A method of Protecting privacy by container

システム情報工学研究科 博士前期課程 1 年
201720763 張　世申
指導教員　新城 靖

2017 年 11 月 22 日

1　Introduction

パソコンがネットワークと通信するときにプライバシを漏れる可能性がある。プライバシの漏洩は、ネットワーク通信先との通信中に起こる、また自分のパソコンにある個人情報は不正なアクセスによって盗まれることもある。本研究では、コンテナという OS 層の仮想マシンを利用し、ホストから分離した OS 環境を作り、プライバシ内容を実行中に検出し、その内容を保存する環境を提案する。

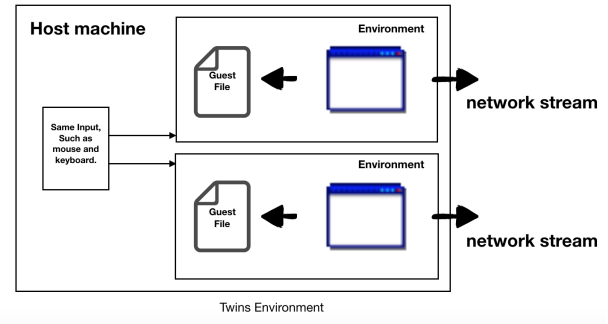

図 1: 双子の環境

2　プライバシ検出

本研究では、２つの方面でプライバシの保護を行う。ひとつはホストマシン内に保存する個人情報、もうひとつは、ネットワーク接続中のリアルタイムなプライバシ保護。プライバシ保護のため、まずプライバシの検出が必要だ。ブラウザを例として、プライバシは訪問歴史や、フォーム¿、Cookie、Session などの内容が考えられる。ユーザトラッキングでよく利用した Cookie ファイルにはサーバが配る唯一な Cookie ID や Session ID の情報がある。これらのユニークデータによく個人情報がある。ファイルにあるユニーク情報を得るため、２つの実行アプリのファイルを比較し、差分の内容にプライバシが含める可能性が高い。

2.1　双子の環境

差分の取るに実行必要な環境として、双子の環境という方法を提案する。双子の環境とは、一つのホストマシンで２つの同様な仮想環境を動け、同じ入力を与えられ環境だ。仮想環境において生成する２つ分のファイルに差分を取って、プライバシであるかどうかを判断する。

仮想環境の選ぶ

一般的な仮想マシンは良い選択が、１個以上の仮想マシンを動くならホストのパフォーマンスが低下する。そしてホストはゲスト OS のファイルシステムも直接的にアクセスできない。本研究では、コンテナという OS の層の仮想マシンを使う。OS サービスの仮想化でホストのパフォーマンスを効率的に使える。本研究は Docker[1] コンテナを使う。一方で Overlay File System でホストとファイル共用ができ、差分を取るためのファイルアクセスもよくできると考えている。

差分を取る

まず、ゲスト生成したファイルは diff アルゴリズムで差分を取る。diff[2] アルゴリズムは平均 O(ND) の時間で完成でき、ファイルの違う内容が少ない場合でスピードが速い。また、HTTPS の情報が暗号化されたため、ウェブ通信内容の差分は Man-In-The-Middle Proxy[3] を使って HTTP と HTTPS の情報をキャプチャ。メールサーバ、文字エディタようなのプログラムはユーザ入力が多い。この場合では入力端の入力も考える必要がある。ホストでのキーボードやマウスなどの入力を２つのコンテナに送信するために Selenium[4] という自動テストツールを用いる。

3　環境シンクロナイズ

環境によるゲスト内容の影響を考えなければならない。２つのコンテナの実行環境が違うならプライバシ判断の結果に影響する。双子の環境をできるだけ同じにする必要がある。

3.1　ランダム性排除

アプリケーションはよく OS のエントロピーデバイスを読み込む。Linux では乱数生成器や UUID などのランダムナンバーデバイス。またマルチスレッドプログラムのスゲジュールもランダム性を引き起こす。コンテナエンジン、またゲスト OS の一部を変えるで実現できる。

3.2　カーネル隔離

コンテナを隔離環境として、ホスト OS のリソース、例えばメモリ、CPU、ファイル、IO、ネットワークの隔離がよくできる一方、ホスト OS のカーネル情報は共有である。というとゲストはホストの CPUINFO やメモリ使用率、IO デバイスなどの情報が読める。ゲスト OS 環境に動くプログラムは自分が独立的な環境で実行しているように認識するのが要求するから。カーネル情報を一部隠す、また改ざんしたほうが良いと思う。

4　関連研究

Qubes-OS[5] はセキュリティに注目する OS の一種である。Qubes-OS は Hypervisor を使い、アプリケーションを違う安全性ドメインで実行し、リソースを隔離する。Qubes-OS は Xen を使うから、ホスト OS がなく、より良い隔離性を提供できる。Blink-Docker[6] はブラウザを Canvas Fingerprint を利用したユーザトラッキングから守る実行環境だ。Canvas Fingerprint はハードウェアや OS のわずかな違うによってクライアントの唯一なタッグを生成できる。コンテナ技術を利用、毎回の Fingerprint 情報を変えることができる。

5　まとめ

本研究では人間の双子の研究に参考した双子の環境を提案した。Docker コンテナに基づく、軽量で分離的な仮想環境を作り、プライバシを検出する。検出の誤差を減るために、Docker エンジンやコンテナ OS カーネルの直すも考える必要がある。

参考文献

[1] Docker - Build, Ship, and Run Any App, Anywhere: https://www.docker.com/, Accessed: 2017-11-22.

[2] EUGENE W.MYERS, ”An O(ND) Difference Algorithm and Its Variations”,

Algorithmica

November 1986, Volume 1, Issue 14, pp 251266

[3] mitmproxy - an interactive man-in-the-middle proxy for HTTP and HTTPS :

https://mitmproxy.org/,

Accessed:2017-11-12.

[4] Selenium - Web Browser Automation:

http://www.seleniumhq.org/,

Accessed: 2017-11-22.

[5] Qubes OS - A reasonably secure operating system:

https://www.qubes-os.org/

Accessed: 2017-11-22.

[6] P Laperdrix, W Rudametkin, B Baudry :Poster: Blink: A moving-target approach to fingerprint diversification

37th IEEE Symposium on Security and Privacy