ネットワークセキュリティとプライバシー

総合数理概論

菊池　浩明

1. インターネット定点観測

- Scannersプロジェクト
  - 2005年から
  - 委託研究: 日立製作所
  - 中央大学，JPCERT, CCC
  - ウィルスの感染規模を観測，全世界の感染数，自動分類決定木，平均感染期間，連携感染パターン検出への応用

ハニーポット
（定点観測センサー，
NIFTY-NET, SO-NET）

2. 生体認証とプライバシー

- Zerobioプロジェクト
  - 2006年~2009年度科学研究費補助金（基盤研究 (B)「ゼロ知識証明を用いた非対称なリモートバイオメトリクス利用者認証」
  - 静岡大学・東京工業大学
  - 暗号技術(ゼロ知識証明プロトコル）を用いた安全な生体認証

研究テーマ

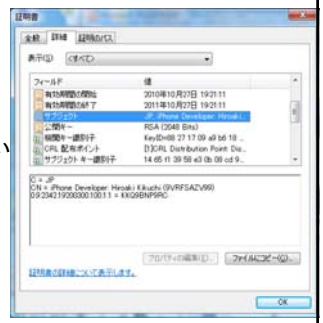
- ネットワークセキュリティ
  - 不正アクセスとコンピュータウィルスの定点観測
  - 迷惑メール（Spam)の観測
  - ブロードキャスト（放送型）暗号とコンテンツ配信
  - 電子すかしによる著作権保護，ユーザ認証
- プライバシー保護
  - 匿名選挙，秘密オークションプロトコル
  - プライバシー保護データマイニング
  - ゼロ知識証明によるリモート生体認証
  - 墨塗りディジタル署名
- ネットワーク応用
  - RFIDによる入退出管理，アドホックネットワーク・センサーネットワーク，セキュリティ心理学

1. フィッシング詐欺の脅威

インターネットの信頼性

公開鍵証明書

- インターネットのパスポート
  - 名前
  -
  (秘密鍵は入っていない)
  - 電子署名:
    本人が作ったものを証明する



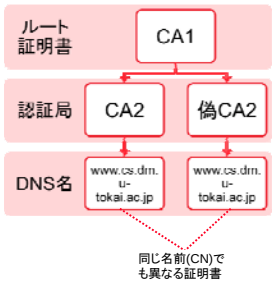
新たな攻撃「証明された嘘」

C.Soghoian and S.Stamm, "Certified lies: Detecting and defeating government interception attacks against SSL", Financial Cryptography 2011, pp . 1-18, 2011.

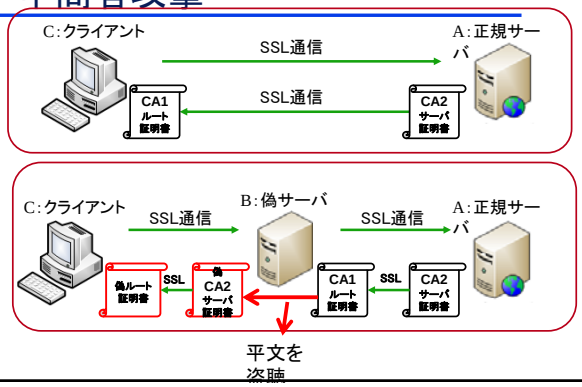
- 「強要された証明書作成攻撃」 (compelled certificate creation attack)
- 政府によるルート認証局へのSSL証明書偽造の強要
- SSL中間者攻撃

問題点：PKIの信頼のパスとDNS名の不一致

- 異なる信頼のパスで同じDNS名の証明書が複数存在可能
- 例）DigiNotar不正証明書事件,2011年



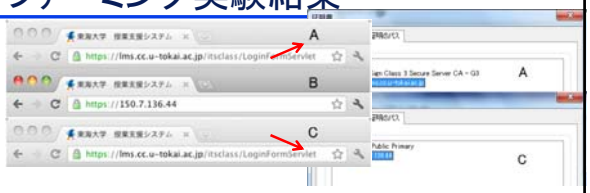
中間者攻撃



ファーミング実験環境

- クライアント環境
  - ❑偽証明書作成(ルート証明書，サーバ証明書)
  - ❑偽ルート証明書インポート
  - ❑DNSサーバ書き換え
- サーバ環境
  - ❑VMWare環境の構築
  - ❑偽サーバ構築(中間者)

ファーミング実験結果



- AとC違いは証明書の信頼パス
- 証明書の内容を詳しく見たり、覚えておかなければならない

リスク評価・実験

- 実験1. 標的型メールを用いた実験
- 実験2. 偽造証明書を用いたSSL中間者攻撃の性能評価
- 実験3. ルート証明書インポートの危険性の評価

実験1.標的型メールを用いた検証

- 2011年8月1日に東海大学の学生52名に送信
- 33名が検証用に作成したサイトにアクセスした
- アンケート回答者の**87%**が気付かずにアクセスしている

回答内容(選択式)	3年	4年	計	割合[%]
本物のサイトだと思った	1	10	11	34.4
URLがあったからクリックした	2	1	3	9.38
偽サイトだと思ったがアクセスした	1	0	1	3.13
メール内容で気付いたがアクセスした	1	0	1	3.13
無回答	8	9	17	53.1
合計	13	20	33	100

結果:標的型攻撃では87%の人は騙される

まとめ

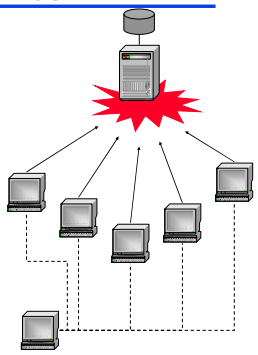
- 実験1:偽メールでは　　%の人は騙される
- 実験2:中間者攻撃サーバは約　　秒で用意可能
- 実験3:Windowsのクライアントへのインポートは
  - 管理者権限なしで10クリック
  - 管理者権限ありで1クリック
- 結論，Soghoianらの攻撃の危険性が実証された

2. Botnetの脅威とその解析

遠隔操作による不正行為

ボットネットの新たな脅威

- 新種ウィルス
  - IRC制御のトロイの木馬型
  - ロ「ボット」から
  - 命令されて攻撃やスキャンを実行
  - 例) PRIVMSG #plazm :.ddos.synflood 66.xxx.xxx.xxx 100 0 27015
  - 変種
    - » Gaobot, spybot, agobot, polybot



ソニーの個人情報流出

- 2011年4月26日
  - ゲーム配信サービスに不正アクセス
  - 氏名，住所，電話番号，メール，性別，生年月日が7700万人分
  - 12,700件カード

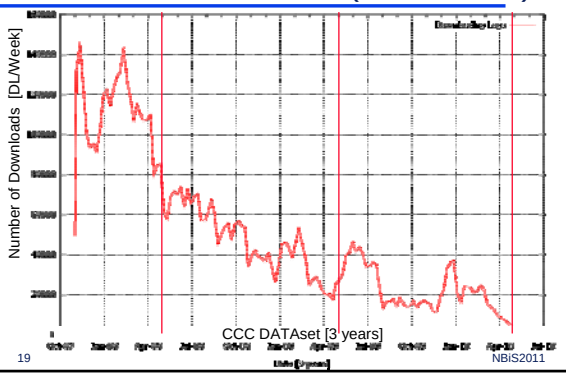
http://www.asahi.com/business/update/0503/TKY201105030069.html?ref=reca

ISDAS: インターネット定点観測

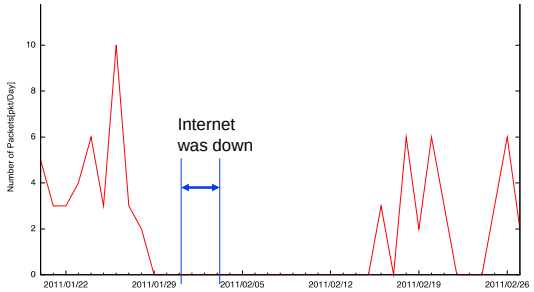
- Internet Scan Data Acquisition System
  - JPCERT/CCによる不正パケットの定点観測
  - 2003年11月より
  - ワームの感染活動，ポートスキャン
  - cf. 警視庁(@police), IPA (TALOT)

http://www.jpcert.or.jp/isdas/

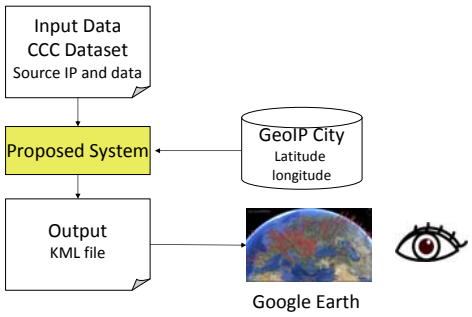
Number of Downloads (2007-2010)



2011年1月エジプトからの攻撃

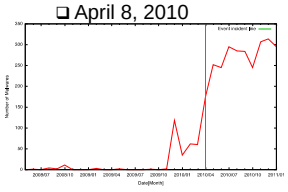


Our Visualization

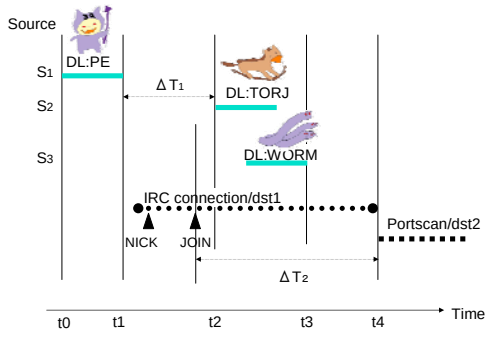


Case 1: Poland in 2010

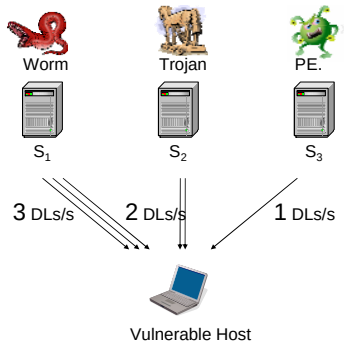
- Cyber Space
  - April 8, 2010
- Real World
  - April 10, 2010



TimeChart



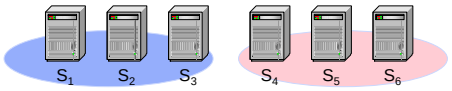
1. 連携サーバ群



2. 動的な振る舞い

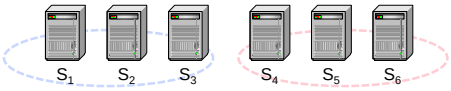
Downloads/day	3	2	1	*A*
April	30	20	10	10A
May	9	6	3	3*A*
June	3	2	1	1*A*

3. 複数のボットネット



	Botnet *A*			Botnet *B*			
DLs/day	3	1	1	4	2	1	*A/B*
April	30	10	10	0	0	0	10*A* + 0*B*
May	9	3	3	4	12	6	3*A* + 3*B*
June	3	1	1	40	20	10	1*A*+10*B*

問題:ログからボットネットを同定せよ



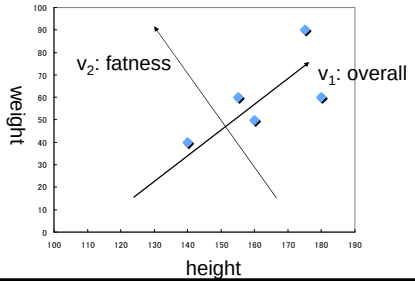
April	30	10	10	0	0	0	10*A* + 0*B*
May	9	3	3	4	12	6	3*A* + 3*B*
June	3	1	1	40	20	10	1*A*+10*B*
August	0	0	0	80	40	20	?
	A	?	?	B	?	?	

攻撃パターンは日々変化する

どのボットネットに属するか分からない

92 Honeypots

- Orthogonal Linear transformation, to reduce multidimensional data to a smaller set that contributes most to its variance by keeping principal components



直交基底

- 固有値

$$X = \begin{pmatrix} 30 & 10 & 10 & 0 & 0 & 0 \\ 9 & 3 & 3 & 12 & 6 & 3 \\ 3 & 1 & 1 & 40 & 20 & 10 \end{pmatrix} \begin{matrix} t_1 \\ t_2 \\ t_3 \end{matrix}$$

(s_1 s_2 s_3 s_4 s_5 s_6)

PCA

$\boldsymbol{u}_1$=(-.5 -.2 -.2 .7 .4 .2)

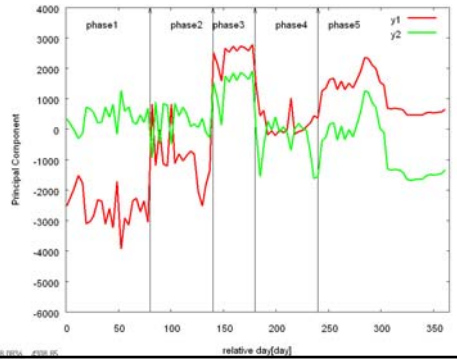
$\boldsymbol{u}_2$=(.8 .3 .3 .5 .2 .1)

$x_1 = y_1 \mathbf{u}_1 + y_2 \mathbf{u}_2 + x_0$
$= -26\ u_1 + 4\ u_2 + x_0$
$= (30.2\ \ 11\ \ 11\ \ 1.1\ \ -1\ \ -.5)$

Experimental Data

- Malware Dataset
  - CCC Data Set "Cyber Clean Center"
  - CCC (Japanese Governmental Organization) observes Backbone of tier-1 Provider.
  - 92 Honey pots
  - Duration: May 2008 – April 2009 (13 month)

2つのボットネットとその勢力変化



まとめ

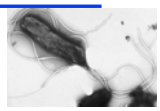
- Sonyのウェブサイトを攻撃していたAnonymousは　　を用いてDoS攻撃をしかけていた.
- ボットネットを対策には，ハニーポットによる検出や企業間の連携が必要である.
- CCCによる 90 台の　　のデータを主成分分析にかけて，
  - 少なくとも 4 つのBotnetが競合していた
  - 1年間に5つのフェーズが観測された

3. プライバシーを保護したピロリ菌疫学調査

菊池 浩明 （東海大）
佐久間 淳 （筑波大, JST）
三上 春夫 （千葉県がんセンター）

ヘリコバクター・

- *Helicobacter pylori*
  - 胃に感染するらせん状の細菌
  - 胃炎，胃潰瘍，十二指腸潰瘍の原因のひとつ
  - 40-50%の感染率(日本の40代以上 70%)
    先進国は低い
  - 発ガン性は認められているが，そのリスクはまだ明らかになっていない



http://ja.wikipedia.org

調査

- 患者-対象調査

要因	がん罹患	対象(無)	罹患率
ピロリ菌	a	b	a/(a+b)
未感染	c	d	c/(c+d)

- 相対危険度 (Relative Risk)

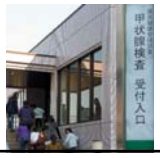
$$RR = \frac{a}{a+b} / \frac{c}{c+d} \approx \frac{ad}{bc}$$

- 統計量

$$\chi = \frac{\sqrt{N-1}((ad-bc) \pm N/2)}{\sqrt{(a+c)(b+d)(a+b)(c+d)}}$$

課題: 疫学調査とプライバシー

- 福島県子供の甲状腺検査
  - 18歳までの子供36万人対象（避難者含む）
  - 2年半で一巡，その後も定期的に生涯実施
  - (2011年10月9日朝日新聞)
- 福島男性の献血を拒否
  - 「福島県の方は放射線で遺伝子が傷ついている可能性」2011年5月東京ビッグサイト献血ブース
  - 「被ばく線量100mSvを超えた人」の献血制限を担当者誤解
  - (AERA 2011.6.13)



http://www.asahi.com/national/update/1009/TKY201110090195.html

既存の疫学調査の問題点

- 個人情報保護の考慮
  - 組織を超えて情報を照合できない
  - 「行政機関の保有する電子計算機処理に係る個人情報保護の法律」
- 従事者の同意が必要
  - 27万人中12,410人(4.5%)が追跡調査を拒否 (原子力発電施設等放射線業務従事者等に係わる疫学調査[1] p. 13)

研究目的: 安全な疫学調査

- 研究目的: 組織A, Bが互いのデータセットを秘匿して，相対危険度RRを求める

氏名	年齢	部位
菊池浩明	37	胃境界
小林 実	48	胃底部
斎藤 佑樹	35	幽門

組織A (千葉がんセンター)

氏名	年齢	検診日
中村 聡	45	2001
菊池浩明	37	2001
橋本 直樹	28	2002

組織B (厚生省・保健所)

加法　　性 (Homomorphic Property)

- 可換な図

$$\begin{array}{ccc} m & \xrightarrow{E} & E(m, r) \\ m' & & E(m', r') \\ \downarrow + & & \downarrow \times \\ m+m' & \xrightarrow{E} & E(m+m', r+r') \end{array}$$

- Privacy-preserving computations

$$E(m,r) \times E(m', r') = E(m+m', r+r')$$
$$E(m,r)^x = E(mx,rx)$$

セキュア内積プロトコル

A: X = (菊池, 小林, 斉藤, 中村) = (1, 0, 1, 1)

B: Y = (菊池, 小林, 斉藤, 中村) = (1, 1, 1, 0)

Xの暗号化 E(1)

E(1), E(0), E(1), E(1)

$c = E(1)^1 E(0)^1 E(1)^1 E(1)^0$
$= E(1*1)\ E(0*1)\ E(1*1)\ E(1*0)$
$= E(1 + 0 + 1 + 0)$
$= E(2)$

c

復号
D(c) = D(E(2)) = 2
= | X ∩ Y | 合計のみ分かる

データセット

- 千葉がんセンター疫学登録

	男性	女性	総数
2003	2,330	1,134	3,464
2004	2,610	1,242	2,852
2005	2,559	1,205	3,764
計	7,500	3,581	11,081

- 厚生省ピロリ菌データセット

	男性	女性	総数
2001 2002	2,671	5,206	7,877

照合結果

	がん患者数	非登録者	計
ピロリ菌	80	2,549	2,629
非保有者	346	106,988	107,334
計	426	2,999,574	3,000,000

相対危険度 RR = 9.70 (ピロリ菌はがんに9.7倍なりやすい)
有意性 χ = 17.81 (98%以上の確からしさで有意)

結論

- 被験者のプライバシー保護と，より詳細な調査が必要であるという矛盾した問題に対して，暗号プロトコルの適用を提案し，試験実装に基づいて実現可能であることを示した．
- がん登録とピロリ菌保有者という異なるデータベースを照合し，相関の大きさを算出した
- 大規模なデータへの適用，パフォーマンスの向上