Vol.2016-CSEC-74 No.18
Vol.2016-SPT-19 No.18
2016/7/14

第一回 IEEE European Symposium on Security and Privacy 参加報告

松本晋一[†1]　松浦幹太[†2]

概要： IEEE European Symposium on Security and Privacy（以下，IEEE Euro S&P）の第一回が，ドイツザールラント州ザールブリュッケンのザールブリュッケン会議場にて，2016 年 3 月 21 日から 24 日の 4 日間の会期で催された．同会議は例年米国西海岸にて催されている IEEE Security and Privacy の欧州における姉妹会議となる．本稿では同会議の概要について報告する．

キーワード：学会参加報告，セキュリティ，プライバシ，情報フロー，カバートチャネル

Report on the First IEEE European Symposium on Security and Privacy

SHINICHI MATSUMOTO[†1]　KANTA MATSUURA[†2]

Abstract: IEEE European Symposium on Security and Privacy has been held at Conference Hall of Saarbrucken in Saarbrucken, Germany from 21st March to 24th. It is a sister conference of annual IEEE Security and Privacy conference held in west coast in US. In this paper, we report the abstract of this conference.

Keywords: Conference report, Security, Privacy, Information Flow, Covert Channel

1. IEEE Euro S&P の概要

IEEE Symposium on Security and Privacy（以下, IEEE S&P）は，これまで米国西海岸でずっと開催されてきた，長い歴史を持つ伝統ある年次学会であるが， IEEE Euro S&P [1]は，この IEEE S&P の，欧州における姉妹学会として企画された学会である．

1.1 IEEE Euro S&P 2016 概要

IEEE Euro S&P の第一回目となる今回は，ドイツ，ザールラント州の州都であるザールブリュッケンで催された．同地は，地理的にも欧州の中心となる象徴的な意味を持つことから，またザールブリュッケン大学やマックス・プランク研究所の研究施設を要するなど，ドイツのみならず欧州内でも科学技術研究の要所としてプレゼンスを持つことから，今回の欧州での初回の開催地として選ばれたものと思われる．

1.2 会場

本会議の会場であるザールブリュッケン会議場（Congresshalle Saarbrücken，図 1）は，駅（Saarbrücken Hbf）より歩いて 10 分ほどの場所にある．

日本からのアクセスはあまり優れず，著者（松本）はフランクフルト国際空港を経由し，鉄道で 3 時間ほどかけて移動した．

ザールブリュッケンはドイツの中でも西の，フランスとの国境近くにあり，一時期はフランス領でもあった．街中の案内表示が，ドイツ語だけでなくフランス語で書かれたものもある点などにもそれは見て取れた．

3 月の気候は，日本より少々寒い程度であり，それほど着込む必要はなかった．

本会の運営に貢献しているザールラント大は会場より北東に 5km ほどの位置にあり，同大はセキュリティ研究の

図 1. 会場となったザールブリュッケン会議場

†1 (公財)九州先端科学技術研究所
Institute of Systems, Information Technologies and Nanotechnologies
†2 東京大学生産技術研究所
Institute of Industrial Science, the University of Tokyo

Vol.2016-CSEC-74 No.18
Vol.2016-SPT-19 No.18
2016/7/14

拠点 CISPA（Center for IT-Security, Privacy and Accountability）を要している．

1.3 スポンサー

Euro S&P 2016 は，以下の支援を受けて運営された．

- プラチナサポーター
  - Federal Ministry of Education and Research(ドイツ連邦教育科学研究技術省)
- シルバーサポーター
  - Universität Bonn, Fraunhofer FKIE (Institute for Communication, Information Processing and Ergonomics)
  - Oxford University Press
- ブロンズサポーター
  - Intel Corporation
- 運営
  - Saarland 大 CISPA(Center for IT Security, Privacy, and Accountability)
  - ザールラント州政府

2. 会議プログラム

2.1 プログラム構成

会議は 4 日間に渡って開催されたが，初日である 3 月 21 日は, 夕方に参加者登録とレセプションが行われただけで，実質的に 22 日からの 3 日間の会議である．会場は，ザールブリュッケン会議場内の大ホール（Grosse Halle）（図 2）一部屋であり，全体が単一トラックで進行したことから，参加者は全てのセッションに参加できる構成であった．3 日間のセッション構成は以下の通りである[1]．各行の右側の数字は，セッション内での発表論文数を示している．

- Day 1(March 22)
  - Keynote (by Adi Shamir)
  - Information Flow 4
  - Security Protocols 4
  - OS & Database Security 3
- Day 2(March 23)
  - Privacy 3
  - Cryptography 4
  - Attacks 3
  - Short Talks
- Day 3(March 24)
  - Security & Learning 3
  - Network Security 3
  - Protocol Analysis 2

全体として，特定のテーマに偏らず，バラエティに富むようプログラム構成が組まれていると感じた．またセッション名が, 例えば近年の IEEE S&P などのものより抽象的，間接的で，表現が抑えてあるため，セッション名から発表テーマを推し量りにくい傾向にある．

図 2 大ホールでのセッションの様子

そんな中で最近の研究動向を反映した発表としては，Security & Learning セッションにおいて, 深層ニューラルネットワークによる画像解析を用いる発表が 2 件行われている．また現在 TLS プロトコルの新版の標準化作業が進められている一方で，当該プロトコルの草案の検証に関する発表が他の学会でも多く，研究が盛んに進められていることが分かるが，Security Protocol セッションにおいては，TLS1.3 プロトコルの検証のためのモデリングに関する発表が行われている．

2.2 オープニング

初日朝のオープニングは，General Chair の Andreas Zeller（CISPA, Saarland University）の言葉で開幕した．またオープニングでは，ザールラント大学の Volker Linneweber 学長よりの挨拶も行われ，同大学が，今回の IEEE Euro S&P に並々ならぬ力を傾けていることが分かった．

2.3 投稿状況

オープニングに続いて，プログラム委員長の Michael Backes（CISPA，SaarlandUniversity & MPI-SWS）より論文投稿および採択状況について説明された．

プログラム委員長の報告によれば，投稿論文は 32 か国から計 168 件を集めたとのことである．投稿件数の地域別内訳としては欧州からが 6 割弱, 北米からが 3 割弱であり，残りがその他の国からの投稿とのことである．採択数は 29 件のため採択率は 17.3%である．第一回の開催ということもあり，今回の採択率が試金石となるものと思われる．

採択論文の筆頭著者の所属を元に判断した，著者の国別内訳を図 3 に示す．欧州での開催にも関わらず，国別では米国が突出して多く，存在感を示していることが明確である．また次に開催国であるドイツが続く．結果，米国を除

Vol.2016-CSEC-74 No.18
Vol.2016-SPT-19 No.18
2016/7/14

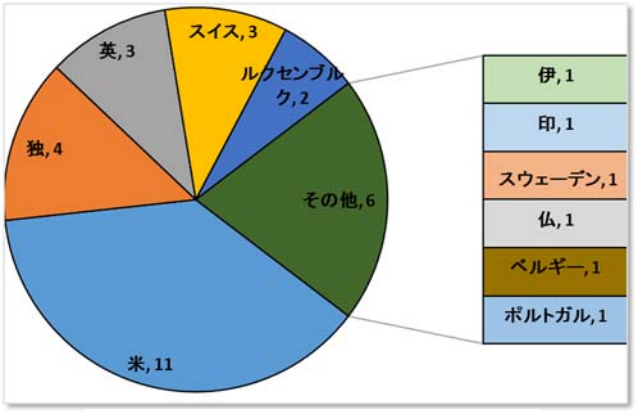

図 3 採択論文の国別内訳

けばほとんどが欧州からの発表となるが，ただ一件，欧米以外ではインドからの発表が採択されていることが目を引く結果となっている．

査読プロセスについても説明があり，プログラム委員 53 名が総計 567 件，一人当たり 10.7 件の投稿レビューを担当し，オンラインでの議論を経た後，フランクフルトでの 2 日間のオフライン会議で最終的な採択が決定されたとのことである

2.4 Keynote “Extended Functionality Attacks on IoT Devices: The Case of Smart Lights”, Adi Shamir [2]

Adi Smamir 先生による基調講演は初日朝に行われた. IoT デバイスのセキュリティについての発表である. 講演では，導入部にて，IoT 技術とその市場についての今後の展望について述べた後, IoT デバイスに対する攻撃を, 以下の 4 種に分類した．

- タイプ 1: IoT デバイスの機能を無視（無効に)するもの．
- タイプ 2: IoT デバイスの本来の機能を制限，性能劣化させるもの．これには DoS/DDoS 攻撃，Jamming や Ransomware も含まれる．
- タイプ 3: IoT デバイスの本来の機能を Misuse するもの. 本来のものとは異なる機能を使った悪ふざけや諜報活動など．
- タイプ 4: IoT デバイスの本来の機能を拡張し，全く異なる物理的効果を得るもの（「MacGyver のような発明工夫」という表現がされていた）．

講演ではこれら四種の攻撃のうち，タイプ 4 が最も興味深いタイプであるとして，このようなタイプの新しい攻撃についての試行の成果が紹介された．

LED 電球は，ネットワークを経由して制御可能なものがある（明るさや発光の色など）．このような LED 電球をワンボードコンピュータから制御することで，遠隔に情報を伝達するカバートチャネルを形成することが可能なことを実験により示した．

実験システムは，送信側に LED 電球を用いている．この電球は明るさのレベルを 25 段階しか表現できず，また制御の速度は一秒あたり 10 コマンドを処理可能である．また受信側には照度-周波数変換デバイスを一般向けの望遠鏡と組み合わせている．

送信側，受信側ともに一般に入手可能な，決して高性能とは言えないデバイスを組み合わせて試作されたが，形成されたカバートチャネルは，情報を 100m 以上の遠隔地にまで到達可能であるという結果を得ている．

Shamir 先生の登壇は今回の IEEE Euro S&P においても目玉の一つであり，初日朝に時間が設けられた点でもそれは分かる．結果，多くの聴衆を集めたが，先生はその後の本会議においても会場の最前列に座られて，質疑においても活発な質問をされ，会議の活性化に一役かわれていた．

2.5 Posters

ポスターセッションは会期初日の夕方に行われた（図 4）. 計 18 件のポスターが展示されたが，各ポスターの概略は, IEEE Euro S&P のウェブページから閲覧可能である[3].

2.6 Short Talks

会期二日目午後の Short Talks のセッションは，一件数分の持ち時間でライトニングトークスのような要領で発表が行われた．

プログラムについては，暫定版が[4]に掲載されているが, これに飛び入り参加が加わることで, 研究成果の発表の他, 研究会などの Call for Participation など多岐にわたる内容となった．以下そのうちのいくつかを紹介する．

(1) "Let's Face It: Faceted Values for Taint Tracking", Musard Balliu, Daniel Schoepe (Chalmers), Frank Piessens (KU Leuven), Andrei Sabelfeld (Chalmers)

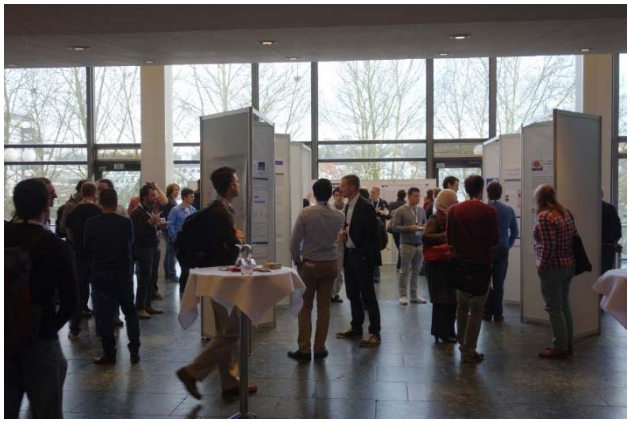

図 4 ポスターセッションの様子

Taint tracking に関する発表．Taint Tracking では各変数について taint status を持たせ taint を追跡する．しかしポインタや配列処理の際の追跡は困難であることから，Faceted Value を用い，セキュリティレベルに応じて処理を行う方式を提案している．

(2) “No Need for Black Chambers: Testing TLS in the E-mail Ecosystem at Large",Wilfried Mayer, Aaron Zauner, Martin Schmiedecker, Markus Huber (SBA-Research)

E-mail におけるトランスポート層セキュリティの使用状況に関するサーベイ結果の報告．

ネットワークスキャンツール masscan を用いて IPv4 アドレス空間全体のメールサーバーをスキャンし，使用されているプロトコルを調査した．最も多く使われているのが TLSv1 であること，SSL v2 や v3 も使われているという結果を得ている．

(3) “Usability and Security of Text and Click-Based Graphical Passwords: User Study on Adolescents”, Omar Al-Megren, Abdullah Bin Suwaydan, Yazeed AlBednah, Mansour Alsaleh (Abdulrahman Alarifi King Abdulaziz City for Science and Technology, Riyadh, KSA)

ユーザにクリック入力を求めて認証を行うグラフィカルな認証方式は，例えば Windows 8 で採用されたピクチャパスワードなどで既に実用化されている．一方で，テキストパスワードによる認証も依然として多く使われており，本発表は両方式を実験により比較している．学生被験者を 2 グループに分け，両方式についてそれぞれ長期記憶/短期記憶に分けて試験を行っている．

この結果，短期記憶では両者の間の recall 率の違いはほぼないこと，長期記憶ではテキストパスワードの方が優れることが判明したと結論付けている．

2.7 TC Business meeting

Short Talks に続いて催された TC Business meeting の時間は，その名前から想像されるようなクローズドな運営会議ではなく，今後の Euro S&P 運営方針についての情報の参加者全員とのシェアの時間であり，通常セッションと同じ大ホールで催された．

それによれば，Euro S&P は今後欧州各地での開催を想定していること，ワークショップの併催も考えており，併催ワークショップを募集していること，次回開催はフランスのパリで，INRIA を中心にオーガナイズされることが示された．

開催時期は 3 月中旬から 4 月下旬との考え方も示されたが，次回の開催日は未定とのことである．EUROCRYPT との連携も視野に入れているとのことである．

3. 発表論文

3.1 “Explicit Secrecy: A Policy for Taint Tracking, Daniel Schoepe”, Musard Balliu (Chalmers University of Technology), Benjamin C. Pierce (University of Pennsylvania), Andrei Sabelfeld (Chalmers University of Technology) [6]

Information Flow セッションでの発表であり，テイント追跡のポリシイについての研究．テイントトラッキングはデータフローを追跡する手法として一般的だが，当該発表では，テインティングの意味論的アプローチを採用し，テインティングが具体化するセキュリティポリシイは何かという問題を扱う．発表では明示的秘匿性（Explicit Secrecy），即ち明示的フローの本質を扱う汎用フレームワークを提案している．このフレームワークはテインティングの健全性の規範を形式化するこれまでの構文的アプローチを一般化した意味論的なものである．

発表ではシンプルな高水準命令型言語と，理想化された RISC マシンの双方を用い，このフレームワークの有効性を示している．テイントトラッキングツールで何ができるかを更に理解するために，動的/静的双方に，ポピュラーな動的/静的テイントトラッカー群のテインティングエンジンコアについて明示的秘匿性に関する健全性を調査した．

3.2 HornDroid: Practical and Sound Static Analysis of Android Applications by SMT Solving, Stefano Calzavara (Universita Ca' Foscari Venezia), Ilya Grishchenko, Matteo Maffei (CISPA, Saarland University)

Information Flow セッションでの発表であり，Android アプリケーションの情報フローの静的解析に関する研究．静的検証のための新たなツール HornDroid を提案している．

Android アプリケーションのセマンティクスを，Horn 節を用いて抽象化し，セキュリティに関するプロパティを SMT ソルバーで解ける証明問題群として表現する．SMT ソルバーは近年，急激な発展を遂げており，実行速度に関して大幅な短縮に成功していることから，これを利用して実行時間を短縮せしめることに成功している．

Horn 節と SMT ソルバーを組み合わせるというアイデアにより，既存の静的解析ツールに対してベンチマークによる比較で優れていることを示した．

評価方法としては，静的情報フロー解析ツールの評価用として 120 のアプリケーション群を集約したベンチマーク DroidBench [7]を用い，AmanDroid [8], DroidSafe [9], IccTa [10]らとの解析精度の評価で優れた結果を得ている．

また代表的な Android アプリケーションマーケットである Google Play から，ポピュラーな大規模アプリケーション複数を入手し，64 コア CPU と 758Gb メモリを備える計

算機にかけて解析を行った結果,(他の解析ツールに対して短い）数十分で解析を完了したとしている．

3.3 Games Without Frontiers: Investigating Video Games as a Covert Channel, Bridger Hahn, Rishab Nithyanand, Phillipa Gill, Rob Johnson (Stony Brook University) [11]

Information Flow セッションの発表．秘匿通信方法の中でも，特に，政府などの権力による検閲から逃れるための，カバートチャネル通信に関する研究．政府によるメディアに対する検閲を用いた取り締まりを回避するために，ビデオゲームを新しいカバートチャネルとして用いる方法を提案している．

検閲を回避するカバートチャネルを構築するにあたって大きな問題は，ただ通信内容を秘密にする必要があるだけでなく，秘密の通信を行っていることを検閲者に悟られてはならない点である．この為秘匿通信とは別の通信を行うチャネルに，秘匿すべき内容を乗せて通信することになるが，このためにオンラインゲーム通信を用いるのが適しているとの主張である．

著者らは，カバートチャネルを用いられている事を検閲者に知られた場合は，直ちに当該チャネルを閉じて別のカバートチャネルを用いることを主張し,この前提を受けて，カバートチャネルを使い捨てにするために，カバートチャネル設定のコストをいかに低廉なものにするかという観点からコンピュータゲームに着目している．ここ著者らの着眼点として新しい点である．

カバートチャネルとしてコンピュータゲームを用いる利点として，ジャンル内のゲームは共通したフィーチャを多く持っていること．次に，ゲームは何種類もあり，それぞれが専用のプロトコルとサーバインフラを持っていることを挙げ，これらのフィーチャは，同一ジャンル内の複数のゲームに適合する単一のフレームワークを構築することで，カバートチャネルを切り替えることで即座に，かつ低廉に検閲回避を可能となるとしている．

発表では三つのリアルタイムストラテジゲームにこの提案方式を実装し，このアプローチの実現可能性をデモしている．

3.4 Translingual Obfuscation, Pei Wang, Shuai Wang, Jiang Ming, Yufei Jiang, Dinghao Wu (The Pennsylvania State University) [12]

Security Protocol セッションでの発表であり，プログラム難読化に関する新手法の提案に関する研究．

プログラム難読化に対する新しいアプローチとして，トランスリンガル（translingual）難読化と呼ばれる手法を提案している．これは，プログラムの一部を，オリジナルのプログラミング言語から（異なるプログラミングパラダイムに基づく）異なるプログラミング言語によるプログラムに変換させるものであり，これを BABEL と呼んでいる．

論文中では，C 言語により記述されたオリジナルプログラムを Prolog 言語のプログラムに変換させる．
Prolog の持つ，ユニフィケーションとバックトラッキングを活用するようプログラム変換を行うことで，オリジナルプログラムのデータレイアウトと制御フローの難読化を実現し，リバースエンジニアリングを阻止することを意図している．

評価においては，Collberg ら [13] の 4 つの指標（porncy, resilience, cost, stealth）に基づき，商用難読化ツールと比較してリーズナブルなコストで効率的なソフトウェア難読化を実現していることを確認している．

3.5 Strong and Provably Secure Database Access Control, Marco Guarnieri (ETH Zurich), Srdjan Marinovic (The Wireless Registry), David Basin (ETH Zurich) [14]

OS & Database Security セッションでの発表．既存の SQL データベースのアクセス制御メカニズムは極めて制限が強い一方，攻撃者はこのデータベース制御システムの高度な機能であるビュー，トリガ，インテグリティ制約などを活用し，自身の権限を昇格させ，情報漏洩などを引き起こすことができる．

著者らは，これは現在のベンダの怠慢というだけではないとしている．

更に，データベースセキュリティの理論的基礎には適切なセキュリティ定義と現実的な攻撃者モデルが掛けており，そのどちらも現代のデータベースのセキュリティ評価に必要とされていると主張し，これらの問題を指摘し，ポピュラーな SQL データベースシステムの攻略を図る攻撃者から守るセキュアなアクセス制御メカニズムを証明したとしている．

この概念は PostgreSQL をベースとするプロトタイプとし実装されている．

3.6 NavigaTor: Finding Faster Paths to Anonymity, Robert Annessi (TU Wien), Martin Schmiedecker (SBA Research) [15]

Privacy セッションでの発表であり，タイトルの通り Tor（The Onion Router）に関する発表である．

Tor はその実現方式故に，通信遅延の大きさと帯域の狭さという二つの課題を抱えている．当該発表では，この二点は近年改善されてはいるものの依然として大きな問題であるとして，改善のための性能測定と性能改善方法の提案を行っている．

NavigaTor と名付けられた提案方式はカスタム Tor パスジェネレータを含む性能測定ソフトウェアであり，発表では，Tor ネットワークの大規模性能測定を行う最初のものと主張している．

同ソフトウェアはまず, 既存の Tor パスジェネレータの，パス選択アルゴリズムはそのままにして若干の変更を加え，秘匿性については論理的に等価なパスジェネレータの実装であり，Tor ネットワークに負荷をかけずに 1 日あたり数百万の回線を構築，評価できる測定器である．

性能改善手法として, NavigaTor は回線 RTT（Circuit RTT）と，事前に作成した RTT の分散に基づき，遅い，破棄すべき回線を特定する．

回線 RTT に基づく方式は CBT（Circuit Build Time）に基づく手法，リンク RTT に基づく手法よりもエンドツーエンドのネットワーク遅延とスループットを改善せしめることを示した．

評価においては PlanetLab 上の複数ホストに NavigaTor ソフトウェアを配備し，効果を評価している．

また CBT と回線 RTT を組み合わせることで，回線 RTT 単独での適用よりも遅延を改善できるという評価結果も得ている．

更に，輻輳検知方式（Congestion-aware scheme）の性能改善効果が，現在の Tor ネットワークに対しては，エントロピーを大幅に減少せしめるのに対する効果としてはわずかであることと，同方式の統計的近似を CBT や回線 RTT において用いることで，エントロピー減少を抑制可能な一方で性能を大きく改善できることを示している．

3.7 ZETA - Zero-Trust Authentication: Relying on Innate Human Ability, not Technology, Andreas Gutmann (Technische Universität Darmstadt), Karen Renaud, Joseph Maguire (The University of Glasgow), Melanie Volkamer, Peter Mayer (Technische Universität Darmstadt), Kanta Matsuura (University of Tokyo), Jörn Müller-Quade (Karlsruhe Institute of Technology) [16]

Security & Learning セッションでの発表. ユーザの記憶負担軽減を狙った質問応答型の認証プロトコルを提案している．通信路やデバイスが信用できなくても利用できるようにするという設計方針であることから、ZeTA (Zero Trust Authentication on untrusted channels)と命名された．

質問と応答の関係は意味論的なものであり，秘密情報の例として“Red OR Bike”，質問の例として“Can any of your terms be used as a means of transportation?”が説明に使われた．論文では，フォーマルなモデルが定義された後，プロトコルの提案と評価が示されている．

理論的評価では，事前観測をせず実行時に正解を推測する攻撃，覗き見に相当する行為を許され機械学習を使う攻撃，保存されている秘密情報に対する攻撃の 3 種類の受動的攻撃に関して安全性が考察されている．

実験的評価では，188 名の被験者に対して，最多で 30 回の質問応答を繰り返してユーザビリティが評価されている．能動的攻撃に対する安全性の評価は，今後の課題とされている．

3.8 It Bends but Would it Break? Topological Analysis of BGP Infrastructures in Europe, Sylvain Frey, Yehia Elkhatib, Awais Rashid, Karolina Follis, John Vidler, Nick Race, Chris Edwards (Lancaster University) [17]

Network Security セッションでの発表. インターネットの根幹をなすネットワークインフラの中でも，BGP（Border Gateway Protocol）による接続網のセキュリティを，特に欧州における実態に基づいて分析を加えた発表である．

当該発表では，BGP の脆弱性を含めた，インターネットインフラへの攻撃ベクターに関する包括的な脅威モデルを構築し，次に，欧州をカバーする地域インターネットレジストリ RIPE（Reseaux IP Europeens）の持つグローバル経路情報 RIS（Routing Information Service）から入手できるデータ群に基づいて, 欧州の BGP バックボーンのマップを構築した．

論文ではバックボーンのトポロジの解析と異なる種類の攻撃の結果起こり得る複数の混乱シナリオを，攻撃の種別ごとに作成し，また既存の被害軽減および回復手法についても論じ，頑健性とレジリエンスの改善手法を提案している．

分析の結果，BGP インフラストラクチャは，長年に渡るアドホックな拡張の結果，既に認識されているものよりも高いリスクに曝されていると結論付けている．

またトポロジ上の改善策を評価するため，バックボーンネットワークのトポロジのコア AS とそれ以外のバックボーンとの間のリンク間のリンク追加，バックボーン内のコア AS の数の増加および両者の組み合わせについてシミュレーションを行っている．

本発表は，BGP ネットワークの実態に関する包括的なセキュリティ分析としては極めて貴重な研究と思われた．

3.9 AppScanner: Automatic Fingerprinting of Smartphone Apps From Encrypted Network Traffic, Vincent F. Taylor (University of Oxford), Riccardo Spolaor, Mauro Conti (University of Padua), Ivan Martinovic (University of Oxford) [18]

Network Security セッションでの発表であり，スマートフォンアプリケーションのフィンガープリンティングに関する研究．

スマートフォンアプリの自動フィンガープリンティングは，例えばスマートフォン端末ユーザやアプリケーション開発者，アプリケーション配布業者など様々なステークホルダが活用しうると同時に，攻撃者にとっても悪用されうる技術である．例えば，当該技術を用いて端末にインストールされたアプリを調べることに成功すれば，これを元に端末の潜在的脆弱性に関する情報を得ることができる．

しかし，アプリケーションフィンガープリンティング技術は，アプリケーションの種類の多さ，インストール可能な端末の広範さ，またインストールに用いられるネットワークプロトコルが HTTPS/TLS などで暗号化されることなどから，困難さが増している．

本発表では新しいアプリケーションフィンガープリンティング技術として，AppScanner と名付けたフレームワークを提案している．これは，暗号化されたネットワークトラヒックから Android アプリのフィンガープリンティングを行うものである．

このフレームワークは端末上で動作し，ネットワークトレースを取得し教師有り機械学習を行うことでアプリケーションを識別する．当該フレームワークはネットワーク上トラヒックが暗号化されていても機能すると主張しており，Google Play の最もポピュラーな 110 のアプリをプロファイル化した評価では，99%の精度で再アイデンティファイに成功したと述べている．

3.10 How Secure is TextSecure? Tilman Frosch, Christian Mainka, Christoph Bader, Florian Bergsma, Jorg Schwenk, Thorsten Holz (Ruhr-Universitat Bochum) [19]

Protocol　Analysis セッションでの発表．インスタントメッセージにおけるセキュリティ，プライバシについての研究である．

メッセージの秘匿性を訴求するインスタントメッセージングアプリケーションについては，Treema，Surespot，TextSecure などが存在する．このうち Android 端末用のアフターマーケットファームウェアとして広く知られている Cyanogenmot にはインスタントメッセージングアプリケーションとして TextSecure が含まれており，セキュリティの高さが注目を集めている．

当該アプリケーションの暗号プロトコルはオリジナルの設計になっており，当該プロトコルは後継アプリケーション Signal でも利用されていることから，本研究では当該プロトコルのセキュリティについて検証を加えている．,暗号プロトコルのモデル化と，三つの主要コンポネント（鍵交換，鍵導出，暗号処理）の解析を行い，秘匿性の検証を行っている．

4. まとめ

本稿では，ドイツのザールブリュッケンにて催された第一回 Euro S&P の概要を報告した．来年はフランスパリにて開催（ただし開催日は未定）とのことである．

謝辞　本発表の一部は JPSP 科研費 26330169 の助成を受けています．

参考文献

[1] “IEEE European Symposium on Security and Privacy 2016（Euro S&P）”. http://www.ieee-security.org/TC/EuroSP2016/index.php (参照 2016-06-10).
[2] Eyal Ronen and Adi Shamir. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016. p3-12.
[3] “IEEE European Symposium on Security and Privacy 2016 Poster Program”. http://www.ieee-security.org/TC/EuroSP2016/program-posters.php, (参照 2016-06-10).
[4] “IEEE European Symposium on Security and Privacy 2016 Poster Program”. http://www.ieee-security.org/TC/EuroSP2016/program-posters.php, (参照 2016-06-10).
[5] “IEEE European Symposium on Security and Privacy 2016 Short Talks Program”. http://www.ieee-security.org/TC/EuroSP2016/program-short_talks.php. (参照 2016-06-10)
[6] Schoepe, D., Balliu, M., Pierce, B. C. and Sabelfeld, A. Explicit secrecy: A policy for taint tracking. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016. p15-30.
[7] Arzt, S., Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J.and McDaniel, P. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. In ACM SIGPLAN Notices (Vol. 49, No. 6, pp. 259-269). 2014. ACM.
[8] Wei, F., Roy, S., & Ou, X. Amandroid: A precise and general inter-component data flow analysis framework for security vetting of android apps. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 1329-1341). 2014. ACM.
[9] Gordon, M. I., Kim, D., Perkins, J. H., Gilham, L., Nguyen, N. and Rinard, M. C. Information Flow Analysis of Android Applications in DroidSafe. In NDSS. 2015..
[10] Li, L., Bartel, A., Bissyandé, T. F., Klein, J., Le Traon, Y., Arzt, S. and McDaniel, P. IccTA: Detecting inter-component privacy leaks in Android apps. In Proceedings of the 37th International Conference on Software Engineering-Volume 1 (pp. 280-291). 2015. IEEE Press.
[11] Bridger Hahn, Rishab Nithyanand, Phillipa Gill and Rob Johnson. Games Without Frontiers: Investigating Video Games as a Covert Channel, In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.
[12] Pei Wang, Shuai Wang, Jiang Ming, Yufei Jiang and Dinghao Wu, Translingual Obfuscation, In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.
[13] Collberg, C., Thomborson, C., & Low, D. Manufacturing cheap, resilient, and stealthy opaque constructs. In Proceedings of the 25th ACM SIGPLAN-SIGACT symposium on Principles of programming languages (pp. 184-196). ACM.
[14] Marco Guarnieri, Srdjan Marinovic, David Basin, Strong and Provably Secure Database Access Control, In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.
[15] Annessi, R., & Schmiedecker, M. (2016, March). NavigaTor: Finding Faster Paths to Anonymity. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 214-226). 2016. IEEE.
[16] Gutmann, A., Renaud, K., Maguire, J., Mayer, P., Volkamer, M., & Matsuura, K. ZeTA-Zero-Trust Authentication: Relying on Innate Human Ability, Not Technology. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016, (pp. 357-371).
[17] Sylvain Frey, Yehia Elkhatib, Awais Rashid, Karolina Follis, John Vidler, Nicholas Race, Christopher Edwards. It Bends but Would it

Break? Topological Analysis of BGP Infrastructures in Europe, BGP. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.

[18] Taylor, V. F., Spolaor, R., Conti, M., & Martinovic, I. Appscanner: Automatic fingerprinting of smartphone apps from encrypted network traffic. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE. 2016, (pp. 439-454).

[19] Tilman Frosch, Christian Mainka, Christoph Bader, Florian Bergsma, Jorg Schwenk and Thorsten Holz, How Secure is TextSecure? In 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE. 2016.