CyberDefense

サイバーセキュリティの課題と脆弱性対策～ICSとITセキュリティ～

その2:
脆弱性の試験と対策

Smart Community Summit 2014

2014年6月19日

株式会社サイバーディフェンス研究所

システムが構築されるまで

IT（情報技術）

- 構築、インストール、使用、再構築、再インストール（の繰り返し）
- 寿命：数年

ICS（産業用制御システム）

- 構築、インストール、運用、維持管理（可能な限り長く）
- システムの寿命：数十年

エンジニア　対　ハッカー

エンジニア

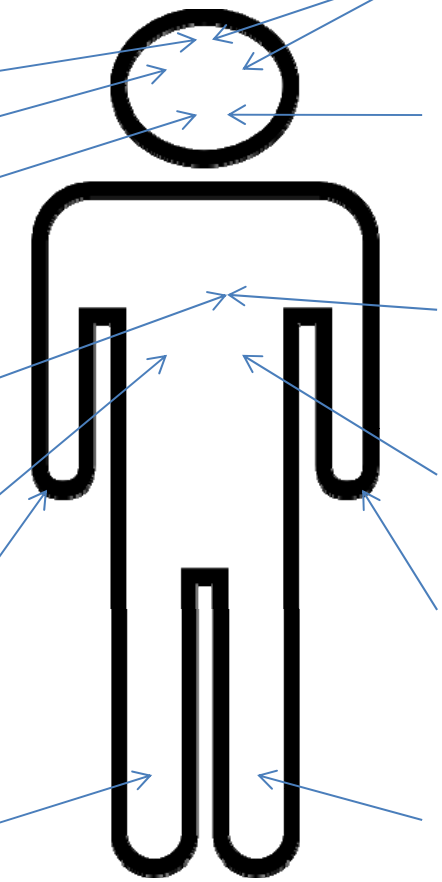
論理と制御ユニット
視覚的なフィードバック
口頭伝達と燃料取り入れ

内部プロセス交換コントローラ

酸素処理機

主要な操舵機

空間的な作動装置



ハッカー

侵入検知＋認証トークン制御機。
可能であれば侵入、不可であれば回避。

口頭認証ユニット。可能であれば複製、偽造。システムの汚染にも利用可能。

99.99%回復不可能なポイントをDOS攻撃。

空中エージェントを利用した内部システムへの侵入可能なポイント。

操舵を制御するための主な標的。
小規模な被害でも内部システムにアクセス可能。

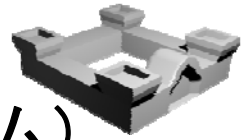
小規模な被害を生じさせる可能性がある攻撃地点。電子信号と比較して速度は極めて遅い。

現状（セキュリティの見地から）

IT（情報技術）

- クラウド系サービス、アカウントパスワードの漏洩、悪性サービスや偽サービスが一般的
- 脆弱性診断に関する広範な方法論
- 選択できるソリューションが多すぎる、（しかし完全なものは皆無）
- 「不安定性」が隠された特性

ICS（産業用制御システム）



- 運用上のニーズが優先されるため、セキュリティは、分離によって達成されることが多い
- 別々のコンポーネントは最小主義によって保護できるが、通常は別々に作動する
- 実システムに関する実践的な役立つ知識を持つ人間はごく僅か
- 「恒久的」がゴールである

最近では、これらのシステムが「スマート」技術によって統合されつつある…

融合体に危険因子を追加する：物＋ハッカーの現状

どれだけ悪くなり得るか?

IT（情報技術）

- 誰かが貴方のPCを利用してBitcoinを収集。または、
- 全員の銀行口座が空にされる。航空会社の事務所にウイルスが感染して航空機が飛べない。既存の全てのウェブカメラや電話機が大量の監視ネットワークに変化。

ICS（産業用制御システム）

- 電気代を支払わずに電気を盗用。または、
- ダム制御やその他の重要なシステムを故意に損傷させることで数百万人を大量殺人。（幸運にもまだ起きていない）

脆弱性の修正

IT way（情報技術の場合）

- 「アップデート」ボタンをクリック
- 別の清潔なVPSインスタンスの生成、データの待避、IPの変更、を行えば完了
  - ラック上の機械に触れる必要もない

ICS way（産業用制御システムの場合）

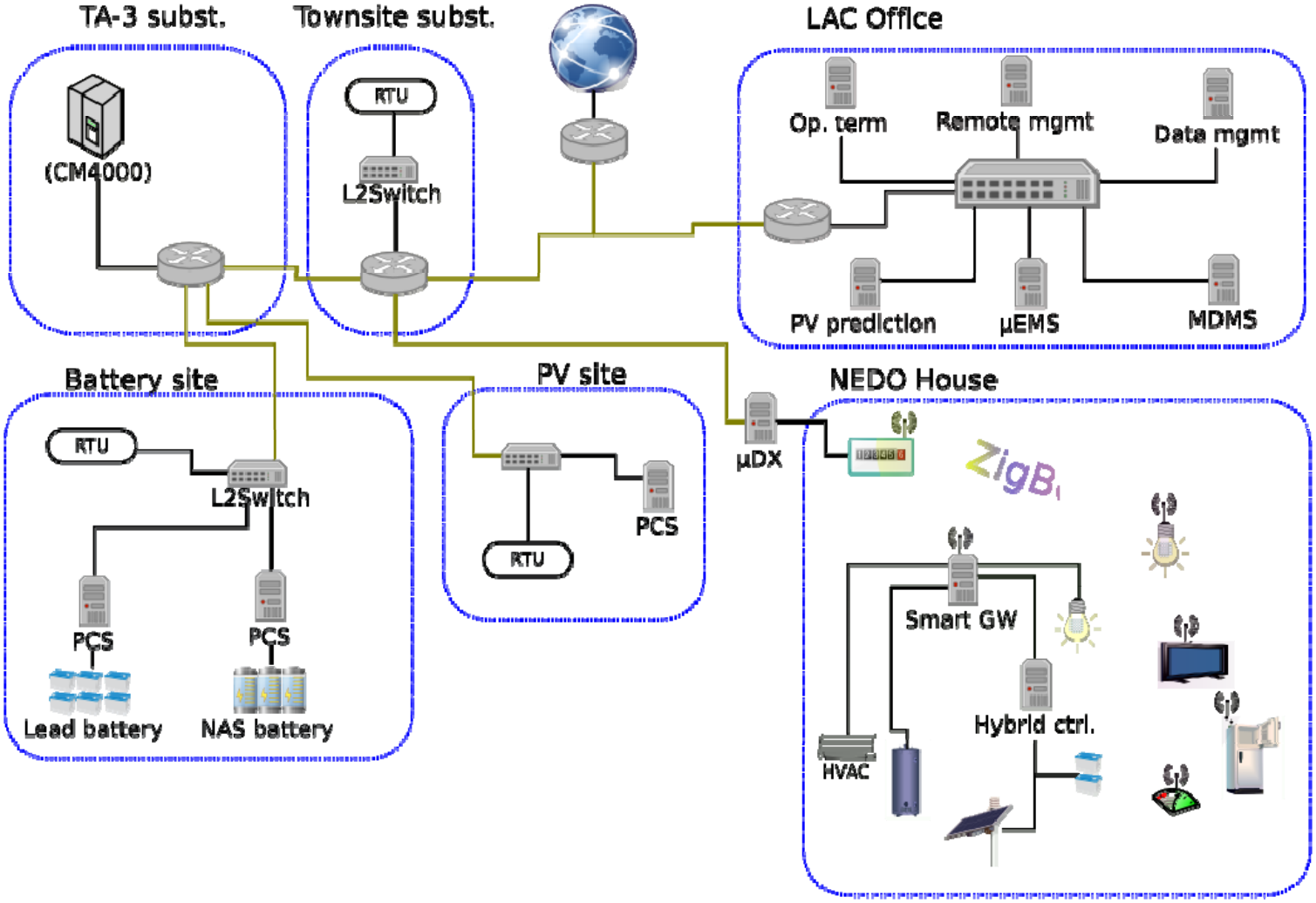
- 主要な機能の運用を阻害する可能性があるため、何も変更しない方がいい
  - 広範な試験要件やハードウェアベースの配置がなされているため、コンポーネントや設定を変更するだけでもかなりコストがかかる

ICS系システム用のセキュリティ試験

マルチフェーズのアプローチ

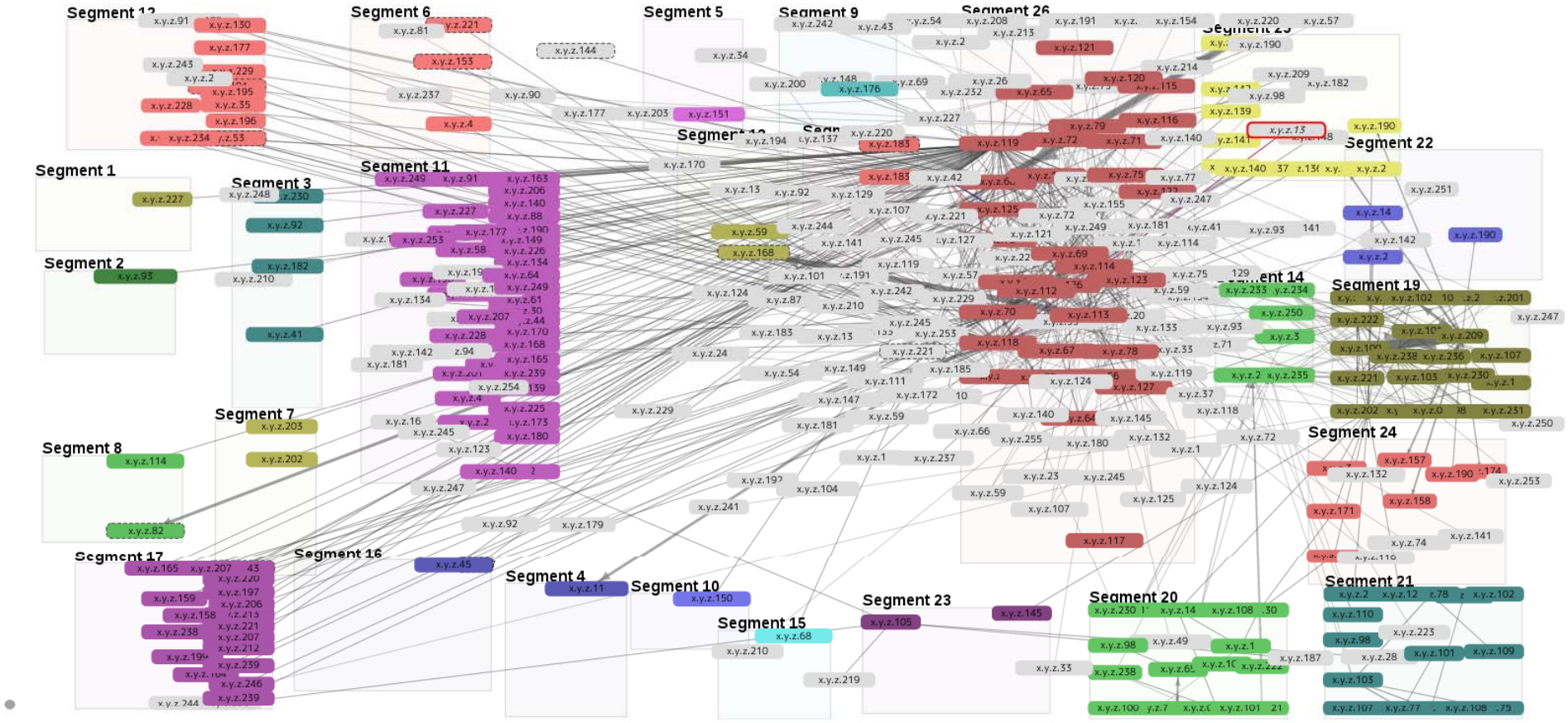
- 壊せるものを全て壊す
  - 制御下にあるラボ環境
  - 一般的には個々のコンポーネントに対して
  - 修正や戻しはいつでも可能
- 何も壊さない
  - 実世界での設定
  - 第一フェーズに基づくデータをチェックするのみ
  - 過去に報告された問題点が実際に修正されていることを確認する

ネットワークの概観



比較的、単純では？

ネットワークの詳細図



- 1,000以上の相互接続…
- 40種類以上のプロトコル…
- 100GB以上のトラフィック/毎日

“ん、この辺のどこかにあるはずだが…

調査結果

- 緊急レベル数件、高レベル数件、低レベル数件の直接的な脆弱性が発見されたが、予想よりは少なかった。
- 従来の手法は、新たな規格の下では巧く動作しない（特に、暗号化が関係する場合）。
- 内部でシステムを適切にセクショニングすることが、疑わしいコンポーネントによるリスクの削減に大きく寄与する。
- 運用上のリスクや慣性が存在するため、事前に個々のコンポーネントをテストすることが不可欠である。
- システムはいつでもテストできる状態にあり、適正なテスト結果を得るためには、無条件にその時間を割り当てなければならない。
- 将来、更にセキュアにするために必要な意識向上や知識のかけらを参加者全員が取得できた。

永続的なセキュリティに向けたステップ

- ITのエンジニアは、生涯利用可能な ソフトウェア設計を学ぶ必要がある
- ICSのエンジニアは、進化型設計の利用を学ぶ必要がある
- ICSのマネージメントは、リスクを常に意識する必要がある
  - ハッカーの作業台を常に観察する
  - 周りで起きていることをちゃんと見る
  - 自分のシステムで起こっていることを良く知り、それが危険な状態に差し迫っているかどうかを知る
- 今、行動を起こさなければ、手遅れになる

本プレゼンに関して

株式会社サイバーディフェンス研究所

ラウリ・コルツパルン <lauri@cyberdefense.jp>

Email: sales@cyberdefense.jp

Tel: 03(3242)8700

Web: www.cyberdefense.jp