Processing言語による侵入防御効果の可視化手法

A Visualization Method for Understanding the Effect of Intrusion Prevention using the Processing 3

小倉有花・法制倫理分科会・情報セキュリティ大学院大学

This research proposes a method for understanding the effect of TOMOYO Linux to intrusion prevention with the aid of the visualization image written in the programming language called the Processing 3. In the proposed method, we use a PoC program for a vulnerability allowing potential local attackers to execute kernel memory corruption and privilege escalation simultaneously, so as to define a progress status of the experimental attack in %, along with a virtual threat model based on the cyber kill chain. In the experiment, we selected frequently used commands from 4 different directories such as /sbin or /usr/bin, to investigate the number of executable commands between when TOMOYO Linux is in disabled mode and enforcing mode at each status of the experimental attack. The experiment result shows that 126 commands were successfully protected from attackers by TOMOYO Linux when the status of the attack progressed to the next level and we manually visualized the results in Processing 3. Improving the evaluation of the visualized image is the future work.

1. 背景・課題

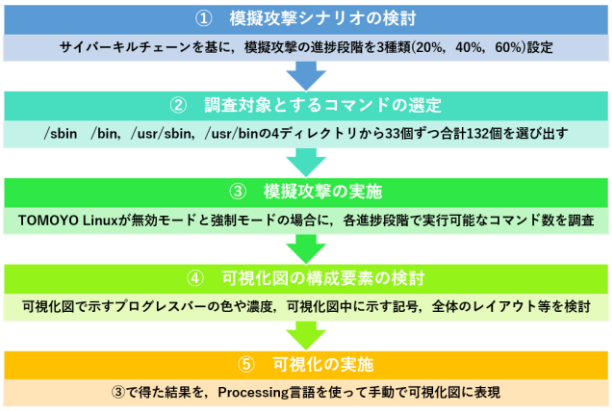
近年，攻撃手法の巧妙化に伴って，セキュアOSを用いた防御策が重要となっている．セキュアOSとは強制アクセス制御機能と最小特権の原則を実装したもので，Linuxへの代表的な実装としては，SELinux や TOMOYO Linuxなどがある．セキュアOSはその有用性がある程度認知されているにもかかわらず普及が進んでおらず，その原因としてポリシーの管理が必要なことによる使い難さや利用に伴うシステム停止のリスク，現時点での使用事例が少なく効果も不明確なことなどが考えられる．使いにくさの改善に向けてアプローチを行った先行研究が既に存在している一方で，セキュアOSの効果やメリットに焦点を当てて明確にすることに焦点を当てた研究は，現状例が少なく不十分である．

2. 目的

本研究の目的は，セキュアOSの中でも特にTOMOYO Linuxに焦点を当て，その効果の可視化することである．本研究では，可視化対象とする**「効果」**を，**「TOMOYO Linuxの強制アクセス制御機能の無効時と有効時に，システムに侵入した攻撃者が管理者として実行可能であるコマンド数を比較した時の差分」と定義**し，この差分の値が大きいほど攻撃者によるTOMOYO Linuxが持つ侵入防御効果が大きいと考える．

3. 提案手法と模擬攻撃

提案手法



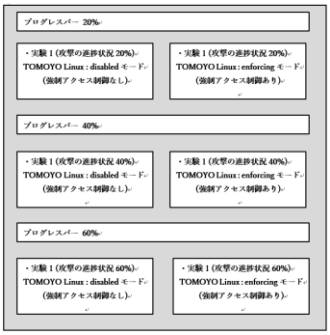
攻撃進捗(%)	TOMOYO Linux の強制アクセス制御なし		TOMOYO Linux の強制アクセス制御機能あり	
	実行可能コマンド数	実行不可コマンド数	実行可能コマンド数	実行不可コマンド数
20%(実験1)	132 個	0 個	132 個	0 個
40%(実験2)	126 個	6 個	3 個	129 個
60%(実験3)	126 個	6 個	3 個	129 個

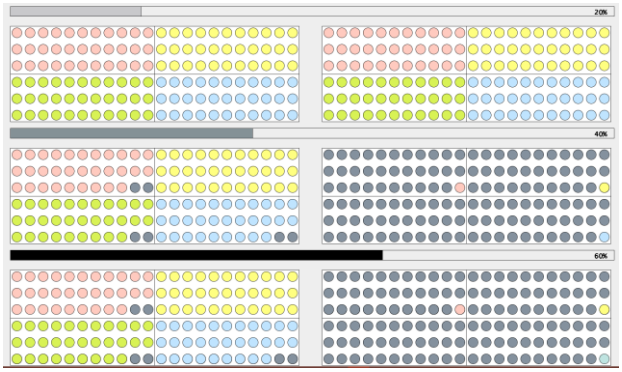
提案手法に従って，模擬攻撃を行い，異なる3つの攻撃進捗段階でTOMOYO Linuxが無効モードと強制モードの時に実行可能なコマンド数と不可能なコマンド数を調査したところ，左図のような結果が得られた．

4. 可視化実験と結果

模擬攻撃を経て得られた結果を手動でProcessing言語を用いて，右図のレイアウトに従って可視化した．

図中の○はそのままコマンド1つ分を表し，色付きのコマンドが実行可能コマンド，灰色が不可のものを示す．ピンク，クリーム，緑、水色の4色はコマンドが属するディレクトリの違いを示す．





5. 今後の課題

- 可視化図のレイアウの改善 ・・・ 可視化図の構成がシンプルであるために盛り込めていない情報もあることから，レイアウトを再検討する．
- 利用する脆弱性の再考 ・・・ バックドアなど，被害を受けた時の深刻度がより大きな脆弱性を使って模擬攻撃をやり直す．
- 評価方法の抜本的見直し ・・・ 現在は定性的な自己評価のみに頼っている評価手法を，定量的，客観的な評価が得られるよう改善する．