Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2013.02.18 10:44:41 +09'00'

制御システムセキュリティと EDSA認証適合ファジングツールの開発

Fourteenforty Research Institute, Inc.
株式会社 フォティーンフォティ技術研究所
http://www.fourteenforty.jp

Ver 2.00.01

Confidential

アジェンダ

- 制御システムのセキュリティ

- 制御システムへのファジング検査
  - 制御システム用プロトコルのファジング
  - EDSA認証適合ファジングツールの開発

制御システムとセキュリティ

制御システムの動向

従来の制御システム

- インターネット非接続
- ベンダー独自プロトコル

制御システムの
「オープン化」

近年の制御システム

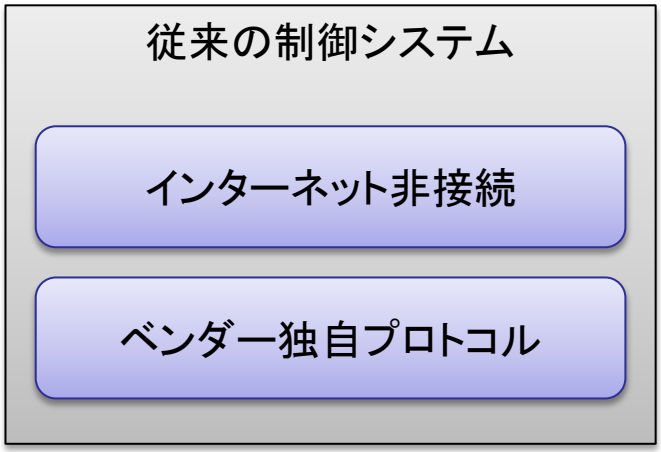
- 情報システムとの接続に伴う
  インターネット接続
- TCP/IPベースのプロトコルの採用
- オープンな通信プロトコルの採用

制御システムの「オープン化」のメリット

- 異なるベンダー間での制御システムの通信が可能
  - システム構成の選択肢が増大
- 情報システムとの接続
  - 情報の一元管理、リモート制御が可能

制御システムの「オープン化」のデメリット

- セキュリティの問題
  - 従来の制御システムでは、独自プロトコルの採用、インターネットへ接続されていないことにより、攻撃の難易度が高かった。



これが「オープン化」により…

制御システムの「オープン化」のデメリット

- インターネットへの接続、汎用プロトコルの採用により、攻撃の難易度が低下
  - 汎用PCを攻撃する感覚で攻撃可能

近年の制御システム

- 情報システムとの接続に伴うインターネット接続
- TCP/IPベースのプロトコルの採用
- オープンな通信プロトコルの採用

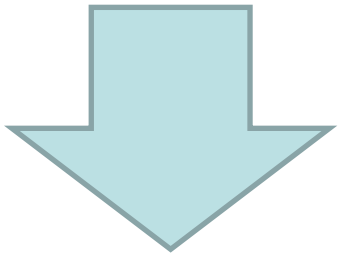
事例

- Stuxnetによるイラン核施設への攻撃
  - ネットワーク経由またはUSBメモリ経由で感染
  - Microsoft Windowsのゼロデイ脆弱性を利用して感染
  - イランの核燃料施設に対するサイバー攻撃が行われた
  - のちにDuquと呼ばれる亜種も出現

制御システムへのファジング検査

制御システム向けプロトコルのセキュリティ

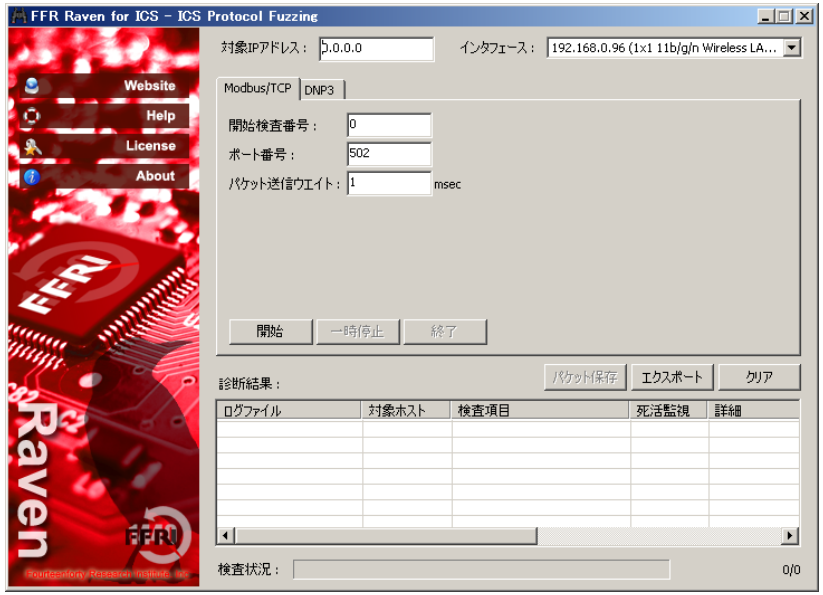
- 既存の制御システム向けプロトコルのTCP/IP上で動作するなど「オープン化」が進んでいる。
  - Modbus/TCP, EtherNet/IP, EtherCAT, BACNet/IP…
- これにより、TCP/IPベースでの攻撃が可能となってくる

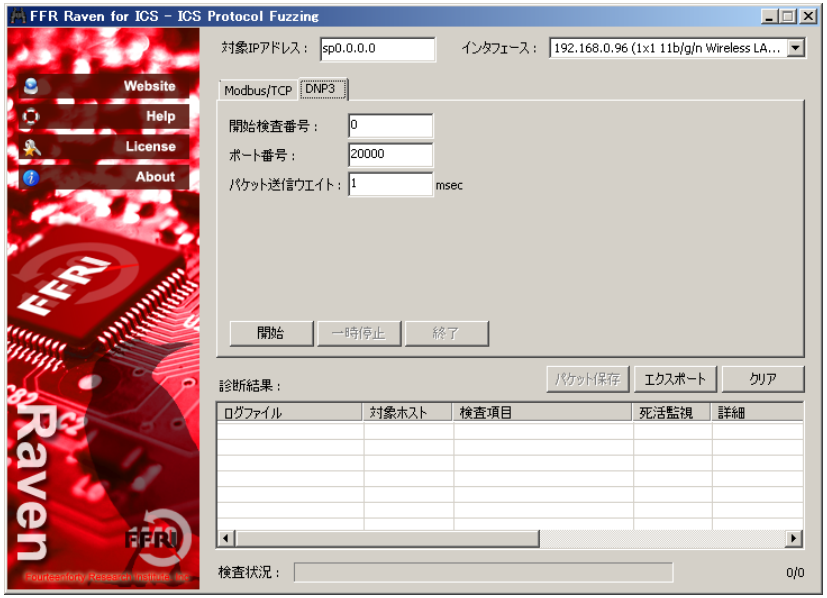


- 制御システム向けプロトコル実装のセキュリティ検査が必要となる
  - 専用ファジング機能の開発
- 一般的なプロトコル実装（TCP/IPなど）のセキュリティ検査も重要
  - EDSA認証適合ファジングツールの開発

制御システム向けプロトコルのファジング

- 制御システム向けのプロトコルに対するファジング機能の開発
  - DNP3, ModbusTCPのファジング機能を開発
  - FFR Raven for ICSへ搭載





  - 実際の制御システムにて1件の問題を発見

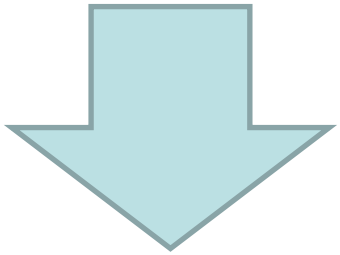
制御システム向けプロトコルのファジング

- ModbusTCPのファジング
  - MBAP(Modbus Appifcation Protocol)レイヤーとPDU(Protocol Data Unit)レイヤーで構成
  - これらの構成に基づき各フィールドの値を変更し、ファジングを実施

- DNP3のファジング
  - Data Linkレイヤー、Transport、Applicationレイヤーの3つから構成
  - これらの構成に基づき、各フィールドの値を変更し、ファジングを実施

EDSA認証適合ファジングツールの開発

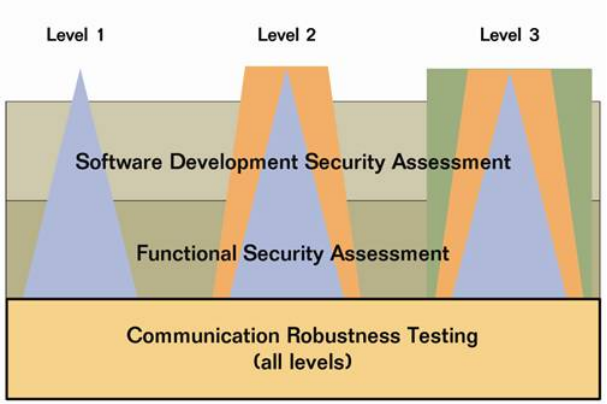
- 「オープン化」が進んでいる制御システムの汎用プロトコルのセキュリティ検査を実施
- ファジングツールを使用してネットワークプロトコル実装のセキュリティを検査
  - ISASecure CertificationであるEDSA認証に適合可能なファジングツールによって制御システムのセキュリティ検査を実施できるようにする。



  - これにより、制御システムが持つネットワーク機能のセキュリティ脆弱性を検査する

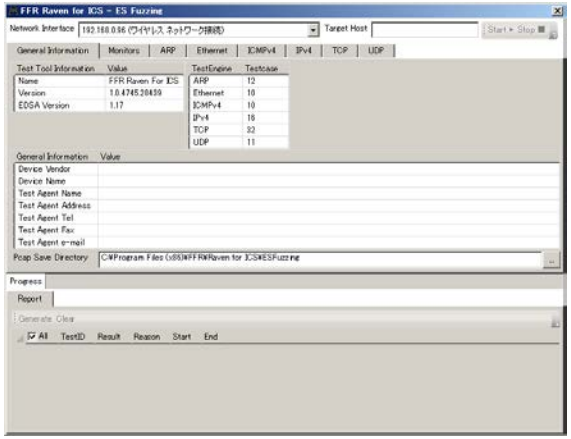
EDSA認証

- EDSA認証(Embedded Device Security Assurance Certification)とは
  - ISASecure Certificationとして規定された認証規格
  - 制御システムのセキュリティについて規定してる認証規格
  - 大きく分けて3つのカテゴリに分かれる
    - Software Development Security Assessment (SDSA)
    - Functional Security Assessment (FSA)
    - Communication Robustness Testing (CRT)

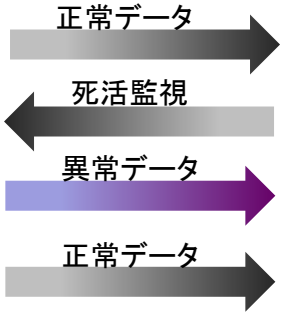


EDSA認証適合ファジングツール

- DUTに対してCRT（Communication Robustness Testing）を実施するためのツール
- デバイスの持つプロトコル実装が、正常に動作し、異常な、または悪意を持ったネットワークトラフィックに対しても問題なく動作することを確認する
- 検査はさまざまなトラフィックレートで実施される



ファジングツール



DUT（Device Under Test）

ファジング対象プロトコル

- EDSA認証のCRTで規定されたGroupのプロトコルをファジング
- CRTではプロトコルが複数のGroupに分類される（Group1～Group5）が、現時点ではGroup1のみ規定されている
  - Group1のプロトコル
    - IEEE 802.3（Ethernet）
    - ARP
    - IPv4
    - ICMPv4
    - TCP
    - UDP

各プロトコルでの検査項目

- EDSA認証で規定されている検査パターン分類
  - ベースラインオペレーション
    - 対象プロトコルでの基本的な通信ができることの確認（正常通信）
  - ロバストネス
    - 不正な値が設定されたPDU（Protocol Data Unit）を送信し、DUTの堅牢性を検査
    - 他にも不正な形式、順序が矛盾している、不正なサイズのPDUを送信し、堅牢性を検査
  - ロードストレス
    - DUTにストレスをかける目的で大量のPDUを送信し、DUTの堅牢性を検査
- 各検査パターンで実際に使用するパケットはツール側で自由に設定可能
  - FFR Ravenで培ったファジングノウハウを活用

検査パターン例（Ethernet, ARP）

	ロバストネス	ロードストレス
Ethernet	• 64バイトより小さいフレームの送信 • 送信先MACアドレスにユニキャストアドレスまたはブロードキャストアドレスを指定 • 複数のQタグを含むフレームを送信（IEEE802.3フレーム）	• 最大処理性能を超える通信データを送信 • 最大処理性能を超えない範囲でのパケット送信
ARP	• キャッシュポイゾニング攻撃を実施 • Ethernetヘッダで指定された長さとARPパケットの大きさが異なる • ARPヘッダの各フィールドに不正な値を設定	• 最大処理性能を超える通信データを送信 • 最大処理性能を超えない範囲でのパケット送信 • ARPキャッシュを飽和させるようなパケット送信

検査パターン例（IPv4, ICMPv4）

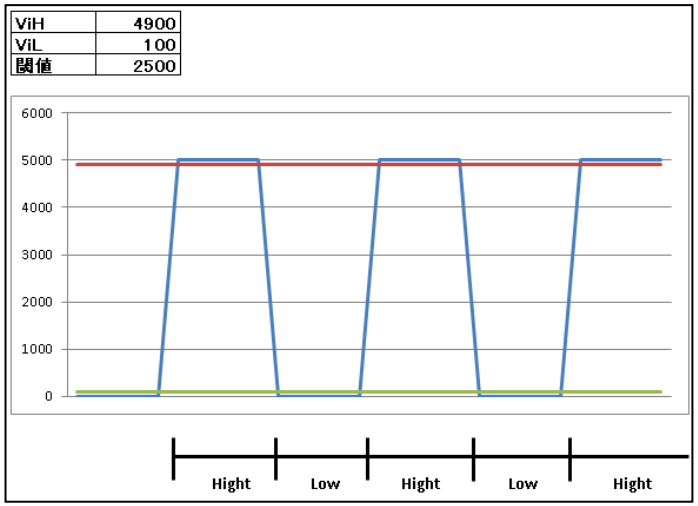
	ロバストネス	ロードストレス
IPv4	• IPヘッダの各フィールドに不正な値を設定 • 送信元に0.0.0.0のような通常設置されないIPアドレスを設定 • オフセットフラグに不正な組み合わせを設定	• 最大処理性能を超える通信データを送信 • 最大処理性能を超えない範囲でのパケット送信 • 再構築不可なフラグメント化IPパケットの送信
ICMPv4	• ICMPヘッダの各フィールドに不正な値を設定 • 順序が矛盾しているICMPパケットを送信 • 送信元IPアドレスにマルチキャスト、ブロードキャストアドレスを設定	• 最大処理性能を超える通信データを送信 • 最大処理性能を超えない範囲でのパケット送信

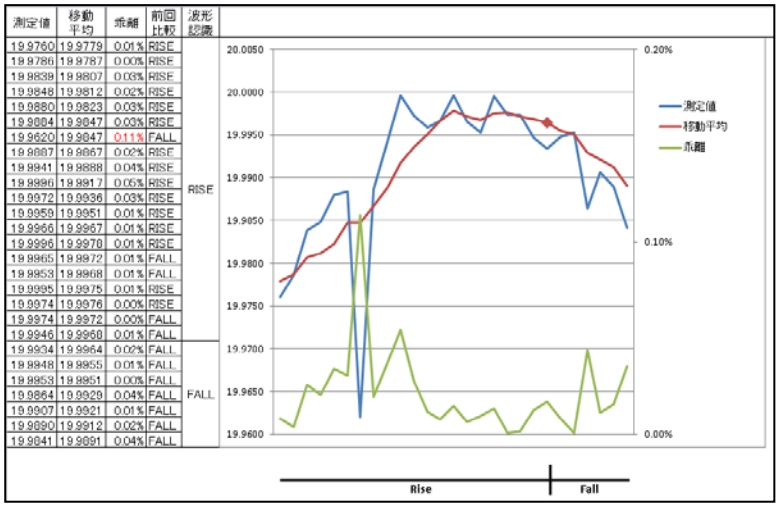
検査パターン例（UDP, TCP）

	ロバストネス	ロードストレス
UDP	• UDPヘッダの各フィールドに不正な値を設定 • UDPフィールドで指定されたパケット長とIPヘッダで指定されたパケット長の整合性が合わない	• 最大処理性能を超える通信データを送信 • 最大処理性能を超えない範囲でのパケット送信 • 送信元ポート番号、宛先ポート番号、パケット長に様々なパターンを設定
TCP	• TCPヘッダが途切れているパケットを送信 • TCPヘッダの各フィールドに不正な値を設定 • LAND攻撃、LaTierra攻撃の実施	• 最大処理性能を超える通信データを送信 • 最大処理性能を超えない範囲でのパケット送信 • SYN Floodの実施

対象機器からの信号計測による死活監視

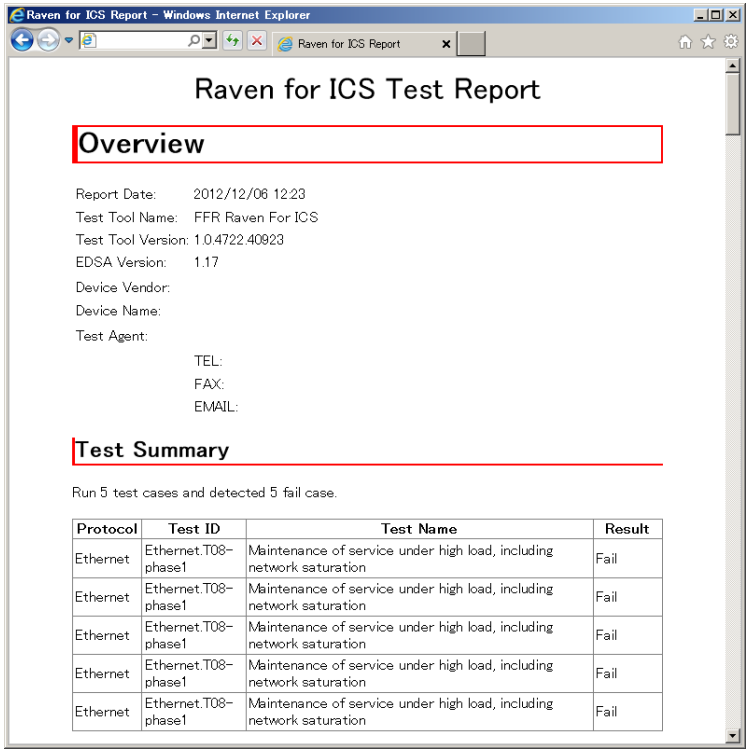
- 対象機器から出力されるデジタル信号またはアナログ信号を監視することで、死活監視を実施
- 測定信号のジッタ計測により死活監視を実現

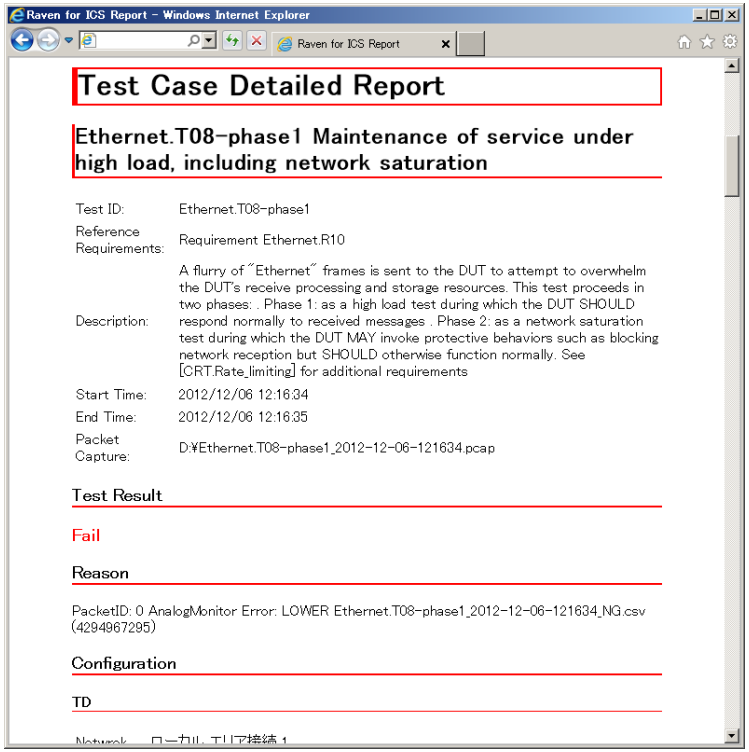




検査レポートの出力

- HTML形式での検査レポートを出力
- 検査したテストケースごとに、パケットキャプチャも合わせて保存

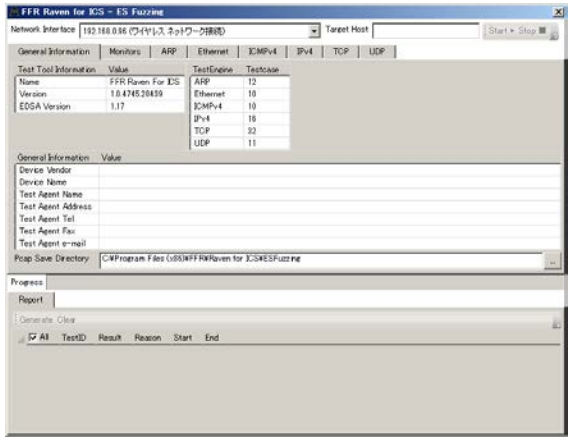




ファジングツールの今後

- EDSA認証の取得
  - 現在認証取得プロセスを実施中
  - 認証プロセスをクリアし、EDSA認証のテストツールとして認められる
  - これにより、ファジングツールを使用したEDSA認証検査が実施可能になる

- EDSA認証規格アップデートへの対応
  - 現時点では、Group1のみ規定されている
  - Group2以降が規定され次第、対応していく



まとめ

- 制御システムの「オープン化」が進むにあたってセキュリティの確保が急務となる
- ネットワーク経由での攻撃が考えられることから、制御システムのプロトコル実装に対するセキュリティ検査が必要
- 制御システム向けのプロトコルに対するファジング機能及び、EDSA認証適合ファジングツールを開発