Hypocrite Commits論文概説

NTT社会情報研究所
渡邉 卓弥

2021/10/27
CSS2021 研究倫理相談TF/MWS/OWS/UWS連携企画

On the Feasibility of Stealthily Introducing Vulnerabilities in Open-Source Software via Hypocrite Commits

NTT

- 攻撃者がOSSに対して脆弱性入りパッチのコミットを試みる“Hypocrite Commits”の提唱
  - 脅威モデル、成立条件、秘匿性を上げるテクニック、 **Proof-of-Concept**、実態調査
  - 特にLinuxカーネルを対象として調査
- 著者: Qiushi Wu、Kangjie Lu
  - University of Minnesota (以下、UMN)
  - カーネルセキュリティ、アプリケーションセキュリティ分野で活躍する研究室
- IEEE S&P 2021に採択されるも、倫理的問題から大議論を巻き起こし、取り下げ
  - 論文: https://github.com/QiushiWu/QiushiWu.github.io/blob/main/papers/OpenSourceInsecurity.pdf

論文取り下げまでの経緯（後で詳解）

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

一度目の騒動:
IRBとの相談、声明発表、倫理的配慮のセクション追記を実施

二度目の騒動:
新規プロジェクトがさらなる問題を招き論文取り下げに追い込まれる

大学側

開発者側

学会

脅威モデル

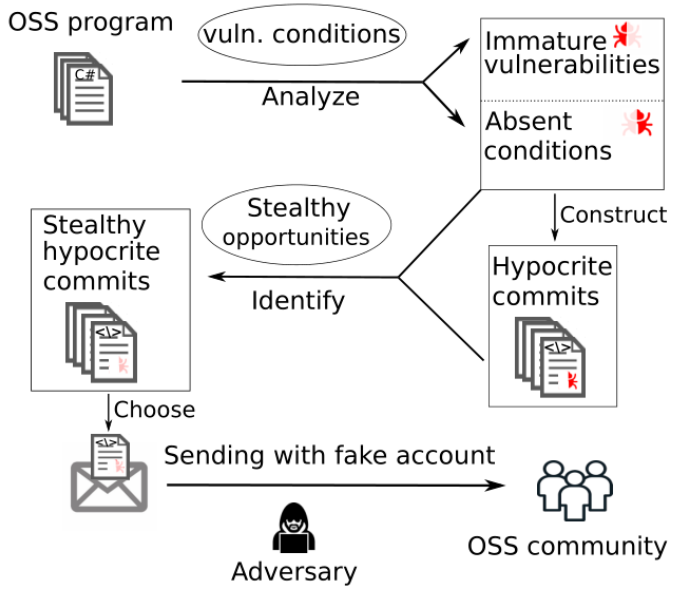
- OSS: 初投稿のパッチ送信が許可されている想定
- レビュープロセス: 限られた人員による自動/手動のレビュー
- 攻撃者: マイナーパッチのみ投稿する第三者
  - エラー処理、些細なバグ修正など
  - 大掛かりな変更には入念なレビューが行われる/そもそも受け入れない
- Hypocrite Commitの定義
  - コードが改善されるように見える30行未満のパッチでありながら、重大なセキュリティ問題（UAFなど）を引き起こすようなパッチ

脆弱性生成方法

- コードに含まれる脆弱性の因子(Immature vulnerabilities)にマイナーパッチを当てることで悪用可能な脆弱性を生成する

```
1  /*Introducing: CVE-2019-12819*/
2  int __mdiobus_register(...) {
3      ...
4      err = device_register(&bus->dev);
5      if (err) {
6          pr_err("mii_bus %s failed to register\n",
7                                  bus->id);
8  +       put_device(&bus->dev);
9          return -EINVAL;
10     }
11 }
```

refcountのバグを修正を試みるも、UAFをもたらしてしまったパッチの実例。5年間残置



本論文における脆弱性生成方法

OSSパッチプロセスにおける問題点

- LinuxカーネルのCVEに対応するすべてのパッチを分析
  - 9.8%がマイナーパッチに起因する脆弱性
  - 138個のCVEに関連するパッチ・修正パッチを収集

1. メンテナンスの哲学
   - 予防パッチの拒否
   - PoC必須

2. コードの複雑性とカスタマイズ
   - 8%がポインタエイリアス・関数の間接参照・コールバック関数など「複雑なコード」に起因
   - カスタマイズされた関数による暗黙的なメモリ解放等

3. OSSのオープン性
   - パッチを受け入れるプロジェクト(大規模)
   - レポートのみ受け入れるプロジェクト(小規模)

Hypocrite Commits –脆弱性の実態と成立条件

単体では「脆弱性の因子」に過ぎないためレビューをすり抜けるが、マイナーパッチと組み合わせることで条件を満たし、悪用可能な脆弱性となりうる

特定の状態をもつ（変数/コード）

特定の状態をもたない

オブジェクトの使用

特定の実行順序

Vuln. conditions	(%)	Common vulnerability types (state)
With a state	36.4%	NULL dereference (nullified) Use-after-free (freed)
Without a state	36.4%	Uninitialized use (initialized) NULL dereference (initialized) Out-of-bound access (bounded) Access-control error (privileged) Integer overflow (bounded)
A use	21.6%	Use-after-free Uninitialized use Access-control error NULL dereference Out-of-bound access
A temporal order	5.7%	Use-after-free NULL dereference

マイナーパッチに起因する脆弱性の成立条件と割合

- マイナーパッチによって強制的に条件を成立させる
  - 「With a state」・・・メモリを解放する関数を挿入する、解放されたメモリを参照する等
    deallocのようなキーワードを含まない(バレにくい)関数は多数
  - 「Without a state」・・・初期化されていない変数を生成する等
  - 「A use」・・・関数のパラメータとしてアクセスする等。if文やエラー分岐等でステルス化できる
  - 「A temporal order」・・・同期を削除し、順序の整合性を崩す等。

ステルス性の向上

- “Hypocrite Commits”をレビュープロセスにおいて検出されにくくするアイデア
  - 並行性
    - 非決定的であり、実行順序を実行前に推定することが困難
  - エラー処理
    - トレースが難しく、テストがないことも多い
  - 暗黙的操作
    - 関数名に表されていないメモリ解放など
  - ポインターエイリアス
    - 静的解析ツールや手動分析を妨げる要因
  - 間接参照
    - トレースが難しく、解析ツールがサポートしていないことが多い
  - その他
    - モジュールのインポートによる複雑化、コーディング規則の不統一など

```
1  static int iowarrior_release(...) {
2      mutex_lock(&dev->mutex);
3      if (!dev->present) {
4          mutex_unlock(&dev->mutex);
5          iowarrior_delete(dev);
6      }
7  }
8  static void iowarrior_disconnect(...) {
9  +   dev->present = 0;
10     mutex_lock(&dev->mutex);
11 -   dev->present = 0;
12     if (dev->opened)
13         ...
14     mutex_unlock(&dev->mutex);
15 }
```

マイナーパッチによってmutexロックで保護されていない箇所に代入コードが移動してしまい、UAFにつながった実例

Proof-of-Concept

- ソースコードから"Hypocrite Commits"を実行できる箇所を特定するLLVMベースのツールを開発
  - メモリリークの脆弱性因子を検出する、エラーパスに含まれるかどうかを判別する等

- 実際にUAFを発生させるマイナーパッチを送信

偽名のメールアカウントを使用

Case1. エラーメッセージ出力の改善
  — 並行性+エラーパス

Case2. メモリリークバグの修正
  — エラーパス+ポインタのエイリアス

Case3. refcountのバグの修正
  — 並行性+暗黙的操作

```
1       err = dev_request(devA);
2       if (err) {
3           disable_device(devA);
4   +       dev_err(&devA->dev, "Fail to request devA!\n");
5           return err;
6       }
```

Case 1のHypocrite Commit

倫理的配慮(一度目の騒動の後に追記)

- UAFを発生させるパッチだけでなく、それを修正するためのパッチを用意している
- メンテナからパッチを導入しようとする旨の返信がきたら、すぐさま撤回し修正パッチを送る

→3つのケースすべてで、脆弱なパッチがGitコミットとなっていないことをメンテナに確認

- パッチ適用プロセスの問題調査であり、個人情報を収集しない
- メンテナを特定できないよう匿名化している

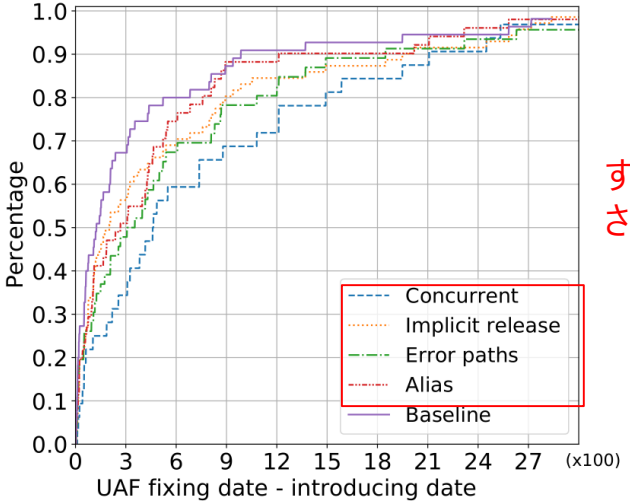
→human subjectではないと判断し、IRB事後審査を正式に免除

- Linux Communityに通達し、フィードバックを得た(事後)
- メンテナへの労力は最小限にした

定量的評価

- 2018/8 - 2020/8の期間におけるGit履歴を調査し、Hypocrite Commitsで悪用されうる脆弱性因子を調査
  - refcountリークバグ修正 353個
  - メモリリークバグ修正　1228個
  - 並列実行の関数で参照される解放後ポインタの参照 1085個

- 2015/1-2020/8のUAF脆弱性修正について、ステルス性なし/ありのそれぞれで、修正されるまでの日数を比較



すべての手法が修正されにくさに貢献

対策

- コミッタの信頼性向上
  - 身元確認プロセス、説明責任
- ツールによるパッチ分析
  - シンボリック実行などによる高度な静的解析
  - ファジングなどによる高カバレッジな動的解析
- メンテナ側の体制
  - 予防的パッチの受け入れ
  - リスク意識の向上
  - パブリックなパッチ監視

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

大学側

開発者側

学会

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

- 意図的に導入された脆弱性が検出されるかを調査する目的
- 身元を偽って投稿された

大学側

開発者側

学会

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

- プライバシー分野の研究者による意見書[1]
- Twitter上で議論がなされた
- 「人間を対象とした実験であるにも関わらずレビューされていない」

意見書[1]: https://hackmd.io/s/BJGs6Tfiw

大学側

開発者側

学会

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

FAQ形式で声明文[2]を公開

- 実験の目的
- 実験の手順
- 実際に脆弱性を混入させる意図はない
- メンテナを対象としたhuman researchではない
- 実験は事前に告知していないが、問題点は指摘した[3]
- メンテナの時間は浪費させるが、最小限
- 産学の関係性を悪化させるとは考えていない

声明文[2]: https://www-users.cs.umn.edu/~kjlu/papers/clarifications-hc.pdf

問題提起[3]: https://lkml.org/lkml/2020/8/27/1197

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

- Hypocrite Commitsとは別の新たなプロジェクト
- 7ヶ月を経てのコミット再開であったため、攻撃が継続されているとの疑念を巻き起こす

問題が再燃

大学側

開発者側

学会

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

問題が公となり、事態が急速に展開

- Pakki新たな研究であると主張（開き直りに近い態度）
- GregはUMNの全パッチをrejectし、過去パッチも削除すべきとの見解[4]を示す

Gregの返信[4]:
https://lkml.org/lkml/2021/4/21/143

大学側

開発者側

学会

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

要求内容[5]
- 既知の脆弱なコードを含むコミットを全特定すること
- ユーザの事前同意を得ていない論文を撤回すること
- human researchを行う際にレビューと事前承認を受けるようにすること

LFによる要求書[5]:
https://drive.google.com/file/d/1bUsiJQesl4pCioE6h4ZUOghg0qHpemcb/

大学側

開発者側

学会

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

UMNの公開レター[6]
- 主な内容は謝罪・反省
- “Hypocrite Commits”と4月以降の実験における190のパッチが別プロジェクトであることを明示

An open letter to the Linux community[6]:
https://lore.kernel.org/r/CAK8KejpUVLxmqp026JY7x5GzHU2YJLPU8SzTZUNXU2OXC70ZQQ@mail.gmail.com

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

2021.6.3にすべてのバージョンにおけるリバート・修復が適用される

大学側

開発者側

学会

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

TABレポート[7]
- 85人の開発者と95人のコミュニティメンバーにより、435のコミットが再検討された
- 349は正しいパッチであった
- 脆弱なパッチはすべてrejectされた
- poorなパッチには修正・リバートが施された

TABレポート[7]:
https://lkml.org/lkml/2021/5/5/1244

論文取り下げまでの経緯

2020.8.9-21	著者らが"Hypocrite Commits"に関する5件のパッチを送信
2020.11.?	IEEE S&Pに採択され、論文ドラフトが公開
2020.11.22	Sarah Jamie Lewisが倫理的懸念に関する注意喚起
2020.12.1	LewisらがIEEEに意見書を提出
2020.12.?	human researchではないとの判断から、UMN IRBは事後審査免除
2020.12.15	著者らによる声明が発表
2021.4.6	UMNの研究者Pakkiによって新たに低品質のパッチが大量送信される
2021.4.20	Greg Kroah-Hartmanがパッチのコミット中断を要求
2021.4.21	Gregのリクエストに基づき、Linux TABがUMNパッチのレビューを開始
2021.4.23	Linux FoundationがUMNに対し改善要求を提出
2021.4.24	UMNが「An open letter to the Linux community」を公開
2021.4.26	著者らがS&P論文を取り下げ
2021.4.27	著者らがコミットおよびLinux Foundationへの返信を公開
2021.5.3	Gregが最後のリバートを投稿
2021.5.5	Linux TABが監査結果のレポートを公開
2021.5.6	UMNとGreg、Linux Foundationが事態改善に向けて直接議論
2021.5.6	IEEEが倫理違反および再発防止に関する声明を発表
2021.5.7	UMNがTABのレポート内容を認める

- Linuxカーネル以外のプロジェクトには影響を与えていないことを表明

私見

- 否定的側面
  - 実社会に与える影響は明白
  - 経験則的に守っていた研究倫理のラインが崩れたかもしれない
- 肯定的側面
  - 攻撃のコンセプトを描き、成立条件に分解し、具体化、定量評価するまでの華麗な流れ
    - 「空想止まり」のオフェンシブ研究を昇華させるヒント
    - もちろん倫理的配慮は必須
- いずれ必ずぶつかる壁だったのでは
  - サイバーセキュリティ研究における「実証主義」
  - 怒られてないだけのような研究もあるのでは