

Connecting the .dotfiles: Checked-In Secret Exposure with Extra (Lateral Movement) Steps

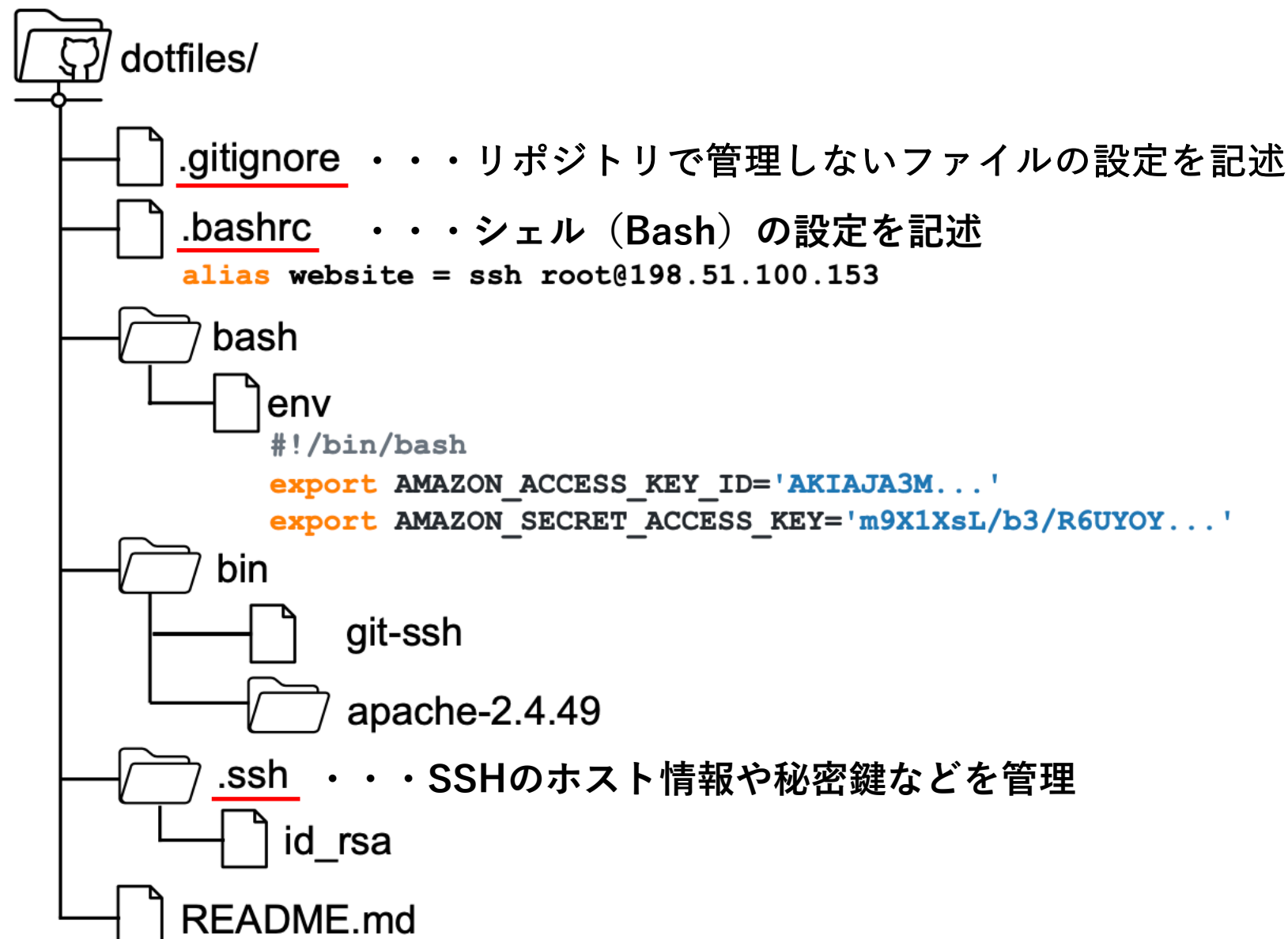
Gerhard Jungwirth,^{*} Aakanksha Saha,^{*} Michael Schröder,^{*} Tobias Fiebig,[‡] Martina Lindorfer,^{*} and Jürgen Cito^{*}
^{*}TU Wien, Vienna, Austria [‡]Max-Planck-Institut für Informatik, Saarbrücken, Germany

Proceedings of 20th International Conference on Mining Software Repositories (MSR '23)
pp. 322-333

ドットファイル（隠しファイル）

ソフトウェアの動作環境などに関する設定ファイル

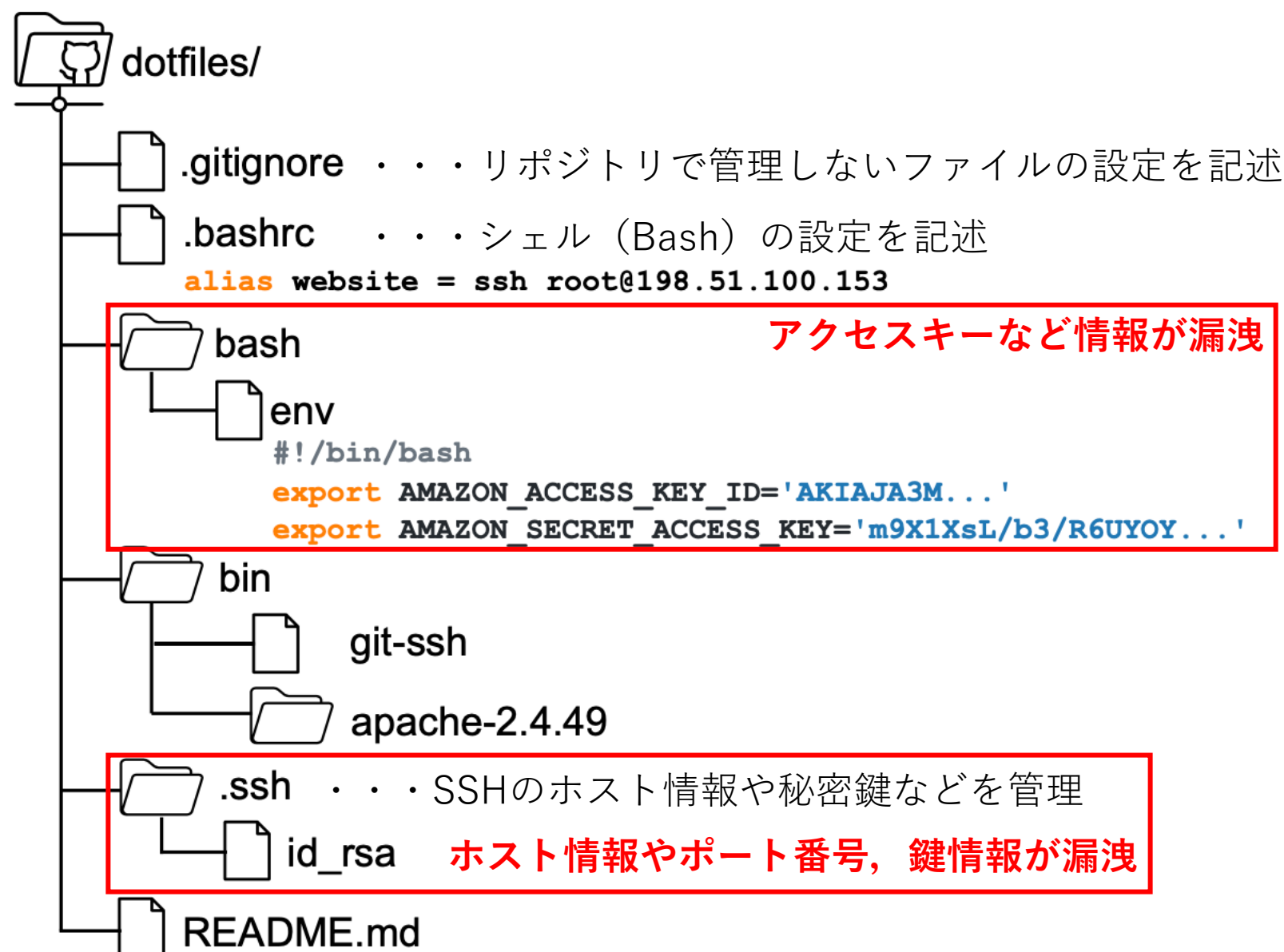
- 最近、GitHubリポジトリでドットファイルが公開管理されることが増加している → 環境の再現性が向上



ドットファイル（隠しファイル）

ソフトウェアの動作環境などに関する設定ファイル

- サイバー攻撃者にとって有利となる情報が公開されるケースが発生^[42] : <https://twitter.com/SchizoDuckie/status/1474087696247279626?s=20>



研究目的

ユーザのドットファイルに対する認識や考えを明らかにすること

- 明白な機密情報でなくともセキュリティプライバシーの問題発生を増長させる可能性がある

Research Question

- (RQ1) ドットファイルの共有によるセキュリティプライバシーへの影響は何か？
- (RQ2) ドットファイルを共有するおもな動機は何か？
- (RQ3) ドットファイル共有による影響をリポジトリ所有者はどの程度認識しているのか？

対象リポジトリ

| GitHubにホストされている124,230リポジトリを対象

- リポジトリ名もしくは説明文に**dotfiles**キーワードを含む
 - キーワード：Dotfile, Dotfiles, dotfile, dotfilesなど

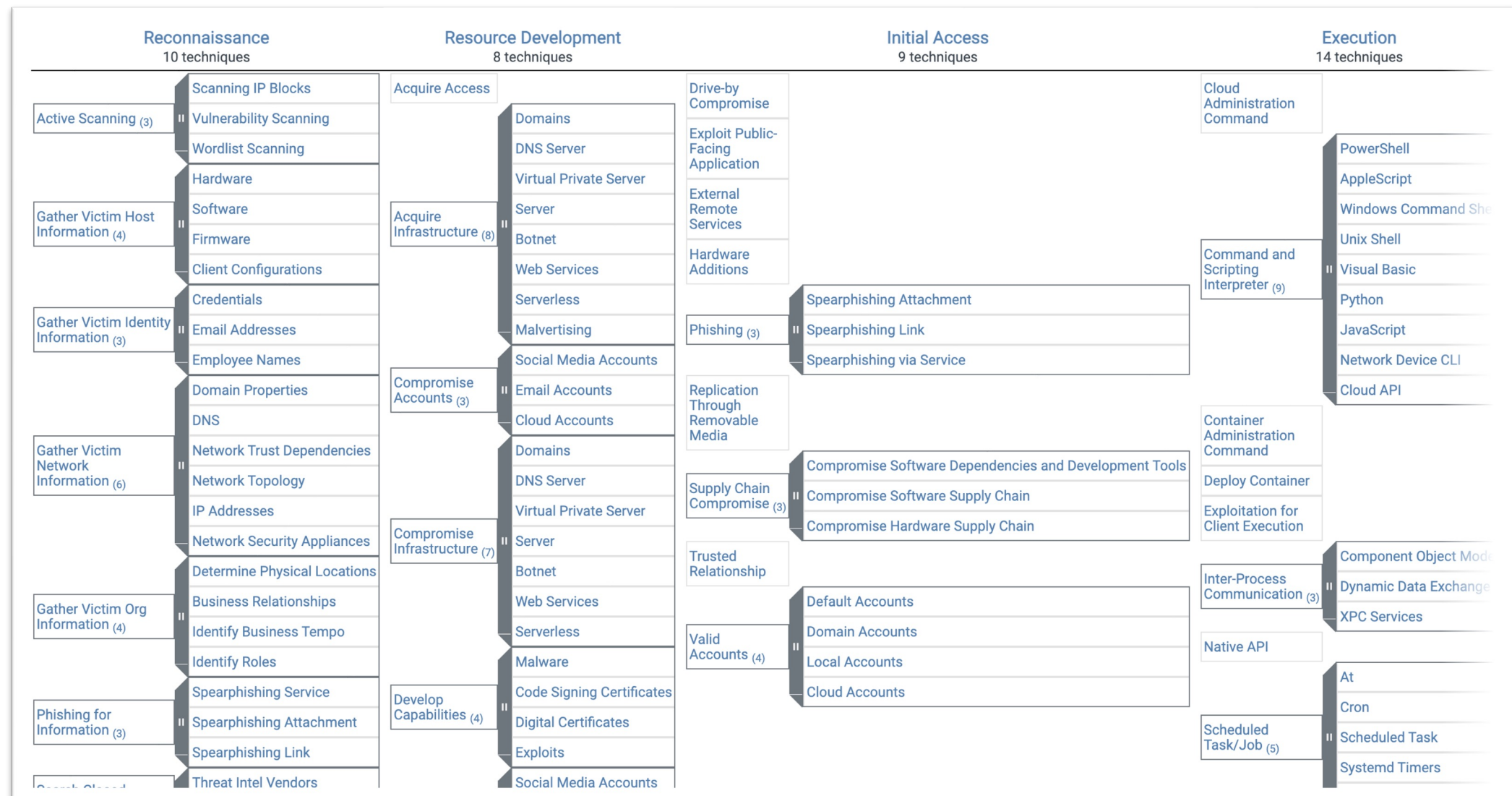
<フィルタリング>

- フォークトリポジトリ
- サイズの大きいリポジトリ
- 非公開あるいは削除済みリポジトリ

RQ1 | 共有による影響（分析方法）

MITRE ATT & CK^[47]

- 攻撃のフェーズとそのフェーズに準ずる技術の分類表
- 機密情報の種類と攻撃の種類を紐づけるために利用



MITRE ATT&CKの一部抜粋

RQ1 | 共有による影響（分析方法）

Gitleaks^[37]

- 正規表現を用いた秘匿情報の検出
- アクセスキーやアカウント情報など

```
description = 'Email Simple'
email = \b[a-zA-Z0-9_+.-]+@[a-zA-Z0-9-]
+\. [a-zA-Z0-9-.] +\b

description = 'Firefox Profile'
path =mozilla/firefox.*(logins\.json|
cookies\.sqlite|places\.sqlite)

description = 'Files with credentials'
file = (?i)(id_rsa|passwd|id_rsa.pub|
pgpass|pem|key|shadow)

description = 'Thunderbird Profile'
path = ($|/)\.?thunderbird/

description = 'Crypto Wallet'
file = wallet\.dat

description = 'Chrome Profile'
path = config.*(google-chrome|chromium) /
```

正規表現の一部抜粋

RQ1 | 共有による影響（結果）

	該当ファイル数	該当リポジトリ数	考えられる攻撃の種類	
Type of Information	#	Repos (%)	Possible Attacks	
API Keys				
GitHub	65,589	6,898 (5.51 %)	Hijacking,	外部からの編集による 管理外コードの実行
Twitter	38,752	3,936 (3.14 %)	Impersonation,	
Other	19,166	4,470 (3.57 %)	Spamming	
RSA Keys				
Private Key	9,452	1,489 (1.19 %)	Hijacking,	利用可能なSSH設定の特定
Public Weak Key	111	n.a.	Spamming	
Public Vulnerable Key	6	n.a.		
PII				
Email Addresses	1,227,175	88,442 (70.7 %)	Spamming, Phishing	
Private Data				
Firefox Logins	40	29 (0.02 %)	Hijacking,	ソーシャルエンジニアリング
Thunderbird Profiles	2	2 (0.002 %)	Impersonation	
Mailboxes	52	52 (0.04 %)		
Software Packages				
Python Dependencies	16,315	1,036 (0.83 %)	Hijacking	サプライチェーン攻撃 依存関係かく乱攻撃
JavaScript Dependencies	145,050	585 (0.47 %)		

RQ2| 共有の動機（分析方法）

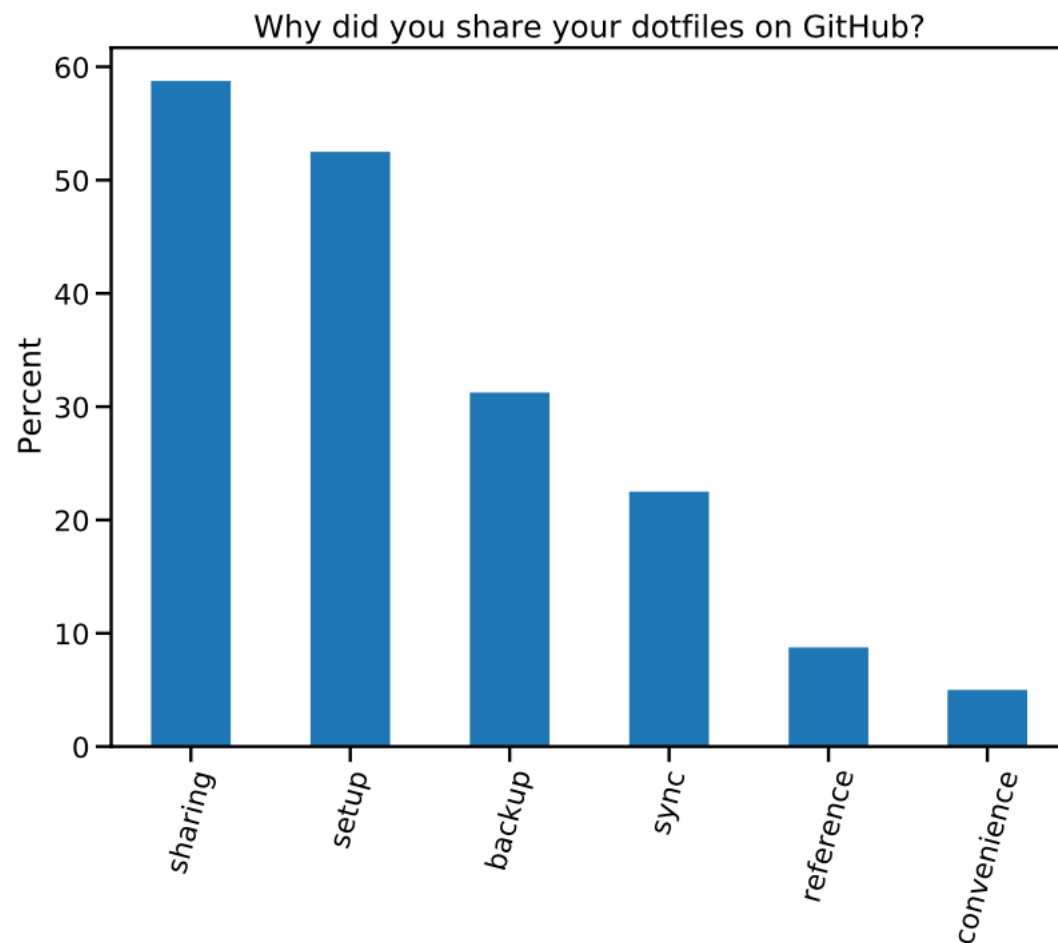
対象リポジトリから特定できた所有者のメールアドレスにアンケートを送信

- アンケート送信数：44,472 ユーザ
- アンケート回答数：1,650 ユーザ（回答率 3.78%）

得られた回答をオープンコーディングを用いて分類

- 無作為に100件選択し、分類のもととなるカテゴリを4人でコーディング
- コーディングされたカテゴリを用いて残りの回答を分類

RQ2| 共有の動機 (結果)



Sharing (59%)

- どのような構成を用いているのか見せるため

Setup (53%)

- システムの構成を容易に再現するため

Backup (31%)

Synchronization (23%)

- 変更の反映

Reference (9%)

- 知人との会話で参照するため

RQ3| ユーザの認識

ユーザにセキュリティリスクを通知し、今後どのような対応を行うのかを集計

対応	
変更なし (58%)	セキュリティに影響を与える機密情報は公開していない
チェック (5.8%)	問題があるか調査し対応を検討
更新 (2.8%)	機密性が高いファイルの削除し安全に運用することを検討
リポジトリの非公開化 (1.2%)	
リポジトリの削除 (1.0%)	git-cryptのような暗号化ツールを利用して安全性の向上に努める
ツールの利用 (0.7%)	

議論 | ドットファイルを公開する理由

オープンソースコミュニティの精神に準ずるタイプ

- 自身の成果を他人に共有することを当然とする
- 他者とのコラボレーションが容易になる

バージョン管理の活用を目的とするタイプ

- 一元的な管理が可能でありバックアップなどが便利である
- 構成の共有が容易で、素早くマシンのセットアップが可能

GitHubに限れば、プライベートリポジトリは無料で利用できるので推奨

まとめ

ドットファイルについてユーザの利用や認識について調査を実施

- (RQ1) ドットファイルの共有によるセキュリティプライバシーへの影響は何か？
- (RQ2) ドットファイルを共有するおもな動機は何か？
- (RQ3) ドットファイル共有による影響をリポジトリ所有者はどの程度認識しているのか？

機密情報の漏洩を防止するための仕組みが必要

- プライベートリポジトリの活用
- ファイルに含まれる機密情報の検出 など

所感

GitHubのようなオンラインリポジトリを活用しながら ドットファイルを管理することについて

- このような事例があることはもともと知っていたが、具体的なセキュリティへの脅威が理解できた (MITRE ATT&CK)
- ただ、良い活用のされ方などが気になった
 - ハードコードを防止するための仕組みなど