FCS-ARSPA'07 参加報告

米山 一樹
太田 和夫

The University of Electro-Communications

会議概要

- 開催地：ポーランド（ヴロツワフ）
- 日程：7/8開催（ICALP・LICSと併設）
- 参加者数：30人弱？

会議概要

- **会議のスコープ**
  - *“The FCS-ARSPA’07 workshop brought together researchers and practitioners who are working on the foundations of computer security and on the development and application of automated reasoning techniques and tools for the formal specification and analysis of security protocols.”*

- **プログラム**
  - 9件＋招待講演1件（投稿13件）
  - 国別内訳
    アメリカ：3件，フランス：3件，
    イギリス：1件，日本：1件，
    トルコ：1件，スイス：1件

講演の（大まかな）分類

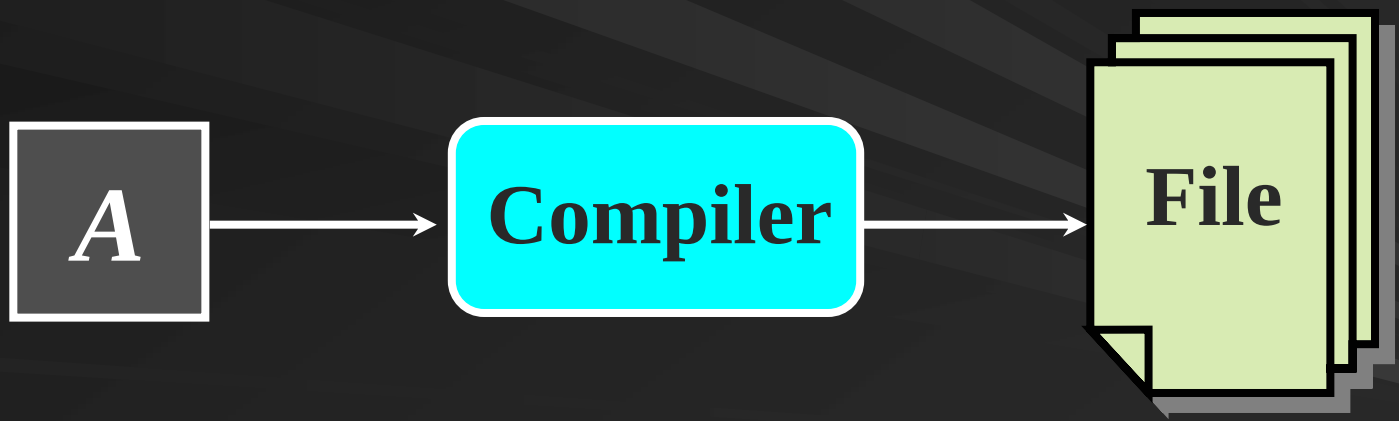
- 新たな解析手法に関する提案
  - 最小特権環境での権限解析，帰納的定理証明の応用，秘匿性検証の計算量解析
- 既存プロトコルの安全性解析
  - Bluetoothデバイス用認証，アドホックルーティング，Diffie-Hellman鍵交換
- 解析結果に基づく新たなプロトコルの提案
  - 匿名鍵管理，位置推定
- 理論的な概念拡張
  - 推論可能性と識別不可能性，メッセージ情報量の定義

新たな解析手法に関する提案

Authority Analysis for Least Privilege Environments

(Toby Murray, Gavin Lowe)

- アクセスコントロールシステムにおける最小権限環境での権限解析の定式化
  - CSPベース → FDRなどのモデルチェッカーで自動解析可能
  - 検出可能になった攻撃の例：Confused Deputyシナリオ



アクセス権限の無いFileにcompilerを利用してアクセスする攻撃

Deciding knowledge in security protocols for monoidal equational theories

(Stephanie Delaune, Veronique Cortier)

- 等式理論における推論可能性（一方向性）と識別不可能性の一般的な扱い方の提案
  - 「攻撃者の知識」の拡張
    既存研究：代数的な結合性・可換性で表現

モノイド理論を導入することで**準同型性**などを攻撃者の知識として扱えるようにした

Secrecy Checking of Protocols: Solution of an Open Problem

(Zhiyao Liang, Rakesh Verma)

- 暗号プロトコルの秘匿性検証の計算量における未解決問題
  - **計算量下界**は決定可能か？

→ あるクラスのプロトコルでは決定不可能であることを証明

		Bounded role instance num.	Unbounded role instance num.	
			Bounded total ∃ from regular agents	Unbounded total ∃ from regular agents
I with unbounded ∃	$\neq$	NPC	???	Undec.
	$=$	NPC	DEXPC	Undec.
I with no ∃	$\neq$	NPC	DEXPC	Undec.
	$=$	NPC	DEXPC	Undec.

既存プロトコルの安全性解析

Formal Analysis of Authentication in Bluetooth Device Pairing

(Richard Change, Vitaly Shmatikov

- 検証ツールProVerifを用いたBluetooth用認証プロトコルの安全性解析
  - 解析対象：
    「流れているメッセージを参加者が観察できるような通信路上」での認証付鍵交換プロトコル
  - 今回分かったこと：
    多重同時実行時における**認証機能の欠陥**を検出．
  - 副産物：
    「**人間が**認証できる通信路」のformalな定式化

Automated Security Analysis of Ad Hoc Routing Protocols

(Todd Andel, Alec Yasinsac)

- SPINモデルチェッカーを用いたアドホックルーティングプロトコルの自動解析
  - モバイルアドホックルーティング（MANET）のモデル化

    • 通信路
    • ソースルーティング
    • 能動的攻撃者

  - Secure Routing Protocol（SRP）の解析

    経路発見攻撃に対して安全（だと思われていた）

    ⇒ モデル化した攻撃者で脆弱性を検出

(Kazuki Yoneyama, Yuichi Kokubun, Kazuo Ohta)

- Task-PIOAフレームワークを用いた安全性解析
  - Case studyの開拓
    既存研究：紛失通信とゼロ知識証明のみ
    → Diffie-Hellman鍵交換
  - 強い攻撃者モデルの適用
    既存研究：非適応的攻撃者のみ
    → 適応的攻撃者の定式化
  - Task-PIOA用に新たに定式化したDDH仮定と従来の定義の等価性証明

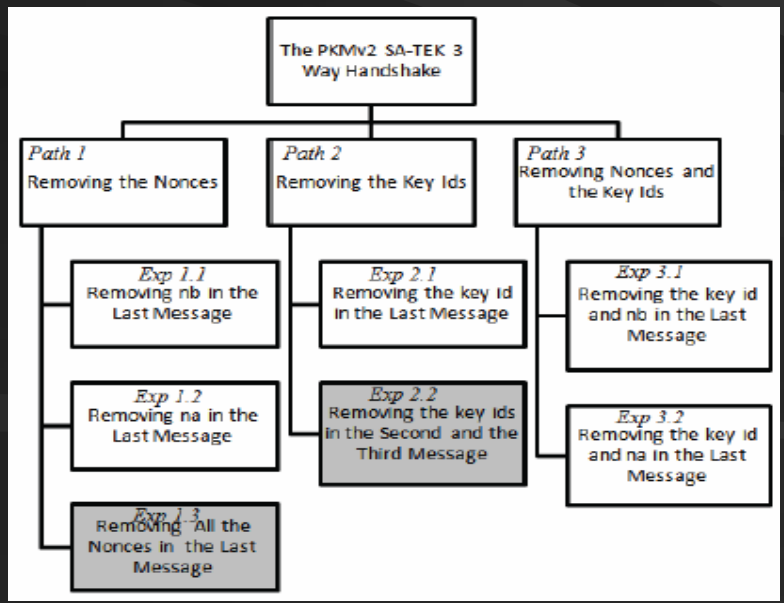
解析結果に基づく
新たなプロトコルの提案

A Secure Simplification of the PKMv2 Protocol in IEEE 802.16e-2005

(Ender Yuksel, Hanne Riis Nielson, Christoffer Rosenkilde Nielsen, Mehmet Bulent Orencik)

- IEEE 802.16e-2005標準化における匿名鍵管理プロトコルPKMv2の単純化
  - LySa計算でモデル化＆解析

⇒ **安全性に寄与しない部分を削除**



From Sec. Navi. Systems to Securing Wireless Communication Through Location-Awareness

(Srdjan Capkun)

- ワイヤレスデバイスの安全な位置推定・位置検証プロトコルの紹介
  - Gallileo, GPSなどに対する攻撃例

    成りすまし攻撃
    位置誤認攻撃
  - SecNavの提案

    ・ビーコンベースで構成
    ・既存の攻撃に対する安全性を証明
  - 応用：事前共有鍵無しの認証通信

理論的な概念拡張

Verifying Regular Trace Prop. of Sec. Protocols with Explicit Destructors and Implicit Induction

(Adel Bouhoula and Florent Jacquemard)

- 内在する帰納的定理を自動証明する方法に基づいた新たな暗号プロトコルの検証手続きの提案
  - 解析例：
    Denning-Saccoの鍵配送プロトコル
    セッション鍵の秘匿性，認証機能の欠陥を検出可能

The Meaning of a Cryptographic Message via Hypothetical Knowledge and Provability

(Simon Kramer)

- AbadiとNeedhamの第1原理
  - *“Every message should say what it means: the interpretation of the message should depend only on its contents.”*

- 暗号学的メッセージの“意味”についての外延的定義
  - コンテンツに基づいたメッセージの情報量を定式化

実際に解析可能なAbadiとNeedhamの第1原理の定式化を与えたことに相当

まとめ

- 具体的なプロトコル解析の話から概念拡張の話まで様々な発表が行われた．
- いわゆる「暗号理論的な」セキュリティを論じた発表はあまり見られなかった．
- Informal proceedingが会議のHPにおいて公開されている．

  “http://profs.sci.univr.it/~vigano/fcsarspa07/fcs-arspa07.pdf”