IEEE SP2016 で面白かった論文

MWS2016意見交換会　ライトニングトーク

2016/5/30

早稲田大学　森　達哉

IEEE Symposium on Security and Privacy

- 2011年までカリフォルニア州オークランドで開催
- 2012年から同州の別の場所へ（サンフランシスコ、サンノゼ）
- The top of the top conferences（ウィンブルドン的存在)

Year	Rank 1			
	IEEE S&P	ACM CCS	USENIX Security	NDSS
2016	55/413(13.3%)			15.4%(60/389)
2015	13.5%(55/407)	19.8%(128/646)	15.7%(67/426)	16.9%(51/302)
2014	13%(44/334)	19.5%(114/585)	19%(67/350)	18.6%(55/295)
2013	12%(38/315)	19.8%(105/530)	15.9%(44/277)	18.8%(47/250)
2012	13%(40/307)	18.9%(80/423)	19.4%(43/222)	18%(46/258)
2011	11%(34/306)	14%(60/429)	17%(35/204)	20%(28/139)
2010	11.6% (31/267)	17.2%(55/320)	14.9%(30/202)	15.4%(24/156)

http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm

今年の投稿/採択数

- 投稿数: 411
  - Round1: 399
  - Round2: 205
  - Round3: 96
  - Round4: 55
    - 20 papers accepted without discussion
    - 76 papers discussed and 35 papers were accepted
- 採択率 = 55/411=13.4%
- Round3 に残った率 = 96/411 = 23.4%
- ざっくりとは $(1/2)^3$ =12.5%なので、$(1/2)^2$=25%のレベルの会議に通る論文のさらに上位半分

表彰された論文

- Distinguished Practical Paper Award
  - Security Analysis of Emerging Smart Home Applications (IoT)
- Distinguished Student Paper Award
  - Verifiable ASICs (hardware)
  - pASSWORD tYPOS & How to Correct Them Securely (usable security)
- Distinguished Paper Award
  - A2: Analog Malicious Hardware (hardware)

今日ざっと紹介する論文

1. **pASSWORD tYPOS and How to Correct Them Securely**
2. **SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis**
3. **Users Really Do Plug in USB Drives They Find**
4. **Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways**

※詳細は論文をご参照ください

紹介しないが面白かった論文

- A2: Analog Malicious Hardware
- Helping Johnny to Analyze Malware: A Usability-Optimized Decompiler and Malware Analysis User Study
- You Get Where You're Looking For: The Impact Of Information Sources On Code Security
- Following Devil's Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS
- Inferring User Routes and Locations using Zero-Permission Mobile Sensors
- No Pardon for the Interruption: New Inference Attacks on Android Through Interrupt Timing Analysis
- SoK: Lessons Learned From Android Security Research For Appified Software Platforms
- Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems
- Domain-Z: 28 Registrations Later
- Seeking Nonsense, Looking for Trouble: Efficient Promotional-Infection Detection through Semantic Inconsistency Search
- Cloak of Visibility: Detecting When Machines Browse a Different Web

pASSWORD tYPOS and How to Correct Them Securely

- Typo を許容するパスワードの提案
- User study により、typo のパターンを調査した
  - Caps lock が多い。その他。
- Dropbox の実サービスで全ユーザを対象にタイポのパターンを調査した
  - パスワードではなく、ミスのパターンだけ記録した
  - 実際に typo correction をしたわけではない
  - Typo の Top-3 が全認証ミスの3%を占めた⇒これらを救うことが出来る
- Top-3 を許容したときに、どの程度セキュリティ強度が変わるか⇒ leaked password sets を使ってシミュレーション
  - セキュリティ強度はまったく変わらない、あるいはほとんど変わらない
  - すべてのパスワードを correction しないという heuristics はあり

SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis

- おなじみ UCSB 一派によるバイナリ解析の SoK 論文
- 背景: DARPA cyber grand challenge (CGC)
  - https://cgc.darpa.mil/
- 過去に発表されたバイナリ解析技術を “systemize” することが目的
  - 静的解析、動的シンボリック実行解析 (concolic)
  - すべての解析技術を実装しなおし、統一的なツールとして使えるようにした
  - ユーザビリティも考慮 (Python から使える)
  - 各解析を自由に組み合わせ出来るところが良い
- CGC のデータを利用して評価
- http://angr.io

Users Really Do Plug in USB Drives They Find

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

Security

Half of people plug in USB drives they find in the parking lot

Why do we even bother with security software?

11 Apr 2016 at 21:09, Shaun Nichols

A new study has found that almost half the people who pick up a USB stick they happen across in a parking lot plug said drives into their PCs.

Researchers from Google, the University of Illinois Urbana-Champaign, and the University of Michigan, spread 297 USB drives around the Urbana-Champaign campus. They found that 48 percent of the drives were picked up and plugged into a computer, some within minutes of being dropped.

出典：http://www.theregister.co.uk/2016/04/11/half_plug_in_found_drives/

この論文でやったこと

- 297個のUSBドライブを1日2回、30箇所で落とした（キャンパス内）
- 落としたUSBドライブに実際にアクセスされたかを調査
  - Bad USB だった場合、ドライブアクセス＝マルウェア感染等のリスクあり
- 結果：290個は拾われた。少なくとも135個はファイルを開かれた（偽装ファイルでのビーコン）

落としたUSBドライブの種類

(a) Unlabeled drive

(b) Drive with keys

(c) Drive with return label

(d) Confidential drive

(e) Exam solutions drive

出典：SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis Y Shoshitaishvili, R Wang, C Salls, N Stephens, M Polino, A Dutcher, J Grosen, S Feng, C Hauser, C Kruegel, G Vigna IEEE symposium on Security and Privacy (SSP) 2016.

ドライブの中身

USB-STICK

Name	Date Modified	Size	Kind
Documents	Apr 26, 2015, 1:21 AM	--	Folder
reflective_essay_02.docx.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
resume_old.pdf.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
resume.pdf.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
Math Notes	Apr 26, 2015, 1:21 AM	--	Folder
2-13.docx.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
2-15.docx.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
2-20.docx.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
2-27.docx.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
3-5.docx.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
3-7.docx.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
Pictures	Apr 26, 2015, 1:21 AM	--	Folder
Winter Break	Apr 26, 2015, 1:21 AM	--	Folder
0101150001.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
0101150002.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
0101150117.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
0106151415.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1224142242.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1224142256.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1224142347.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1226141212.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1226141431.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1226141505.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1226141506.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1230141922.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1231142356.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1231142357.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML
1231142359.jpg.html	Apr 26, 2015, 1:21 AM	13 KB	HTML

(a) **Personal Contents**—Unlabeled, keys, and return label drives contain these files.

USB-STICK

Name	Date Modified	Size	Kind
2015_proj1	Apr 26, 2015, 2:09 AM	--	Folder
feb12proposalA.pptx.html	Apr 26, 2015, 2:09 AM	13 KB	HTML
patent_app_0217.pdf.html	Apr 26, 2015, 2:09 AM	13 KB	HTML
employee	Apr 26, 2015, 2:09 AM	--	Folder
termination_notice_4317_05_17_2015.pdf.html	Apr 26, 2015, 2:09 AM	13 KB	HTML
termination_notice_4318_05_17_2015.pdf.html	Apr 26, 2015, 2:09 AM	13 KB	HTML
strategy	Apr 26, 2015, 2:09 AM	--	Folder
0417_meeting_notes.pdf.html	Apr 26, 2015, 2:09 AM	13 KB	HTML
0425_meeting_notes.pdf.html	Apr 26, 2015, 2:09 AM	13 KB	HTML
plan_for_2015_2016.pptx.html	Apr 26, 2015, 2:09 AM	13 KB	HTML

(b) **Business Contents**—Confidential drives contain these files.

USB-STICK

Name	Date Modified	Size	Kind
fa10	Apr 26, 2015, 1:52 AM	--	Folder
examA.pdf.html	Apr 26, 2015, 1:52 AM	13 KB	HTML
examB.pdf.html	Apr 26, 2015, 1:52 AM	13 KB	HTML
solutionsA.pdf.html	Apr 26, 2015, 1:52 AM	13 KB	HTML
solutionsB.pdf.html	Apr 26, 2015, 1:52 AM	13 KB	HTML
fa11	Apr 26, 2015, 1:52 AM	--	Folder
fa12	Apr 26, 2015, 1:52 AM	--	Folder
fa13	Apr 26, 2015, 1:52 AM	--	Folder
fa14	Apr 26, 2015, 1:52 AM	--	Folder
fa15	Apr 26, 2015, 1:52 AM	--	Folder
sp10	Apr 26, 2015, 1:52 AM	--	Folder
sp11	Apr 26, 2015, 1:52 AM	--	Folder
sp12	Apr 26, 2015, 1:52 AM	--	Folder
sp13	Apr 26, 2015, 1:52 AM	--	Folder
sp14	Apr 26, 2015, 1:52 AM	--	Folder
sp15	Apr 26, 2015, 1:52 AM	--	Folder

(c) **Exam Contents**—Exam drives contain these files. Note that only one folder is expanded for brevity; all other folders contain the same file names.

いずれもHTMLファイル
Javascript 等のコードは一切入っていない

出典：SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis Y Shoshitaishvili, R Wang, C Salls, N Stephens, M Polino, A Dutcher, J Grosen, S Feng, C Hauser, C Kruegel, G Vigna IEEE symposium on Security and Privacy (SSP) 2016.

調査方法

- ファイルを開いた時点で種明かし。インターネット調査による協力を依頼（10ドルの謝礼付き）

1) **Demographics.** We asked demographic questions fro SurveyMonkey's question bank (e.g., age, sex, and lev of education) [17].
2) **Affiliation.** We asked a participant their affiliation wit the University of Illinois (e.g., faculty, staff, or student
3) **Previous Knowledge.** We asked if the participant ha previously heard about the study. We later discarded responses where the user had pre-existing knowledge.
4) **Motivation.** We asked the participant why they picked up the flash drive and if external appearance or any other factor affected their decision.
5) **Computer Expertise and Behaviors.** We asked questions from the SeBIS Survey [12] to measure the participants' computer and computer security behaviors and three questions from another study [27] to measure their computer expertise.
6) **Risk Attitude.** We presented questions from the DOSPERT Survey [4], a standardized survey for measuring how likely a participant is to take part in risky behavior.
7) **Internet Usage.** We asked how much time the user spent online on a weekly basis. We asked this because previous studies have found that time spent on the Internet and visits to certain types of websites correlate with cybercrime victimization or malware encounters [6], [27], [32], [51], [54].

出典：SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis Y Shoshitaishvili, R Wang, C Salls, N Stephens, M Polino, A Dutcher, J Grosen, S Feng, C Hauser, C Kruegel, G Vigna IEEE symposium on Security and Privacy (SSP) 2016.

攻撃成功要因

Category	Drives Opened		p
Drive Type			
Confidential	29/58	(50%)	0.72
Exams	30/60	(50%)	0.71
Keys	32/60	(53%)	0.47
Return Label	17/59	(29%)	0.10
None	27/60	(45%)	–
Location Type			
Academic Room	25/58	(43%)	0.35
Common Room	26/60	(43%)	0.36
Hallway	24/59	(41%)	0.23
Outside	28/60	(47%)	0.58
Parking Lot	32/60	(53%)	–
Location Geography			
North	49/100	(49%)	0.26
South	46/97	(47%)	0.36
Main	40/100	(40%)	–
Time of Day			
Morning	71/149	(48%)	0.52
Afternoon	64/148	(43%)	–
Day of Week			
Tuesday	58/147	(39%)	0.05
Tuesday (no Return Label)	41/88	(47%)	0.57
Monday	77/150	(51%)	–

Return label がつくと成功率が低くなる他はあまり成功率を変えない

出典：SoK: (State of) The Art of War: Offensive Techniques in Binary Analysis Y Shoshitaishvili, R Wang, C Salls, N Stephens, M Polino, A Dutcher, J Grosen, S Feng, C Hauser, C Kruegel, G Vigna IEEE symposium on Security and Privacy (SSP) 2016.

その他調査項目

- どのファイルを開いたか
- OS/ブラウザ
- ユーザの用心・動機・リスク管理・デモグラフィ、知識について

（意外な）ユーザの用心方法

「大学のパソコンを生贄にした」

議論

- Q: なぜ倫理委員会(IRB)が許したのか?
- A: campus police 等、ステークホルダーとの調整を念入りに進めた。リスクが無いように細心の注意を払った。

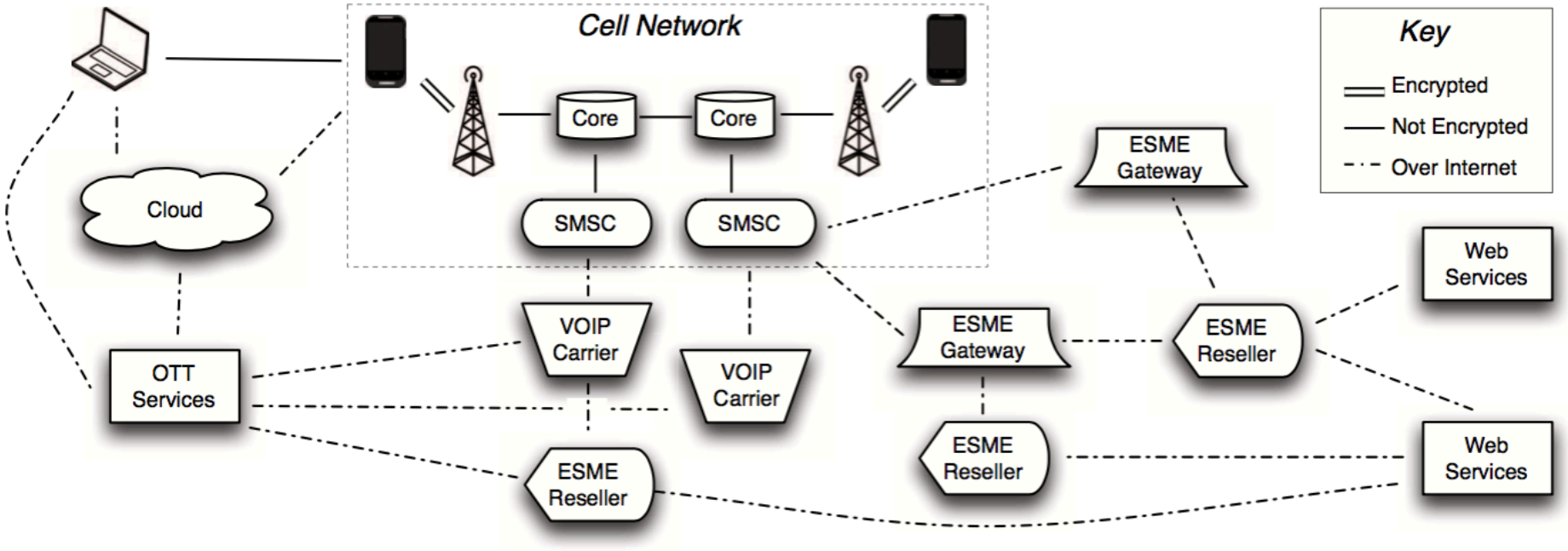
- Q: 大学（イリノイ大学）ではセキュリティ教育はあるのか？
- A: 標準的なものは恐らくやっている

Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways

- SMS の public gateway サービスをクロールし、SMS データを収集
  - 14ヶ月で400,000メッセージ
  - 400個の電話番号、28カ国
- サービス毎の OTP やverification code のパターンを分析 ➔ ランダムではないことがわかった
- 平文でセンシティブなデータが流れているケースが多い
- SMSのアカウント生成に使われていると考えられる
  - 2要素認証
- スパムやフィッシングもある

出典: B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor and K. Butler, Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways, Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2016.

SMS ecosystem



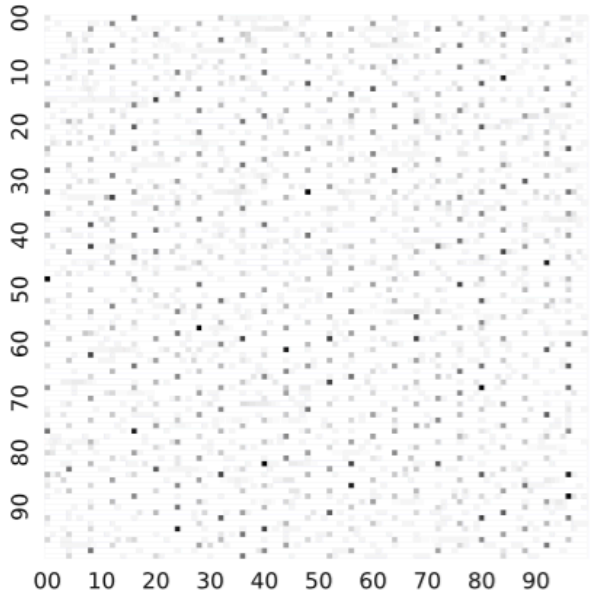
ESME = External Short Message Entities

出典: B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor and K. Butler, Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways, Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2016.

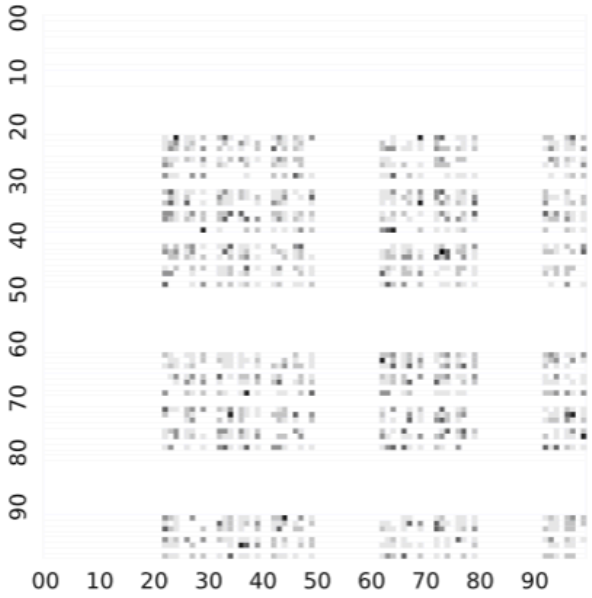
Public SMS gateway の例

論文中に示されているURLを参照

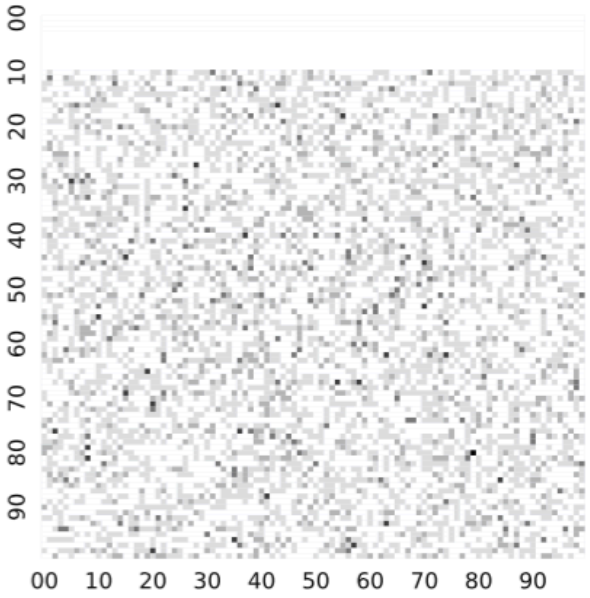
各サービスのコードの分析例



(a) WeChat



(b) Talk2



(c) LINE

出典: B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor and K. Butler, Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways, Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2016.

倫理に関する議論

- IRBが承認（と、確か口頭発表では述べていたと思うが、論文には書いていない。Ethical consideration の記載はあり）

- 単純には Public なデータであり、かつ opt-in であるので、問題は無いと考えられる
- ただし業者等は public になっていることを知らずにユーザに情報を送っている
  - バルクに送信しているデータであれば、損失になる情報では無いとも考えられる
- データから得られたパスワード等のデータを他人に渡してはいない

- この論文をきっかけに議論が促進されることを期待・・・というあたりで査読者に許してもらった

倫理の議論の続きは秋山さんのLTにて