NSL
Networked Systems Laboratory

研究室紹介

森　達哉

情報理工学科　研究室説明会
2015/3/24

研究室（主宰者）の理念

- 研究の自由と主体性
  自分が一番やりたいことを主体的にやろう！
- 実社会のリアルに基づいた研究
  （机上の空論ではなくリアルを追求）
- 十二分な仕事と深い思考→オリジナリティ
- 研究を楽しみながら個々のメンバーが着実に成長

研究室のミッション

サイバー空間あるいはネットワークに接続された物理的オブジェクトを攻撃や濫用から保護する技術の確立と一般化

研究成果の具現化と世の中への貢献

知識・教訓，サービス，ソフトウェア

研究テーマの例

- セキュリティ& プライバシー
  - マルウェアの収集・解析・検出・分類
  - スマートデバイスのサイドチャネル攻撃
  - ネットワークの異常検知・解析
  - スパムの大量収集と解析
  - ソーシャルエンジニアリング
  - サイバー犯罪・サイバー戦争への対策
- インターネットの計測
  - スマートフォン通信解析
  - 広告ネットワークの計測
  - Twitter ユーザー行動分析
  - 超高速ネットワークモニタリングとアルゴリズム

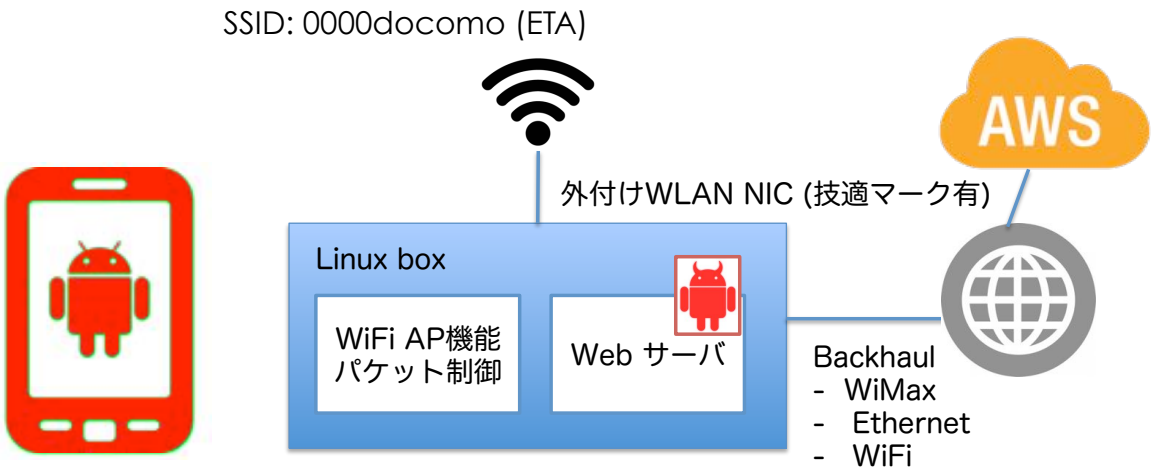
セキュリティ研究の面白さ

- 人間がシステムに深く関与
  - 「思わぬ」使い方，「思わぬ」脆弱性，「思わぬ」挙動
  - 多数の人間が使い出すとシステム設計時にはまったく想定していなかった問題が噴出
    →そのような問題にいかに対処するか．まずは「敵を知る」ことが重要
- パズル的要素
  - すべてではないが，パズル的な面白さがある問題がある
  - リバースエンジニアリング
- 学際的研究
  - セキュリティ外の知識が大いに役に立つ
  - ネットワーク，機械学習，自然言語処理，時系列解析
  - 心理学，社会科学
- 成果の社会への還元
  - 得られた研究成果が実際に役に立っている機会が多い
    - UC サンタバーバラ → Lastline Inc.
    - Michigan Ann Arbor → Arbor Networks

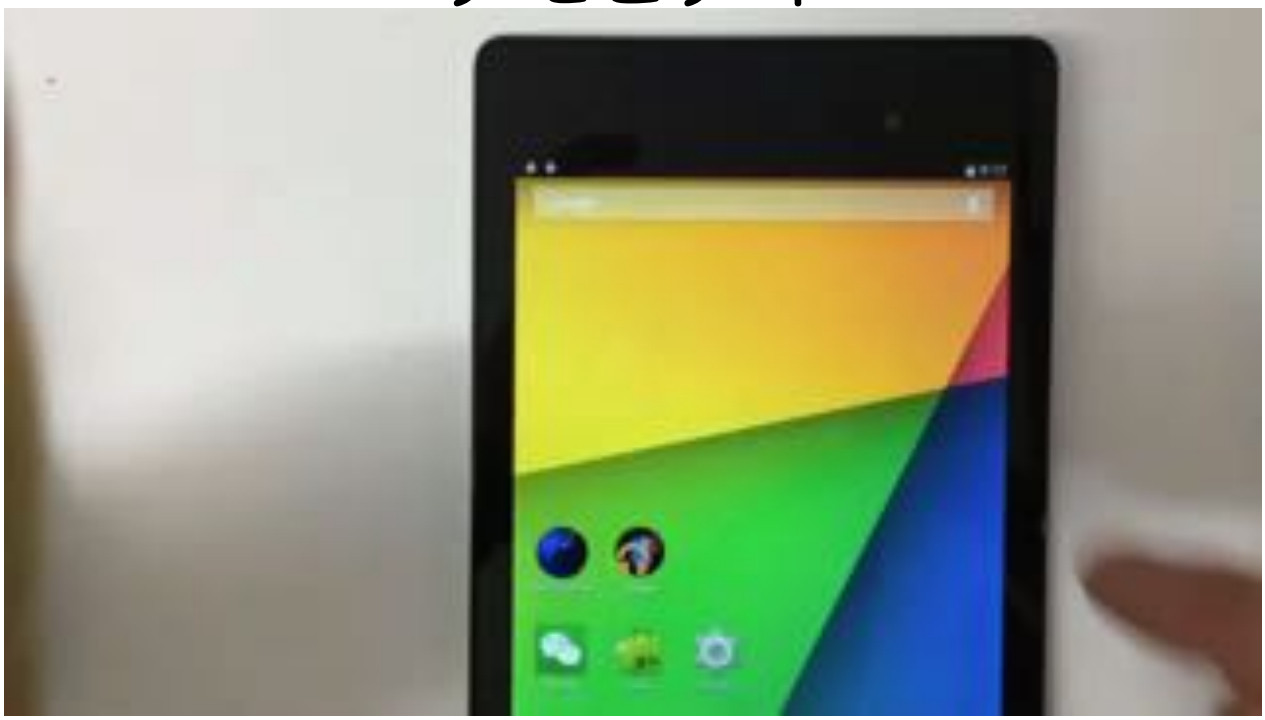
研究の一例： Mobile Security

- 様々なセンサーを持つ
  - プライバシーの問題が生じやすい
- ユーザが多い（億単位）
  - インパクトが大きい
- アプリが多い（数100万）
  - 研究室保有 Android アプリ数: 100万
  - 「ビッグデータ」的アプローチが有効
- 新たなデバイスの登場
  - これからも成長が期待されるマーケット
  - Smart Watch, IoT, etc.

デモ概要


SSID: 0000docomo (ETA)
AWS
外付けWLAN NIC (技適マーク有)
Linux box
WiFi AP機能
パケット制御
Web サーバ
Backhaul
- WiMax
- Ethernet
- WiFi

デモビデオ



デモの解説

- いわゆる Fake AP あるいは Evil Twin Attack (ETA)
- Android に対するドライブ・バイ・ダウンロード攻撃によるマルウェア感染
- マルウェアは秘密裏に撮影＋画像をクラウド(AWS/EC2)にアップロード
  - 試験用マルウェアは大学院生が開発（学部での卒論テーマの一貫）
  - オープンソース・ソフトウェア (metasploit) を用いた遠隔操作も実証済

日本経済新聞

小 中 大 印刷

携帯３社、無線ＬＡＮの環境整備で協力　五輪見据え

2014/6/3 22:02 | 日本経済新聞　電子版

東京都は３日、2020年に予定する五輪開催に向けて、携帯電話や公衆無線ＬＡＮ「Ｗｉ－Ｆｉ」の通信状況について、携帯３社のトップらを対象にヒアリングを開いた。各社は訪日外国人が快適にスマートフォン（スマホ）でネットを利用できる環境づくりで協力すると表明した。

都庁で開いたヒアリングに出席したソフトバンクの孫正義社長は、五輪開催に向け「Ｗｉ－Ｆｉを無料で提供する」ことを明らかにした。日本のＷｉ－Ｆｉは外国人にとって使

訪日客に無線ＬＡＮ　全国共通の無料ＩＤで観光促進

2014/5/23 14:07 | 日本経済新聞　電子版

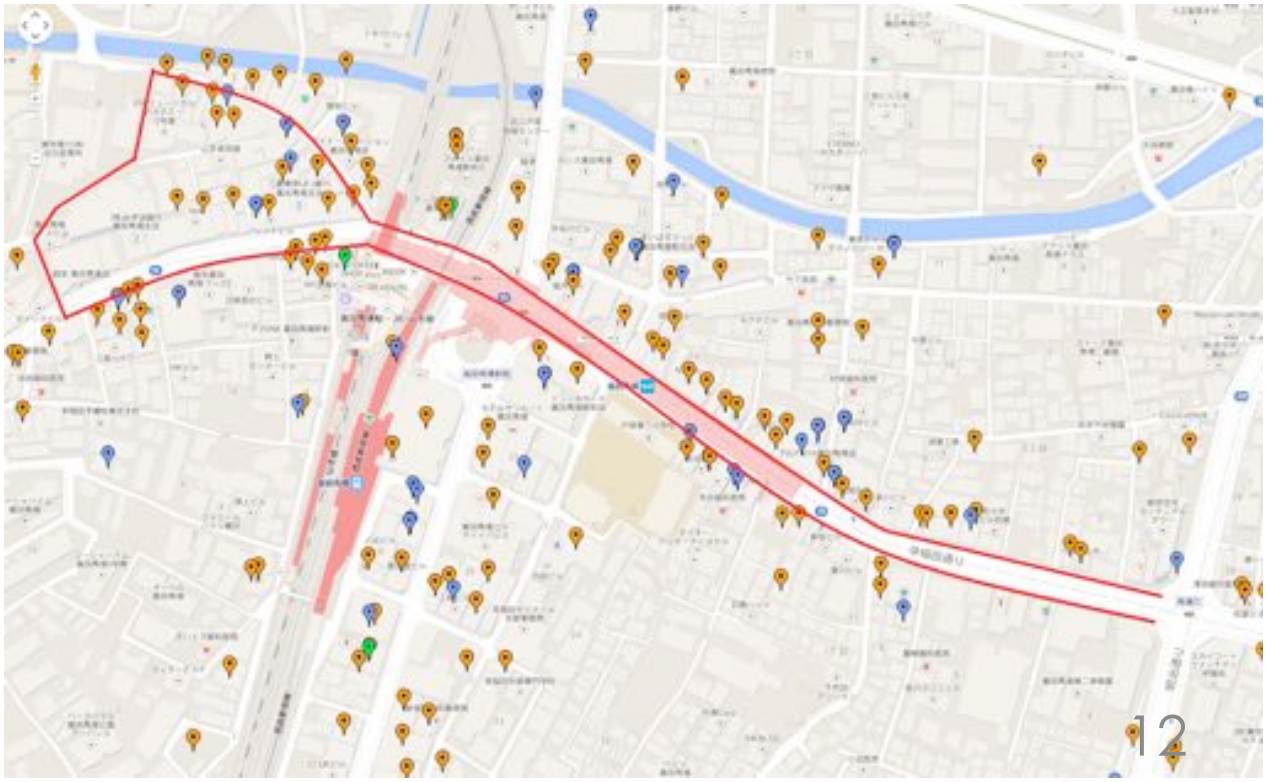
小 中 大　保存　リプリント　▼共有

政府はＮＴＴグループなどと共同で、日本を訪れる外国人が駅や観光地などの無線ＬＡＮ（構内情報通信網）サービスを簡単に使えるようにする。空港などでＩＤを配り、滞在中は全国どこでもひとつのＩＤで無線ＬＡＮを無料で使えるようにする。2016年度をめどにサービスを始める。無線ＬＡＮの使いにくさは訪日客の最大の不満の一つ。観光立国や20年の東京五輪に向け、官民一体で改善を急ぐ。

Fake AP に関する調査

- Fake AP 検出技術に関する研究(B4原田君卒業論文テーマ)
  - ハードウェア clock skew，IPアドレス，認証情報，公開鍵証明書等を総合的に利用して Fake AP を自動的に検出するソフトウェアを開発
  - ラボ環境でのテスト＋フィールド調査

Fake AP のフィールド調査例



ETA に対する対策技術と課題

- IEEE 802.11u
  - Wi-Fi にシームレスなモビリティ/ローミングを実現するためのプロトコル
  - ANQP: EAP による認証技術
  - Hotspot 2.0, PassPoint
    - Apple iOS7以降，Samsung Galaxyの一部が対応
  - Next Generation Hotspot (NGH)
    - さらに 802.11x に対応

- 新しい技術に対応できない古いデバイスをどうするかは依然として課題

教訓

- セキュリティ = chain of trust (信頼の鎖)
  - システムの一部が弱いと全体に影響
  - 部分最適化ではダメ
- 脅威は現実に身の回りに偏在
  - 大学の学部生が簡単に攻撃を実現できる
  - 対象は PC だけではなく多種多様に
  - スマートデバイス，IoT，M2M，…
  - デモレベルの攻撃は学生でも簡単に作れてしまう
- 穴をふさぐ新技術は万能ではない
  - IEEE 802.11u で利用される認証技術 (EAP)は good
  - しかし古い端末・技術はすぐには捨てられない
    - IPv4, WEP, SSLv3, …
  - 実態・リアルの理解が必要

サイバーセキュリティの研究に求められるものは何か？

大学における
サイバーセキュリティの研究

- ×個々の攻撃や事象を追いかけることのみを追求
- ◯個々の攻撃や事象を理解するとともに，攻撃・対策技術の一般化や抜本的な解決を図る

- サイバーセキュリティの問題は歴史が浅く，学問体系としてまだまだ未成熟．教科書もあまり無い（対象が変化する）．
- これからパイオニアになれるチャンスがある！

どういう人が向いているか

- 主宰者の理念や研究室のミッションに共感できる（就職活動と同じ！）

- プログラミングが得意 or 好き
- パズル的なゲームが好き
- 応用数学が好き（機械学習，パターン認識，アルゴリズム等々）
- セキュリティの問題に非常に高い興味を持っており，自分なりの問題意識がある
- 新しいアイディアをどんどん試してみたい
- 色々と新しいことを積極的にやってみたい

MWS での研究発表






賞　状
MWS 2013 優秀論文賞

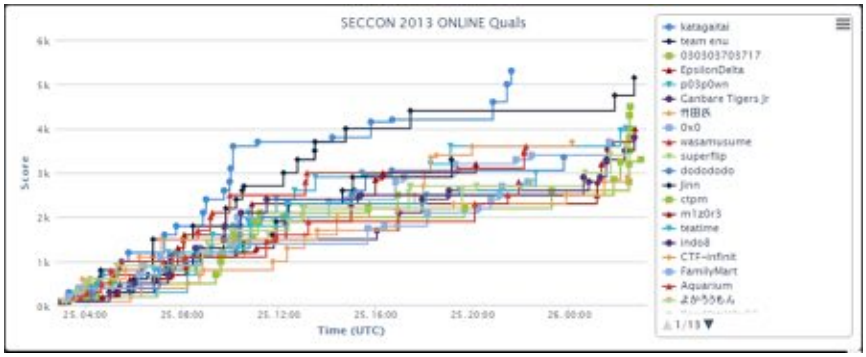
賞　状

2013 優秀論文賞　2014 学生論文賞

MWS CUP での活躍

CTFサークル m1z0r3

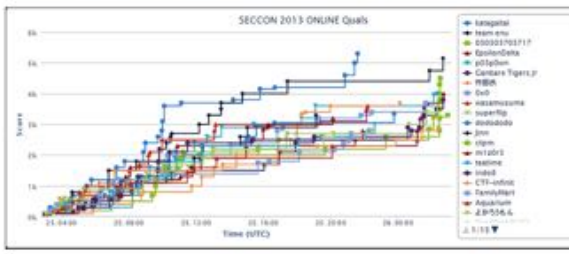
- 2013年12月発足
  - 森研＋後藤研の有志が中心
  - SECCON CTF 2013 全国大会出場
    - オンライン予選：14位/327チーム



SECCON CTFでの活躍

http://2013.seccon.jp/blog/2014/02/seccon-2013-ctf-online-result.html

http://score.quals.seccon.jp/ranking/



SECCON 2013 CTF
オンライン予選324チーム中14位
⇒ファイナル進出

SECCON 2014 CTF
オンライン予選425チーム中6位
⇒ファイナル進出

外部組織との連携状況

大学の弱み＝実社会との接点．敵を知る＝課題の現状を知る
弱みを補うために共同研究，インターンシップを積極的に
実施中．関連する企業社員と密接に仕事を進める

共同研究パートナー

ゼミ・勉強会の予定

全体ゼミ：毎週火曜日 13:00〜14:30
　全員が参加．論文紹介もしくは各自の研究進捗報告

機械学習勉強会：毎週木曜日　時間調整中
　希望者により，機械学習のサイバーセキュリティ課題への実践にむけた勉強会を開催．理論の理解に加えて実データを用いた実践的ノウハウの修得を重視．

CTF勉強会 (m1z0r3)
　希望者が自主的に実施（曜日未定）

その他，自主的な輪講や勉強会の開催を強く奨励します（研究室内に閉じる必要はまったくないです）

興味を持った人は

オープンハウスで話をしにきてください．本当に自分がその研究室に合うかは実際に行ってみて話をしなければ判断できません（就職活動も同じ！）

http://nsl.cs.waseda.ac.jp/

場所: 55N-606 （エレベータの裏・下記ロゴが目印）

3/24(火) 16:00-18:00
3/25(木) 13:00-18:00
3/26(金) 13:00-18:00

NSL
Networked Systems Laboratory