Innovative R&D by NTT

MWS意見交換会
「Ethicsを議論しよう」

NTTセキュアプラットフォーム研究所
秋山 満昭

2016.5.30

査読コメント:
「Ethicsについて議論せよ」

私が昨年投稿した国際会議の査読コメントより抜粋

The authors should include a note on **ethics** for their honeypots. … . **There are arguments** to be made on both sides: this **causes harm to users**; but the overall impact is minimal compared to …

→ Ethicsの議論が査読結果に影響を与える

著名国際会議論文における記述
(USENIX Security 2014/2015より)

Innovative R&D by NTT

7 Discussion and Ethical Considerations

4.5 Measurement ethics

We have been careful to design experiments that we believe are both consistent with current U.S. legal doctrine and are fundamentally ethical as well. While it is beyond the scope of this paper to

In our study we were particularly careful to work within legal and ethical boundaries. First, we obtain firm-

6 Ethical Discussion

Using leaked passwords raises ethical concerns. We believe our use of such sets in this research is justifiable because the password sets are already available publicly

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

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.

NTT

研究領域とEthicsの議論

Innovative R&D by NTT

・データセットを用いた研究
・ラボテスト

・通信の取得/分析
・外部とのインタラクション
（動的解析、クロール、等）

・攻撃を仕掛ける
・プライバシーの濫用
・不当に金銭を得る

Ethicsに関する
議論が必要な領域

NTT

革新的な研究は “グレーな領域”を攻めている

Innovative R&D by NTT

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

NTT

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

- C&Cサーバのドメインをシンクホールにより乗っ取って、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」
  - 「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 [Security'13]

Innovative R&D by NTT

- 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

NTT

- 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について論じる必要がある

著名国際会議論文における記述

Innovative R&D by NTT

7 Discussion and Ethical Considerations

4.5 Measurement ethics

We have been careful to design experiments that we believe are both consistent with current U.S. legal doctrine and are fundamentally ethical as well. While it is beyond the scope of this paper to

In our study we were particularly careful to work within legal and ethical boundaries. First, we obtain firm-

6 Ethical Discussion

Using leaked passwords raises ethical concerns. We believe our use of such sets in this research is justifiable because the password sets are already available publicly

Ethical Considerations: We took careful protections to ensure that our liv… anonymity. In p…

IRB（研究倫理委員会）の承認を得ている

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.

NTT

しかし、日本国内の現状は

- 研究倫理委員会は「生命・医療倫理」を主としている
  - 医療・バイオ系学部を保有する大学や研究機関には必ず設置されている
- コンピュータサイエンスを扱った事例で公知のものは多くない
- またそもそも倫理委員会を保有しない組織も多い（企業など）

提案

- 研究コミュニティにおいて組織横断的にサイバーセキュリティの研究倫理について議論・判断したい
  - MWSは日本のサイバーセキュリティ研究者が揃っている最良の場
  - 研究倫理委員会を持たない組織も、“自信を持って”研究ができる
- MWS2016の企画セッション/パネルディスカッションで改めて議論したい
  - 世の中の動向、文献、方針、、、
  - そのように組織として運用するか