YNU

自動車セキュリティ技術の研究と教育における先端実験車両の活用

2014年7月1日

松本　勉
横浜国立大学大学院環境情報研究院
横浜国立大学　情報・物理セキュリティ研究拠点

講演概要

YNU

- 自動車に関わるイノベーションの展開が期待される中、自動車そのものや自動車を含むシステムの情報・物理セキュリティの強化は重要な課題であると広く認知されている。例えば、車載LANに関するセキュリティ技術の研究開発は既に盛んになっている。
- これらには、（1）通信内容の暗号化や、認証子やディジタル署名による認証機能の追加などの暗号技術の活用、（2）通信データの監視による不正検出、（3）CANのエラーフレームの機構を利用した不正送信の阻止などがある。
- このような研究を大学で本格的に行い、真に実力があり頼りになる人材を育てるには、自由に使えるリアリティのある対象システムと関連する研究支援システムが必要である。本講演では、RoboCar PHV やRovoCar MV などを活用した、横浜国立大学における情報・物理セキュリティに関する最先端研究教育事例を紹介する。

情報・物理セキュリティという考え方 YNU

- 情報セキュリティ／物理セキュリティ　だけ？

情報・物理セキュリティ
＝　情報セキュリティ　U　情報と物理の絡むセキュリティ　U　物理セキュリティ

情報を担う媒体

情報を扱うシステム

- 情報のセキュリティは、それを扱う物理的実体を伴う機器やシステムのセキュリティと一体のものとして捉えることが望ましいケースが多い。
  - ✓ ICチップ、モバイル機器、車、端末、設備、建物、サーバ、データセンタ、情報ネットワーク、電力ネットワーク、インフラ、環境、人間、社会、・・・・・
  - ✓ つまり、**組込みシステムを意識しよう！　研究者にとっては宝の山！**
  - ✓ 量子＊＊・・・ももちろん。

【情報・物理セキュリティ解析力強化プログラムの展開】<環境情報研究院／学府>

IPS Research

YNU

従来のセキュリティ教育

コンピュータネットワーク
運用・インシデント対応・
ソフトウェア中心

横浜国立大学
の教育計画

補完

今までにない
「ハードウェアを含む」
セキュリティ教育

情報・物理セキュリティ解析力の高いハイエンド人材への公的機関・民間組織からの強いニーズ。
横浜国立大学の四半世紀余にわたる圧倒的研究成果（次ページ）の強みを生かす。

「情報・物理セキュリティ解析力強化プログラム」

リアリティのある解析演習が必須

自由に解析して構わない**解析対象システム**と

解析支援システムからなる設備を開発し導入することが必須！

活用

関連機関・企業・大学等と
のネットワークでも活用

- 情報のセキュリティは、それを扱う**物理的実体を伴う機器（ハードウェア）やシステムのセキュリティと一体のものとして**捉える必要がある。これを指し示すために「**情報・物理セキュリティ**」というキーワードが用いられる。
- 「**セキュリティ解析力**」とは、対象の情報・物理セキュリティの本質を見抜く直観力・技術力を意味する。基盤的知識の上に**実践的なセキュリティ解析の経験を通してはじめて養成できる。**

そのためには、コンピュータネットワーク・ソフトウェアだけでなく、ハードウェアを含めた、リアリティのある対象上で経験を積むことが有効。

しかし、機器が、実製品であり、実運用されているものであったら、解析を自由に行うターゲットとしては適当でない！

情報・物理セキュリティの代表的研究実績例

YNU

- **暗号モジュールのセキュリティ評価**

  暗号技術を実装したICカード等の暗号モジュールの消費電力や漏洩電磁波等のサイドチャネル情報を活用してモジュール内の鍵などを暴くサイドチャネル攻撃、および、不正クロック信号の入力、レーザ照射などに対する振る舞いを観察して鍵などを暴く故障利用攻撃の、評価技術と対策技術についての拠点。関連する試験／評価／認証制度の構築と運営も支援。

  国際暗号学会理事。暗号ハードウェア国際会議開催。平成24年9月、第3回DPAコンテスト（暗号モジュールに対する電力差分攻撃所要波形数の最小値を競うテレコムパリテック大学（フランス）と産業技術総合研究所（日本）が共同主催したコンテスト）にて優勝。ELEX Best Paper Award in the Year 2012 受賞。

- **バイオメトリクス**

  指紋照合技術が精巧な人工指による攻撃されうるという結果はNature誌をはじめ多数のメディアを通じて世界的に衝撃を与えた。バイオメトリクス（生体認証技術）のセキュリティ評価に内外の機関から知見を求められることも多い。

  平成22年度文部科学大臣表彰科学技術賞（研究部門）、平成18年度ドコモ・モバイルサイエンス賞大賞を受賞。

- **人工物メトリクス**

  人工物の個体に固有のランダムな物理的パタンをベースに個体識別を行う技術を人工物メトリクスと命名し研究。磁性微細繊維を用いた方式は株券の真贋判定にも実用された。日本銀行とも共同研究。ナノ構造を用いた画期的人工物メトリクスにおいては、第26回先端技術大賞（平成24年度）フジサンケイビジネスアイ賞を受賞。

- **自動車等の制約の多いシステムに対する実用的セキュリティ技術**

  制約条件の多い組込みシステムに対する情報理論的セキュリティ技術の現実的適用を推進。

  車載ネットワークCANでは、不正送信の検出だけでなく阻止ができる画期的事実を発見。

  自動車などの機器への組込みシステム向けの学術的セキュリティ研究の拠点。

横浜国立大学のポテンシャル

横浜国立大学は四半世紀余にわたり一貫して情報・物理セキュリティ分野をリード：研究面で世界初・第１級の成果。修士10名/年、博士1～2名/年を輩出。博士は日本の公的組織・民間部門を支える存在。セキュリティ分野研究で一般からも認知。平成23年12月に横浜国立大学「情報・物理セキュリティ研究拠点」を設置。 http://ipsr.ynu.ac.jp/

【教育研究内容：方法論】
情報・物理セキュリティ解析力強化プログラム

YNU

攻撃者・対策者の立場からの解析を徹底して行う

解析者
（模擬攻撃者・
対策考案者）

指導

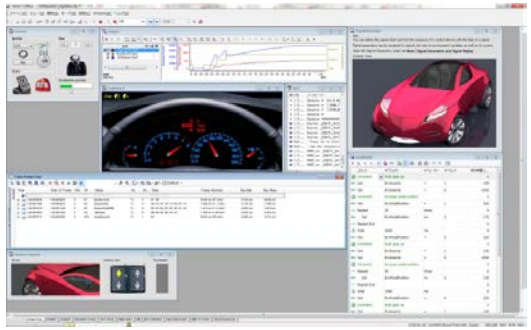
対象システムの
エキスパート
および担当教員

リアリティがあり
自由に解析してよい
対象システム

例：対策技術検証用車載ネットワーク実験装置

解析／
攻撃例

- インスツルメンタルパネルの表示の変更
- ブレーキの無効化などの運転者が意図しない動作
- 外部からドアの解錠やエンジンの始動
- 外部に位置情報や車内の会話を送信

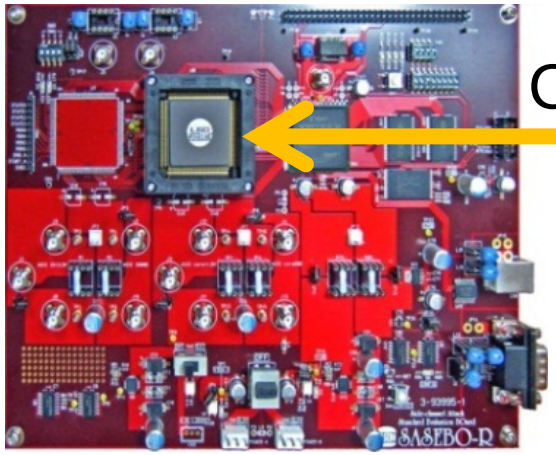


例：車載ネットワークのシミュレータ

解析支援
システム例

【参考】 暗号モジュール

YNU



SASEBO-GII for FPGA

SASEBO-R for ASIC Crypto LSI

“Side-Channel Attack Standard Evaluation Board”

- Originally Developed by AIST funded by METI
- Based on Pilot Project INSTAC-8 and INSTAC-32 by JSA/INSTAC
- Widely distributed for Researchers and Evaluation Laboratories
- Many academic papers did emit results based on SASEBO

【準備段階を経て本格実施開始・展開】
情報・物理セキュリティ解析力強化プログラム

YNU

準備「H23-24年度・学内重点化競争的経費による、セキュリティ解析演習カリキュラム開発」

例①「不正プログラム・ネットワーク侵入の解析」のために、仮想マシン技術により多数のコンピュータを実装し、不正プログラムを動作させる計算機を多数利用する形態のシステムを開発。情報工学が専門の学生を対象に演習を実施。

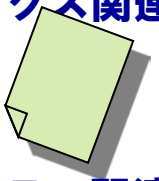
例②「暗号ソフトウェアのセキュリティ解析」の目的で、既設の一般的なソフトウェア開発環境を用いて、改竄が困難な耐タンパーソフトウェアを開発し解析する技術の実践的教育カリキュラムを、ソフトウェアセキュリティの専門家と共に開発した。

本格設備導入

（１）暗号ハードウェア関連

（２）自動車関連

（３）バイオ・人工物メトリクス関連



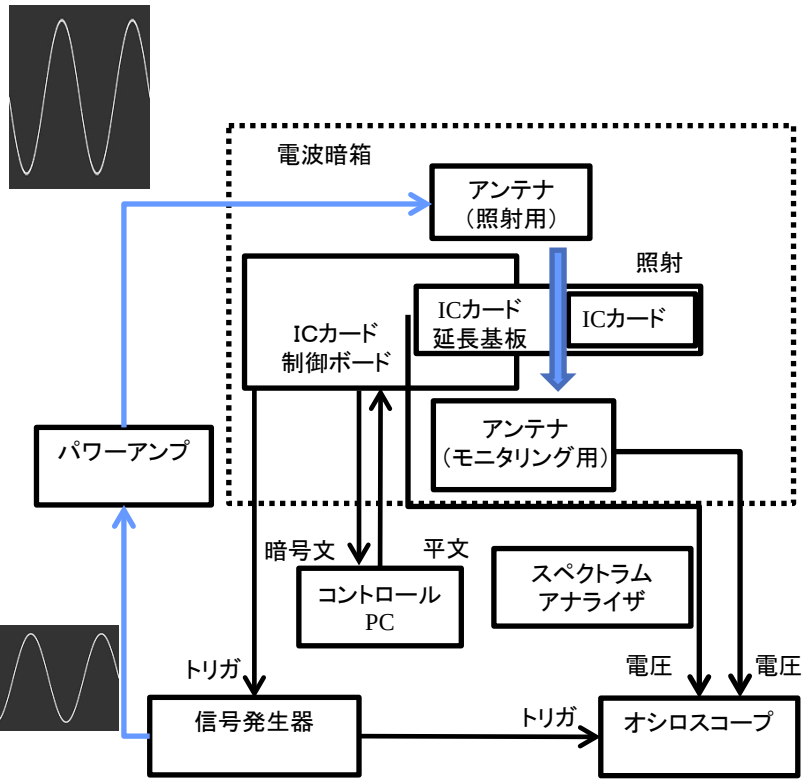
（４）ネットワークセキュリティ関連

★リバースエンジニアリングに関する制約や、実際に運用されているシステムに対する解析行為が不正行為とされるおそれから、本格的教育研究には困難が伴う。
★しかし、文科省予算および学内重点化競争的経費によりH25年度に導入した本格的設備により、いくつかのテーマにおいてはこの困難性が軽減され、真に実力を有する人材を育成することを目指した挑戦的な「**情報・物理セキュリティ解析力強化プログラム**」を効果的に実施することが可能となった。さらに展開したい。

（事例紹介）

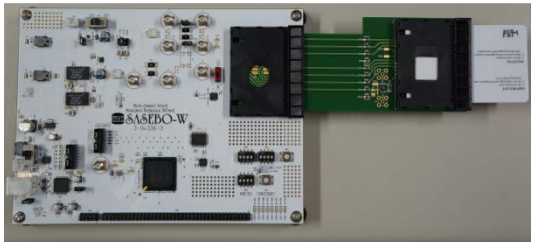
暗号ハードウェア（ICカード、ICチップ）解析支援システム

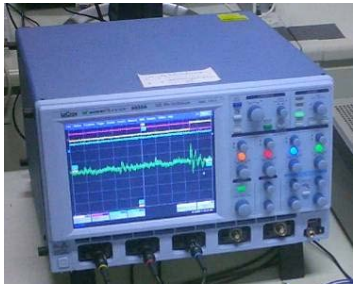
- ICチップやICカードは、各種のサービスのセキュリティを支える重要構成要素であり、暗号技術を実装した暗号モジュールである。
- 動作中の消費電力や漏洩電磁波に漏れ出る情報からICチップ等の内部に隠された鍵を暴く【サイドチャネル攻撃】や、クロックに標準的でない波形を注入したり回路に電磁波を照射したりして誤動作を誘発しICチップ等の内部に隠された鍵を暴く【フォールト攻撃】などが対策を要する攻撃であり、これらの脅威に対するセキュリティ評価と対策の高度化が課題となっている。



フォールト攻撃解析支援システム（例）

攻撃対象
ハードウェア （ICチップ、ICカード、
ボードなどの暗号モジュール）



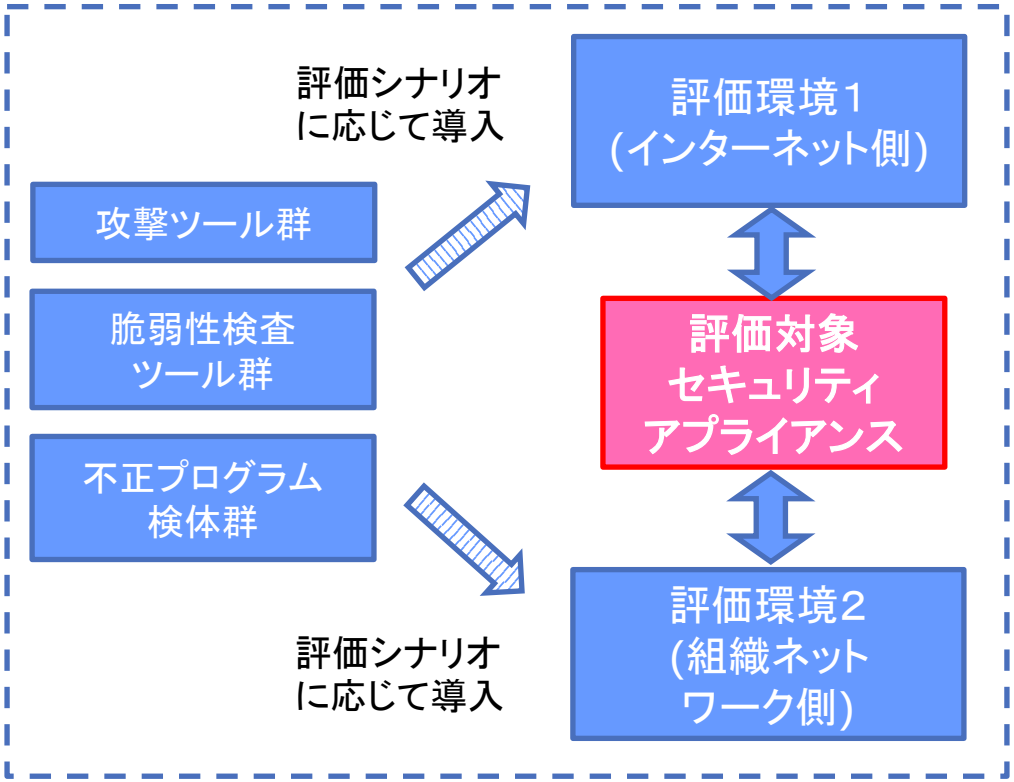


自由に攻撃して
構わない、
リアリティのある
対象システムと、
関連する解析支援
システムから構成
される。

（事例紹介）セキュリティアプライアンス評価・分析

YNU

- セキュリティアプライアンス(Security Appliance): セキュリティ機能(侵入検知、ウイルス対策、メールフィルタなど)に特化したコンピュータ機器. 多くの組織に導入が進んでいる.
- 本演習では、セキュアな演習環境において様々なサイバー攻撃を再現し、これらのセキュリティアプライアンスの攻撃検知能力・防御能力を評価すると共に、近年増加している情報漏えいなどのインシデントを減らすために必要な改善点を見出す.



セキュリティアプライアンス評価・分析演習環境

セキュアな演習環境で実際の製品に対して模擬サイバー攻撃を行い、その結果を分析することで本質的な問題点・課題を学ぶ.

（事例紹介）自動車セキュリティ関連システム

YNU

リアリティのある対象システム（ RoboCar PHV等）と、
関連する解析支援システムから構成される。

【カリキュラム上の位置づけ】
演習重視の講義を設置・改編・拡充

YNU

（平成27年度から実施予定）

博士課程前期向け講義	（博士課程後期向け（特設）講義）
情報・物理セキュリティ総合学	情報・物理セキュリティ総合学Ⅱ

平成25年度から

春学期	秋学期	春学期	秋学期	春学期	秋学期
(博士課程前期向け) 情報メディア学特設講義			(博士課程後期向け) 情報メディア環境学特設講義		
情報・物理セキュリティ解析			情報・物理セキュリティ解析		
1	2	3	4	5	6

平成20年度から
平成24年度まで

春学期	秋学期	春学期	秋学期
(博士課程前期向け) 情報メディア学 特設講義		(博士課程後期向け) 情報メディア環境学 特設講義	
数理・論理セキュリティ1	ドキュメント・決済セキュリティ1	数理・論理セキュリティ2	ドキュメント・決済セキュリティ2