto-Processor(Idea Paper)

[Peter Breuer(University of Birmingham), and Jonathan P.Bowen(London South Bank University)]

著者らが Crypto-processor と呼ぶ, 新しいプロセッサアーキテクチャの提案.

筆者らの呼ぶ Crypto-processor は(既存の用法における暗号プロセッサとは異なり)，プロセッサとしては RISC アーキテクチャに基づくが，暗号化されたデータも平文のデータも，復号の必要なく直接演算可能なものである．

当該プロセッサの命令セットアーキテクチャは R. Milner の型推論機構を備え，型安全性を保持するよう設計されている．

(2) A sound decision procedure for the compositionality of secrecy

[Martin Ochoa(TU Dortmund/Siemens AG), Jan Jürjens (TU Dortmund/Fraunhofer ISST) and Daniel Warzecha (TU Dortmund)]

秘密保持プロセスの合成後の秘密保持性は，Dolev-Yao 攻撃モデルにおいては保証されない．著者らは，この証明の効率化は，システムの検証をスケーラブルなものにするためには不可欠である事，また再利用可能なコンポネントを用いたソフトウェア開発において特に重要となると主張し，大規模なコンピュータシステムの検証における，合成的モデル検査のスケーラビリティ実現のための手法について述べた．

本手法では，コンポネントに対して将来のプロセス合成時に使用できる依存木を予め生成し，合成時には当該ツリーをマージする．これにより，スクラッチからの解析ではなくインクリメンタルな解析を可能とすることで，検証の効率改善を図っている．

本手法に基づツールの実装を行い，検証対象として TLS(旧版)を例に，有効性の検証を行っている．

(3) Design of Adaptive Security Mechanisms for Real-Time Embedded Systems

[Mehrdad Saadatmand, Antonio Cicchetti and Mikael Sjödin(共に Mälardalen University)]

実時間性とセキュリティを実現可能な，組込みリアルタイムシステムのための OS の設計についての研究．時間制約に対して，使用する暗号化アルゴリズムを適切に選択することで，実時間性を満たす．

アプリケーションが，暗号化処理を行う必要が生じた場合, これまでの暗号化処理時間の履歴を収めたログ情報と，暗号化アルゴリズムのプレファレンスを参照し，時間制約を元に暗号化アルゴリズムを選択する．暗号化処理に要した時間はモニタリングプロセスが測定し，ログに追加することで，タイミングに関する振る舞いを参照可能にする．

当該アーキテクチャを，ENEA OSE 上に拡張することで構築し，評価を行っている．

4. 次回開催について

本会のクロージングにて，次回開催はフランスのパリでの開催予定であることが示された．3 月末の時点では，スケジュール等詳細については未だ示されていない．

5. おわりに

本稿では，2012 年 2 月 16 日と 17 日の二日間，オランダのアイントホーフェンで開催された，第 4 回 ESSoS (International Symposium on Engineering Secure Software and Systems 12)に関して，その概要を示した．

参考文献

1 ESSoS| International Symposium on Engineering Secure Software and Systems
http://distrinet.cs.kuleuven.be/events/essos/2012/index.html
2 G.Barthe, Benjamin Livshits, and Riccardo Scandariato(Eds.) “Engineering Secure Software and Systems”, volume 7159 of LNCS, Springer, 2012
3 ESSoS 09
http://distrinet.cs.kuleuven.be/events/essos/2009/
4 ESSoS 10
http://distrinet.cs.kuleuven.be/events/essos/2010/
5 ESSoS 11
http://distrinet.cs.kuleuven.be/events/essos/2011/
6 Formalisation and Implementation of XACML
http://rap.dsi.unifi.it/xacml_tools/
7 11th Annual Workshop on the Economics of Information Security(WEIS 2012).
http://weis2012.econinfosec.org/