SCIS2017 MWS企画セッション (MWSCIS)

研究活動とResponsible disclosure

研究倫理に関して我々の置かれている状況

NTTセキュアプラットフォーム研究所
秋山 満昭

2017.1.27

査読コメント:「Ethics(倫理)について議論せよ」

とある難関会議の査読結果
(ハニーポットに関する研究)

The authors should include a note on **ethics** for their honeypots. In effect, they run a compromised site that is actively used in serving exploits to users. **There are arguments** to be made on both sides: this **causes harm to users**; but…

つまり「Ethicsを考慮した研究」を進め、
論文中で適切に議論をしなければならない

Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer (USENIX Security'13)

BBC News Sport More Search

NEWS

Home Video World Asia UK Business Tech Science More

Technology

Car key immobiliser hack revelations blocked by UK court

29 July 2013 | Technology Share

A High Court judge has blocked three security researchers from publishing details of how to crack a car immobilisation system.

Megamos Crypto transponders are built into car keys to disable the vehicles' engine immobilisers

German car maker Volkswagen and French defence group Thales obtained the interim ruling after arguing that the information could be used by criminals.

http://www.bbc.com/news/technology-23487928

なぜこのようなことが起きてしまったのか？

情報開示手順は正しかったか？

Questions

- Q1: 世の中ではどのようなEthicsのコンセンサスがあるのか？

- Q2: どのようにEthicsを議論し、実践すれば良いか？

サイバーセキュリティの先進的な研究を
萎縮することなく促進したい

世の中の研究倫理に関する動向:
生物医学からサイバーセキュリティへの発展

- 研究倫理のガイドライン
- 国際ワークショップ開催
- 国際会議CFPでの明記
- 国際会議でのパネルディスカッション

Belmont Report (1978)

- 生物医学/行動科学分野の研究倫理に関するガイドライン
  - 米国政府関連の委員会（National Commission for the Protection of Human Subjects）が策定
- 人間被験者（Human subjects）を用いた研究が主な対象
- 中核となる倫理3原則
  - Respect for Persons（人格の尊重）
    - 本人が自由に意思決定することを尊重
    - 実験参加の自由、適切なインフォームドコンセント
  - Beneficence（恩恵）
    - 患者/被験者や広く世の中に対して恩恵があること
  - Justice（正義）
    - 個人の平等な取り扱い（研究対象の公正な選択/平等な負担、研究の恩恵の平等な配分）

Menlo Report（2012）

- コンピュータ/情報のセキュリティにおける研究倫理のガイドライン/フレームワーク
  - アメリカ合衆国国土安全保障省（DHS）が公開
- 中核となる倫理原則
  - [Belmont Reportから継承]
    Respect for Persons, Beneficence, and Justice
  - [Menlo Reportで新たに追加]
    Respect for Law and Public Interest
    - 法令遵守、公共の利益を尊重
    - 説明責任（Responsible Disclosure）と評価/実行手順の透明性

CREDS (2013) / CREDSII (2014) / NS-Ethics (2015)

- CREDS (2013) / CREDS II (2014)
  - https://www.caida.org/workshops/creds/
  - IEEE S&Pの併設ワークショップ
  - “ethics-by-design”が目標
  - ベストプラクティス/ケーススタディの共有
  - 過去研究のEthicsの観点からの再検証
  - CREDS tool (2015)
    - Cyber Risk Ethics Decision Support tool
- NS-Ethics (2015)
  - http://conferences.sigcomm.org/sigcomm/2015/netethics.php
  - ACM SIGCOMMの併設ワークショップ
  - ネットワーク観測を中心とした話題

[参考] CREDSでの議論

- “Ethics in Security Research: Which lines should not be crossed?” Sebastian Schrittwieser, Martin Mulazzani and Edgar Weippl
  - Do not harm humans actively
  - Do not watch bad things happening
  - Do not perform illegal activities to harm illegal activities
  - Do not conduct undercover research

CFP

USENIX Security'16

Human Subjects and Ethical Considerations

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should

1. Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (IRB)—if applicable).
2. Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

If the submission deals with vulnerabilities (e.g., software vulnerabilities in a given program or design weaknesses in a hardware system), the authors need to discuss in detail the steps they plan to take to address these vulnerabilities (e.g., by disclosing vulnerabilities to the vendors). The same applies if the submission deals with personal identifiable information (PII) or other kinds of sensitive data. If a paper raises significant ethical and legal concerns, it might be rejected based on these concerns.

IEEE S&P'17

Human Subjects and Ethical Considerations

Drawn from the USENIX Security 2016 CFP

NTT

「Panel on Research Ethics」 at USENIX Security 2015

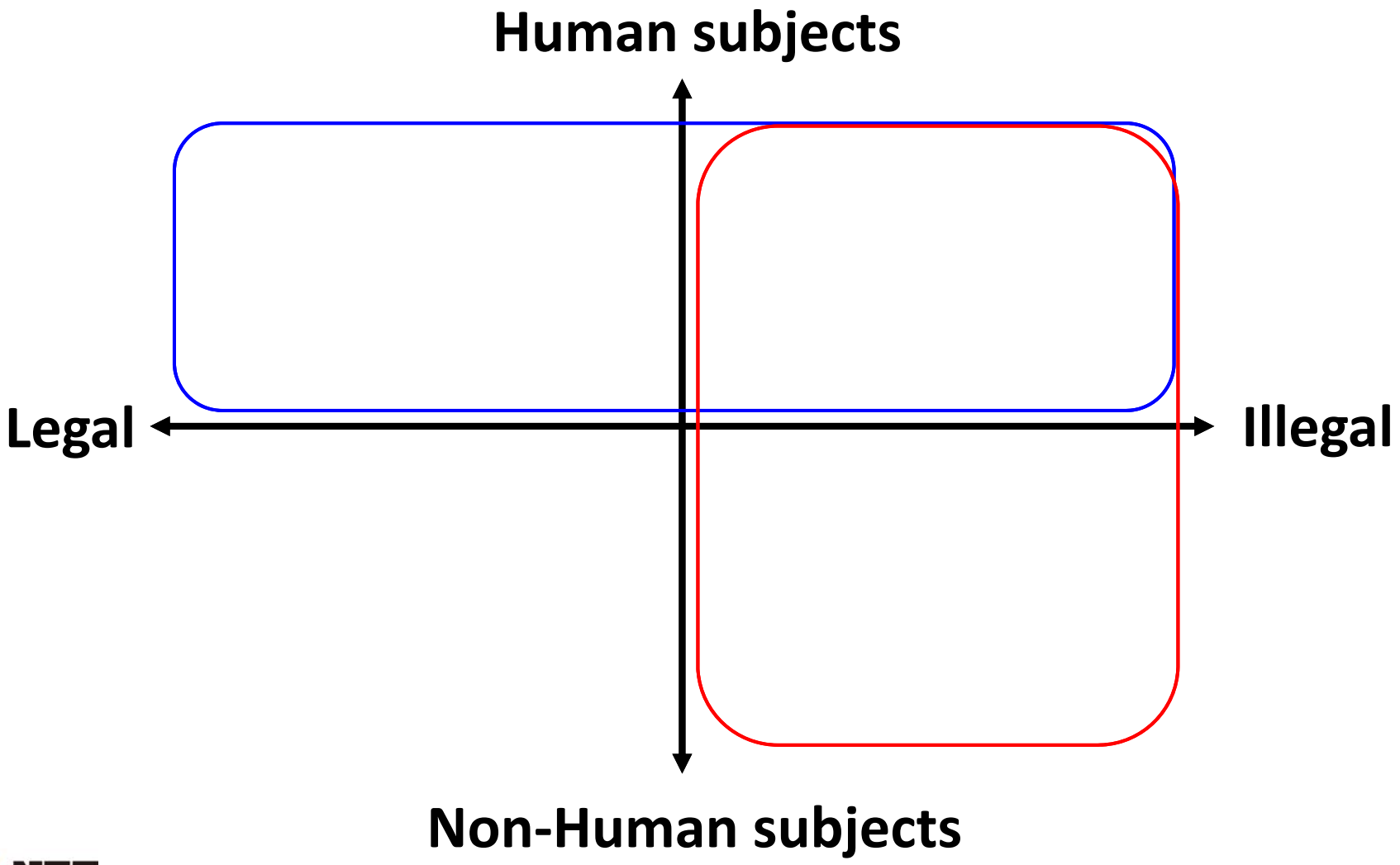
- パネリスト
  - Michael Bailey, Erin Kenneally, Niels Provos, Stuart Schechter

- 「Ethicsに問題があり Reject された論文が存在する」
- 「PCはEthicsに関する判断をしない」
  - （PCではない、別の）専門家に判断を委ねる
  - 研究倫理委員会（Institutional Review Board, IRB）の承認が得られているか？

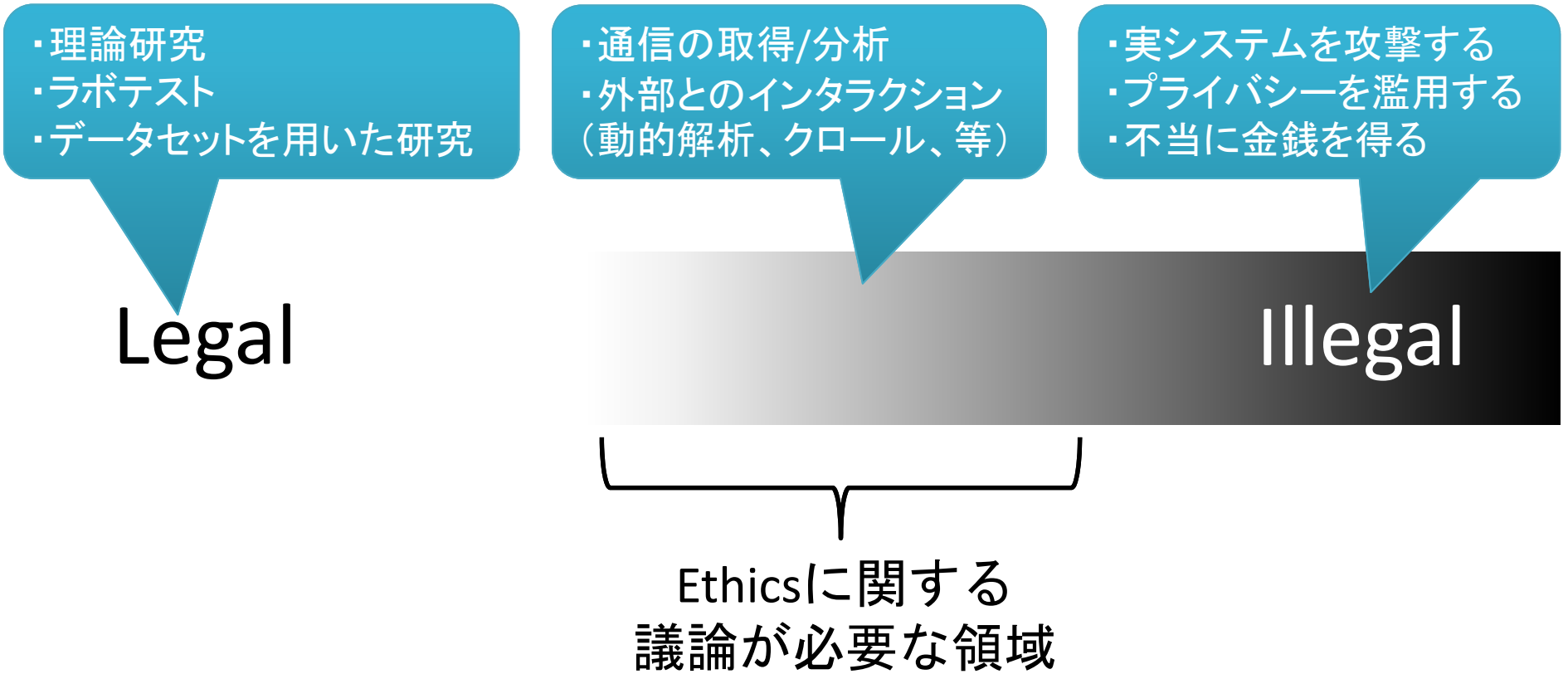
世の中の研究倫理に関する動向:
生物医学からサイバーセキュリティへの発展

- 研究倫理のガイドライン
  - **Belmont Report (1978)**
  - **Menlo Report (2012)**
- 国際ワークショップ開催
  - **CREDS (2013), CREDSII (2014), NS-Ethics (2015)**
- 国際会議でのパネルディスカッション
  - **「Panel on Research Ethics」USENIX Security (2015)**
- 国際会議CFPでの明記
  - **「Human Subjects and Ethical Considerations」USENIX Security (2016)**
  - **「Human Subjects and Ethical Considerations」IEEE S&P (2016)**

対象とする領域



違法/適法の狭間のEthics



革新的な研究は “グレーな領域” を攻めている

- Your Botnet is My Botnet: Analysis of a Botnet Takeover [ACM CCS’09]
- ZMap: Fast Internet-Wide Scanning and its Security Applications [USENIX Security’13]

ケーススタディ: Your Botnet is My Botnet: Analysis of a Botnet Takeover [ACM CCS'09]

- シンクホールでC&Cサーバのドメインを乗っ取り、感染ホストから送信される個人情報を収集

```
POST /accounts/LoginAuth
Host:  www.google.com
POST_FORM:
Email=test@gmail.com
Passwd=test
```

感染ホストから送られてきたデータ(例)

Data Type	Data Items (#)
Mailbox account	54,090
Email	1,258,862
Form data	11,966,532
HTTP account	411,039
FTP account	12,307
POP account	415,206
SMTP account	100,472
Windows password	1,235,122

収集した個人情報

- Ethicsの議論
  - 「新たな被害の発生を抑える様々な努力をしている」
  - 「ステークホルダ/法執行機関(ISP, DoD, FBI)と協力している」

ケーススタディ：ZMap: Fast Internet-Wide Scanning and its Security Applications [USENIX Security'13]

- インターネットを超高速にスキャンする技術
- Ethicsに関する議論
  - インターネットに与える悪影響が少ないことを主張
  - 研究者に対してスキャンのガイドラインを提示
  - 著者が実際に経験した、ユーザからの応答（苦情）も共有

1. Coordinate closely with local network admins to reduce risks and handle inquiries.
2. Verify that scans will not overwhelm the local network or upstream provider.
3. Signal the benign nature of the scans in web pages and DNS entries of the source addresses.
4. Clearly explain the purpose and scope of the scans in all communications.
5. Provide a simple means of opting out, and honor requests promptly.
6. Conduct scans no larger or more frequent than is necessary for research objectives.
7. Spread scan traffic over time or source addresses when feasible.

スキャンのガイドライン

Responses from 145 users

Blacklisted 91 entities
(3.7 M total addresses)

15 hostile responses

2 cases of retaliatory traffic

Entity Type	Responses
Small Business	41
Home User	38
Corporation	17
Academic Institution	22
Government	15
ISP	2
Unknown	10
Total	**145**

ユーザからの応答

- 革新的な研究をするためには
  ”グレーな領域” に踏み込まざるを得ない

- そのためには、われわれ自身がEthicsについて論じる（論じることができる能力/研究力を身につける）必要がある

著名論文におけるEthicsの議論

- サイバーセキュリティ分野においてトップカンファレンスの一つである USENIX Security の論文を調査
  - Ethicsに関わる論文を抽出
  - Ethics関わる対処/記述を体系化

Ethical Considerations: We took careful protections to ensure that our live data collection did not breach users' anonymity. In particular, *we captured only buffered*

6 Ethical Discussion

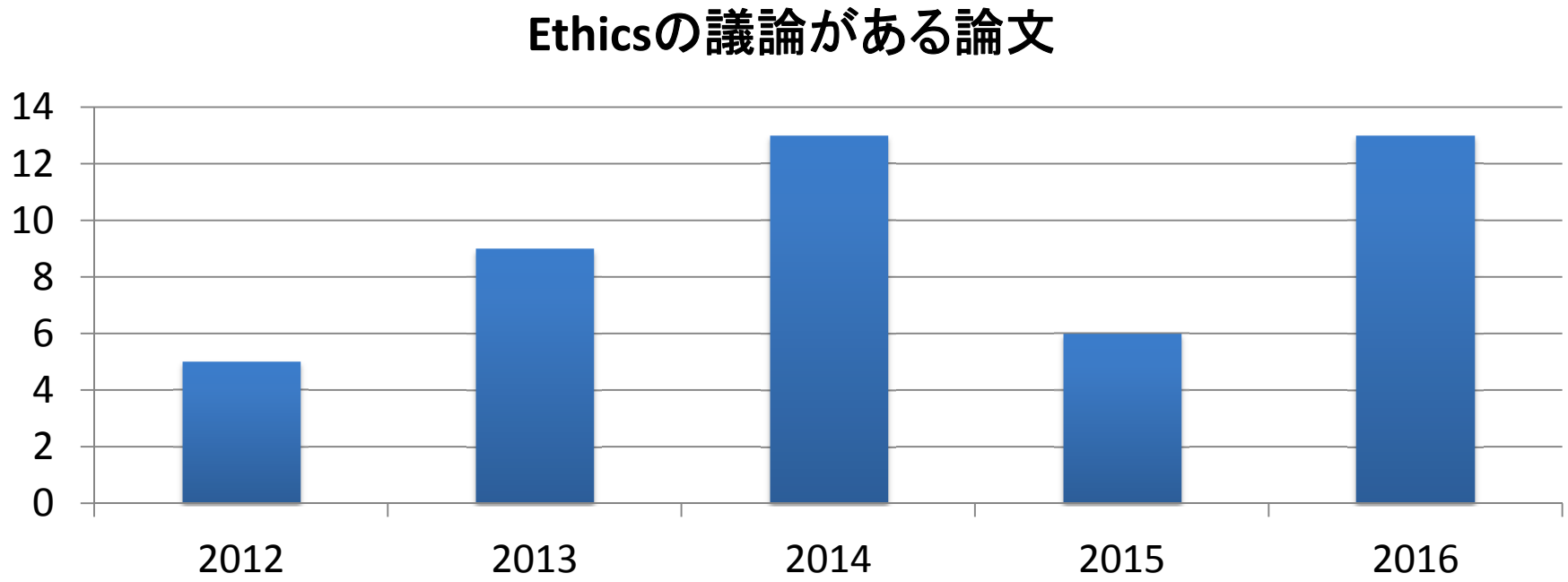
7 Discussion and Ethical Considerations

Human subjects and ethics. Our study was approved by the human subjects review boards (IRBs) of our institutions before any research activities began. We obtained

[1]Our work received approval from our local IRB review board.

Ethicsの言及がある論文数

USENIX Securityの過去5年間（2012-2016）で発表された論文 全293本を調査
→ **<u>計46本でEthicsの議論があった</u>**



※ キーワード（ethics/ethical/IRB等）ベースで大まかに抽出したため正確な数字ではない可能性あり

Ethics議論の種別

- 同意/承認の獲得
  - ユーザ(被験者)の同意
  - サービス事業者の承認
  - 研究倫理委員会の承認
- 手順の正当性
  - Responsible disclosure
  - ポリシー/ガイドラインの準拠
  - 匿名化
  - 適法性
  - 代替手段なし
- リスク/被害のコントロール
  - 新たな被害は発生しない
  - リスクの最小化
- 利益
  - ベストプラクティスの共有
  - 公益性
- その他
  - Human subjectsではない
  - 研究用途

具体例: 同意/承認の獲得

- [サービス事業者の承認] We directly contacted Twitter to receive permission to conduct our study [1]
- [ユーザ(被験者)の同意] We obtained informed written or verbal consent from all participants, both to participate in the study as well as to have the interviews audio recorded. [2]
- [研究倫理委員会の承認] The studies have received an approval from our institutional ethics review board. [3]
- [(例外)] Our Universities do not have an IRB, but the study conformed to the strict data protection law of Germany and informed consent was gathered from all participants [4]
- [(例外)] We worked with the director of UC San Diego's Human Research Protections Program, who certified our study as exempt from IRB review. [5]

具体例: 手順の正当性

- [匿名化] We took careful protections to ensure that our live data collection did not breach users' anonymity. [6]
- [ポリシー・ガイドラインの準拠] All telemetry data is subject to strict privacy policies and participants can opt out by changing their settings [7]
- [ポリシー・ガイドラインの準拠] We followed the guidelines for ethical scanning behavior outlined by Durumeric et al. [8]
- [Responsible disclosure] We reported all the attacks discussed below to the software vendors affected in the last week of August 2013. [9]

具体例: リスク/被害のコントロール

- [リスクの最小化] Following the ethical hacking practice, we immediately removed the app from App Store [10]
- [新たな被害は発生しない] We use the passwords alone, excluding usernames and email addresses. [11]
- [新たな被害は発生しない] This data is already broadly available [12]

具体例: その他

- [研究用途] We followed the ethical practice and never utilized the leaked passwords for reasons other than understanding the overall statistical observation of passwords [13]
- [Human subjectではない] This work is not considered human subjects research [7]

具体例で引用した論文

- [1] Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse, USENIX Security 2013
- [2] Investigating the Computer Security Practices and Needs of Journalists, USNEIX Security 2015
- [3] Privacy in Epigenetics: Temporal Linkability of MicroRNA Expression Profiles, USNEIX Security 2016
- [4] An Empirical Study of Textual Key-Fingerprint Representations, USENIX Security 2016
- [5] Measuring the practical impact of DNSSEC Deployment, USNEIX Security 2013
- [6] Never Been KIST: Tor's Congestion Management Blossoms with Kernel-Informed Socket Transport, USENIX Security 2014
- [7] Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness, USENIX Security 2013
- [8] You've Got Vulnerability: Exploring Effective Vulnerability Notifications, USENIX Security 2016
- [9] The Emperor's New Password Manager: Security Analysis of Web-based Password Managers, USENIX Security 2014
- [10] Jekyll on iOS: When Benign Apps Become Evil, USENIX Security 2013
- [11] How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation, USENIX Security 2012
- [12] PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs, USENIX Security 2012
- [13] A Large-Scale Empirical Analysis of Chinese Web Passwords, USENIX Security 2014

Questions and Answers

- Q1: 世の中ではどのようなEthicsのコンセンサスがあるのか？
  - **Belmont Reportをサイバーセキュリティに拡張したMenlo Reportに原則が規定**
  - **さらに精緻な議論/個別事例の議論がCREDS/CREDSII/NS-ethicsなどの会議で実施**

- Q2: どのようにEthicsを議論し、実践すれば良いか？
  - **トップカンファレンスの最先端研究事例から学べる**

課題・提案

- 課題1：研究倫理委員会を持っている研究組織は？サイバーセキュリティの審議事例があるか？
  - 特に企業においては設置されるケースが少ない
  - 設置されていた場合でも、サイバーセキュリティに知見はあまりない
- 課題2：単一の研究組織がEthicsの知見を蓄積し、判断するのは難しい。
  - 巨大な大学/研究機関でない限り、知見が十分に蓄積されない
- 提案：学会/研究コミュニティでの議論を、Ethicsに関する判断に活用できないか？
  - ガイドライン、研究倫理委員会、、、