Connecting the `.dotfiles`

Checked-In Secret Exposure with Extra (Lateral Movement) Steps

MINING SOFTWARE REPOSITORIES (MSR 2023), MELBOURNE, AUSTRALIA

Gerhard Jungwirth[TU], Aakanksha Saha[TU], Michael Schröder[TU],
Tobias Fiebig[MPI], Martina Lindorfer[TU], **Jürgen Cito**[TU]

What are `.dotfiles`?

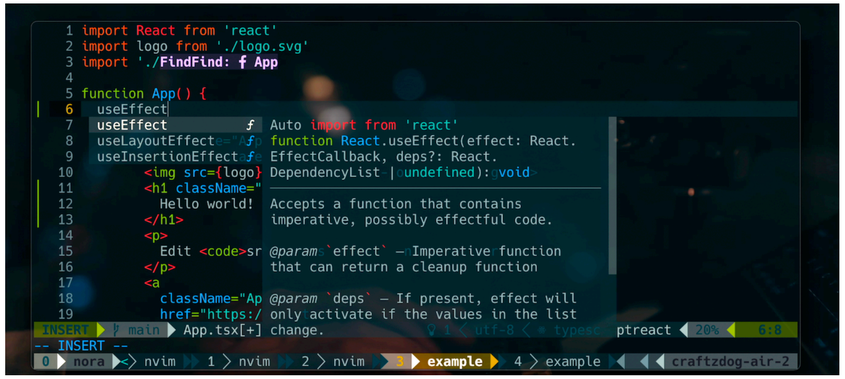
- Text-based configuration files under UNIX systems that typically start with a dot (hidden under normal display)

settings	Updated Sublime Settings
.aliases	Nevermind... back to Sublime
.bash_profile	Updated dotfiles
.bash_prompt	Changed the prompt colors
.bash_server_prompt	Server Prompt Correction
.bashrc	New Preferences
.gitignore	Initial Commit
LICENSE-MIT.txt	Initial Commit
brew.sh	Updated dotfiles
install.sh	Updated dotfiles
sublime.sh	Updated Theme Settings for Sidebar Font

```
$ ls -d .*
.CFUserTextEncoding     .node_repl_history
.DS_Store               .npm
.Trash                  .pylint.d
.anyconnect             .python_history
.bash_profile           .ssh
.cache                  .synamedia
.cisco                  .vim
.conda                  .viminfo
.config                 .vscode
.cups                   .wget-hsts
.docker                 .zsh_history
.gitconfig              .zsh_sessions
.lesshst                .zshrc
.local
```

.config/fontconfig	update
.fonts	update fonts
.github/workflows	cleanup
.gnupg	update
.i3	update i3status
.irssi	cleanup;
.urxvt/ext	fix copy/paste
bin	fix
etc	fix
usr/share/applications	update gpg card settings
.Xdefaults	updates
.Xprofile	add tests
.Xresources	update fonts
.aliases	update
.bash_profile	google cloud sdk
.bash_prompt	update
.bashrc	more completions
.dockerfunc	update
.exports	update exports
.functions	update
.gitconfig	Update .gitconfig (#50)
.gitignore	update .gitignore
.gtkrc	updates
.inputrc	initial commit
.mpd.conf	updates
.path	update
.rainbow_config.json	add cheese
.tmux.conf	Removes status-utf8 (#12)
.xsessionrc	slim is a fucing shit show
LICENSE	thing
Makefile	update aliases
README.md	update
central-park.jpg	add background image;
gitignore	fix
test.sh	make find compatible with alpine (#32)

What are `.dotfiles`?

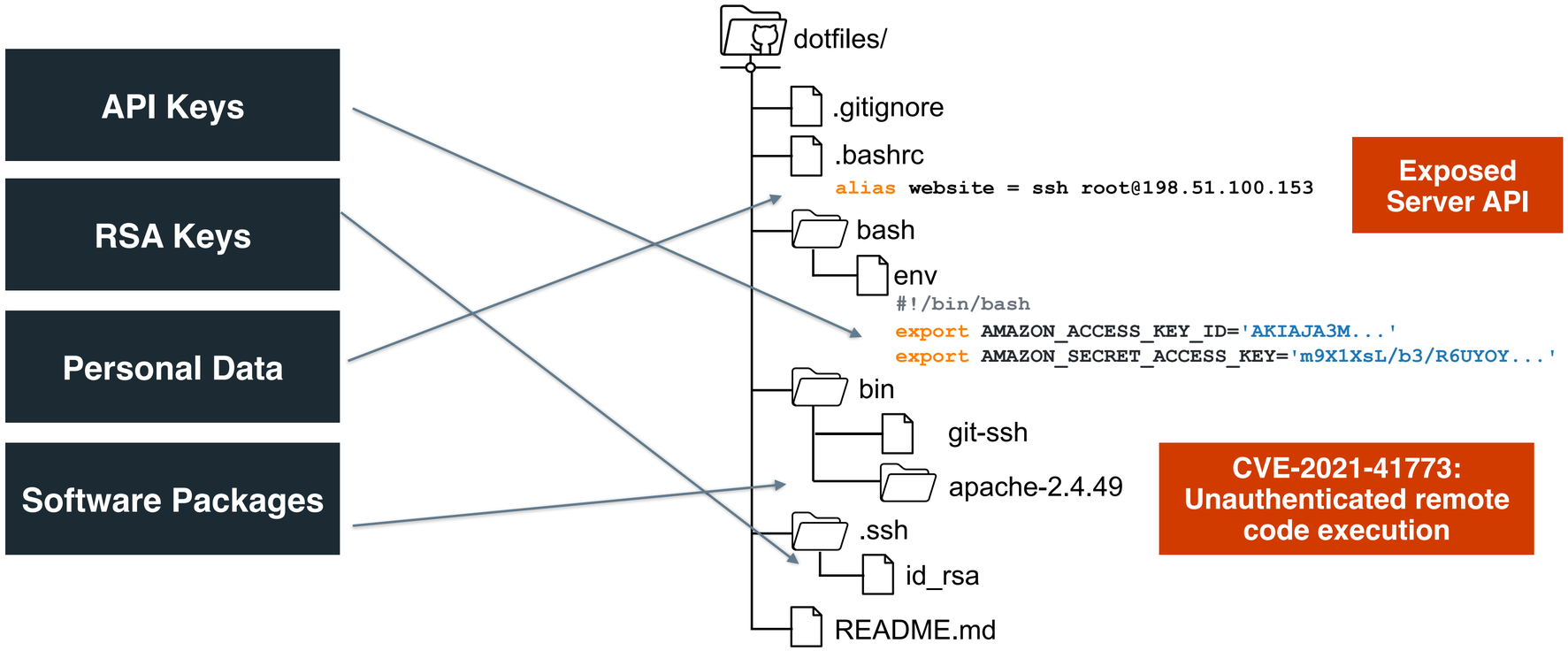


- Customize editors and Shell environments
- SSH and API keys
- Software packages installed on your machine
- Private information such as browsing history and mail inboxes
- Logs and traces from various applications (e.g., VPN logs)

`.dotfiles` are personal configuration files that customize your environment and store potentially private information

Security & Privacy Concerns in `.dotfiles`

Storing personal configurations can have **unintended consequences** that leads to **lateral movements**



Dutch IRS experienced a full compromise by an ethical hacker due to an employee's `.dotfiles` repository

Attack Scenarios in `.dotfiles`

Context found in .dotfiles can lead to multiple attack vectors

- **Credential Stuffing**
- **Vulnerable Packages**
- **Impersonation**
- **Spear Phishing**

MITRE AT&CK classification of our findings

Tactic ("why")	**(Sub)-Techniques ("how")**
TA0009: *Collection*	T1602: Data from Configuration Repository
TA0043: *Reconnaissance*	T1592: Gather Victim Host Information
	T1589: Gather Victim Identity Information
	T1590: Gather Victim Network Information
	T1591: Gather Victim Org Information
	T1593: Search Open Websites/Domains
TA0006: *Credential Access*	T1555: Credentials from Password Stores
	.003: Browser Credentials
	T1552: Unsecured Credentials
	.001: Credentials in Files
	.004: Private Keys

Research Questions

Quantitative / Repository Mining

RQ1: Characterization of Security & Privacy issues of sharing `.dotfiles` on GitHub

- Define search scope and query public GitHub API
- Download all identified repositories (including their history)
- Iteratively sample repositories to refine S&P leak hypotheses
- Extend existing secret identification (GitLeaks)
- Statistical analysis

Qualitative / Developer Survey

RQ2: Motivations for sharing `.dotfiles` publicly

RQ3: Post-disclosure Awareness/Interventions

- Careful development of survey questions for inductive research (expert review, pilot)
- Inviting all `.dotfiles` repository developers to answer survey (with and without disclosure)
- Open coding (two iterations) of responses
- Analysis

RQ1: Security & Privacy Issues of Sharing `.dotfiles` on GitHub

124k `.dotfiles` repositories
>20 million files (61% were text files)
~1 TB of data

Extended Secret Identification (GitLeaks)
to find attack vectors according to MI&TRE

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

Type of Information	#	Repos (%)	Notes	Possible Attacks
API Keys GitHub Twitter Other	**123k API keys in 15k repositories**		20,760 across GitHub [30]	Hijacking, Impersonation, Spamming
RSA Keys Private Key Public Weak Key Public Vulnerable Key	**9.4k private keys in ~1.5k repositories**		158,011 across GitHub [30] Key length $\leq$ 1024 bit Debian RNG attack [55]	Hijacking, Spamming
PII Email Addresses	**1.2 mio email addresses**			Spamming, Phishing
Private Data Firefox Logins Thunderbird Profiles Mailboxes	**~100 mailboxes, email logins, client profiles**		Actual user data, not metadata From Thunderbird and Mutt	Hijacking, Impersonation
Software Packages Python Dependencies JavaScript Dependencies	**1.6k repositories defining 160k dependencies**			Hijacking

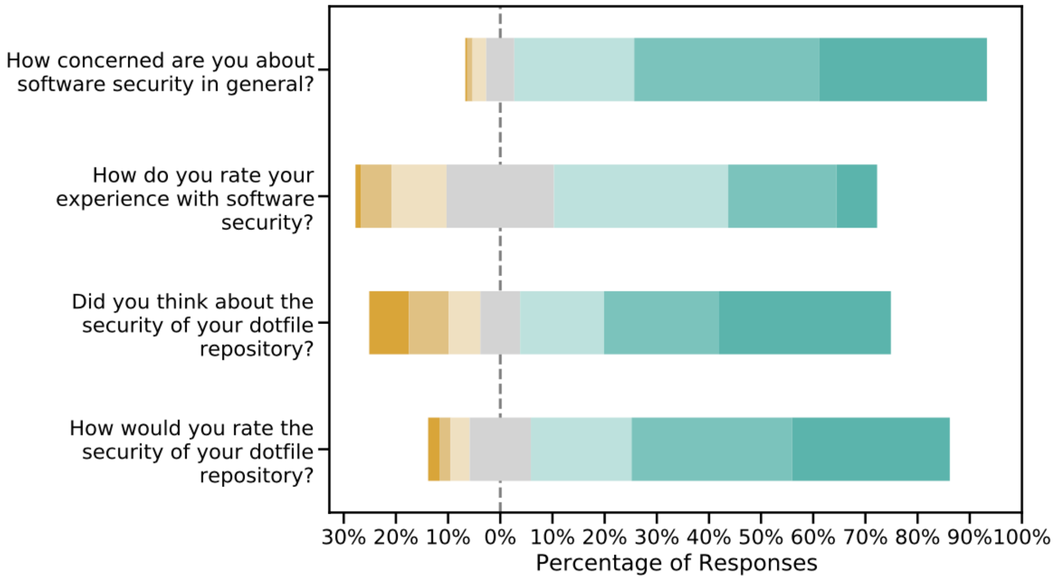
Survey Demographics & Info

1650 survey respondents

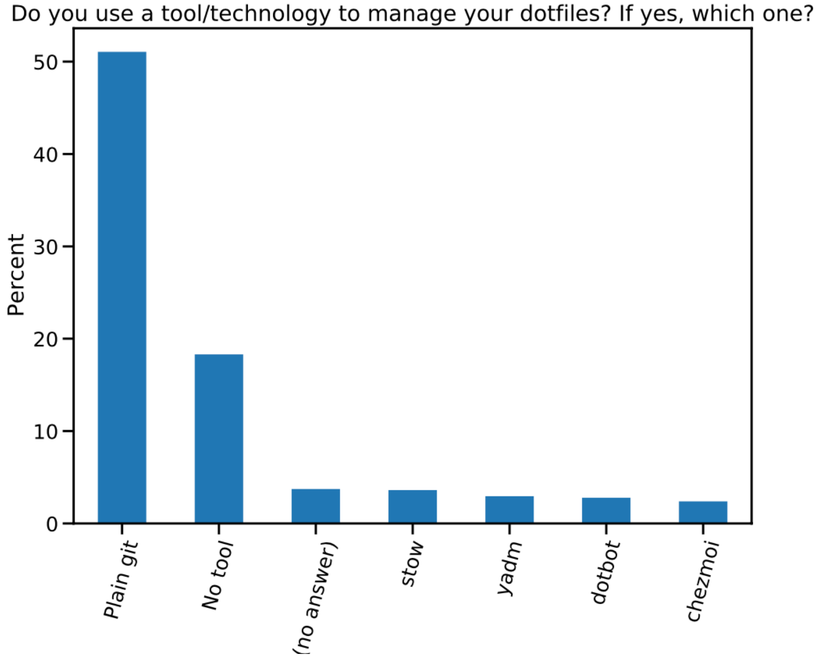
Demographics: 50% are between 20-29 years old, 33 % are between 30-39, 88% male

Most .dotfiles self-written (i.e., not tool generated)

Most respondents are security conscious



… and do not use tools to manage their repo



RQ2: Motivations for Sharing `.dotfiles` on GitHub

Survey Question: Why did you share your `.dotfiles` on GitHub?

Sharing (59%)

Reference (9%)

Community

Machine setup (52%)

Backup (31%)

Synchronization (23%)

Utility

> *The dotfiles I share are simply cosmetic Linux configurations and/or small useful utilities, scripts, and customizations. There is a big community of "ricers" who like to show off these customizations, and so share and remix each other's dotfiles. I share mine because I want them in version control (I've lost them before), and so that folks who find aspects of them useful can use them.* – n0758

RQ3: Post-disclosure awareness/intervention

Survey Question: We found several security & privacy issues across `.dotfiles` repositories on GitHub. What are your planned changes to your repository?

No change in behavior (58%)

> *I am careful to segregate sensitive information from configurations, so am fairly confident that I have not leaked anything.* – n0013

Of the remaining 42%:

Check (14%)

> *I will take a good look on what might be there that you found and remove it from all of that repositories history. Thank you for your project!* – l0041

Update (7%)

> *The first thing I did was to delete my history backup file. Though it was a sqlite db file but anyone who had the deserializer that I was using, can get in plain text which contained a bunch of secret credentials.* – l0114

Delete/Make Private (5%)

Tooling (2%)

Connecting the `.dotfiles`

Checked-In Secret Exposure with Extra (Lateral Movement) Steps

Quantitative / Repository Mining

RQ1: Characterization of Security & Privacy issues of sharing `.dotfiles` on GitHub

Type of Information	#	Repos (%)	Notes	Possible Attacks
API Keys				
GitHub	**123k API keys in 15k repositories**			Hijacking, Impersonation, Spamming
Twitter			20,760 across GitHub [30]	
Other				
RSA Keys				
Private Key	**9.4k private keys in ~1.5k repositories**		158,011 across GitHub [30]	Hijacking, Spamming
Public Weak Key			Key length $\leq$ 1024 bit	
Public Vulnerable Key			Debian RNG attack [55]	
PII				
Email Addresses	**1.2 mio email addresses**			Spamming, Phishing
Private Data				
Firefox Logins	**~100 mailboxes, email logins, client profiles**			Hijacking, Impersonation
Thunderbird Profiles			Actual user data, not metadata	
Mailboxes			From Thunderbird and Mutt	
Software Packages				
Python Dependencies	**1.6k repositories defining 160k dependencies**			Hijacking
JavaScript Dependencies				

Qualitative / Developer Survey

RQ2: Motivations for sharing `.dotfiles` publicly

- **Sharing (59%)**
- **Reference (9%)**
- **Setup (52%)**
- **Backup (31%)**
- **Synchronization (23%)**

RQ3: Post-disclosure Awareness/ Interventions

- **Check Repo (14%)**
- **Update Repo (7%)**
- **Delete/Make Private (5%)**
- **Use Tooling (2%)**

Gerhard Jungwirth[TU], Aakanksha Saha[TU], Michael Schröder[TU], Tobias Fiebig[MPI], Martina Lindorfer[TU], **Jürgen Cito**[TU]

TU WIEN TECHNISCHE UNIVERSITÄT WIEN

max planck institut informatik

https://bit.ly/dotfiles-paper