大久保研ゼミ 2026-06-30 18:22(GMT+9:00)

主要な成果

ファンクション・セレクター衝突（4バイトのハッシュ衝突）を悪用したバックドア攻撃がイーサリアムのプロキシパターン上で実証された。 [1] 攻撃コストは低く、一般的なGPU搭載機器で最短4.2秒での生成が確認された。 [2] 既存の監査ツールはこの攻撃を検出できないことが判明しており、防御手法の開発が次のフェーズとして位置づけられている。 [3]

決定事項

- **研究スコープ**：イーサリアム・Polygon・BSC等のEVM互換チェーンを対象とし、デリゲートコールを使用するプロキシアーキテクチャに限定 [4] [5]
- **検証対象**：ERC-20の主要関数（`approve` 等）に対するセレクター衝突バックドアの生成可能性を実証 [6]
- **次フェーズ目標**：Slitherへのプラグイン追加によるバックドア検出ツールの開発・GitHub公開 [7]
- **投稿先**：Asia CCS（締め切り12月21日）、採択時はIEEE S&P AC3への提出を検討 [8]

技術的知見

- **攻撃メカニズム**：プロキシ側のセレクターと同一値を持つ悪性関数をimplementation側に埋め込むことで、デリゲートコールを経由せずプロキシ側で悪性コードが実行される [9]
- **攻撃コスト**：GPU並列探索により4.2秒での衝突生成が可能。スクリプトキディレベルでも実行可能 [2] [10]
- **影響範囲**：DeFiマーケット規模は約1,000億ドル。攻撃者母数増加を考慮したエスティメーションが必要 [11] [12]
- **既存ツールの限界**：Hardhat等のテストフレームワーク、Slither等の静的解析ツールでは現状この衝突を検出できない [13]

想定攻撃シナリオ

- **シナリオ1**：開発者・監査機関を欺いたコードレビュー通過による直接埋め込み [14]
- **シナリオ2**：秘密鍵漏洩後のアップグレード機能悪用 [14]
- **シナリオ3**：OSSコミュニティへの長期貢献で信頼を獲得後、悪性コードをマージ（XZ Utils事件と同構造） [15]

フィードバック・指摘事項

- **インパクト定量化**：市場規模の提示だけでなく、攻撃による実質被害額のエスティメーション（攻撃者母数 × 被害額）を追加すべき [16] [17]
- **残存リスクの明確化**：UPSへの移行で脆弱性は改善されるが、スイッチングコストが高くTrustable Proxyを使い続けるユーザーの割合推定が必要 [18] [19]
- **関数名の工夫**：ブルートフォース生成した関数名よりも、元の関数名を活かした辞書ベースのアプローチがコードレビュー通過に有効との提案 [20]
- **4バイト選択の背景**：セキュリティ意識の低い初期設計に起因し、業界全体での変更は事実上困難との認識を共有 [21] [22]

未確認・保留事項

- Slitherプラグインの実装詳細および公開時期
- 残存リスクとしてTrustable Proxy継続利用ユーザーのシェア推定値
- AIを活用したセマンティック解析（UBD検知）の具体的実装方針 [23]

アクションアイテム

- **Speaker 2**：被害額エスティメーション（攻撃者母数 × 影響額）をスライドに追加
- **Speaker 2**：Trustable Proxy継続利用ユーザーの残存シェア推定を関連研究から調査
- **Speaker 2**：Asia CCS投稿に向けて論文を12月21日締め切りまでに提出 [8]
- **Speaker 2**：コアコンセプト2（Slitherプラグイン）の実装をGitHubで公開予定 [24]