

6.9 ネットワークトラフィック処理の基盤技術と実装

[開講科目名]

(授業科目)高度サイバーセキュリティ PBL II / (enPiT-Pro) ネットワークトラフィック処理の基盤技術と実装

[開講科目名(英)]

Fundamental Technique and Implementation of Network Traffic Processing

[単位数] 1 単位

[開講日]

(調整中)

[担当教員]

高野 祐輝(大阪大学), 宮地 充子(大阪大学)

[授業の目的・概要]

ネットワークトラフィック処理技術は、スイッチングやルーティングといったネットワークの基本機能を実現する技術であるだけでなく、ファイアウォールや侵入検知システム (IDS) といった、ネットワークセキュリティ機器・ソフトウェアを実現するための基礎技術でもある。

特にネットワークトラフィックに対するパターンマッチは、ファイアウォールや IDS を実現するために必須の技術である。このパターンマッチは、バイトコードインタプリタである疑似レジスタマシンを用いて行われることが多い。

例えば、BSD や Linux などのオペレーティングシステムでは、BSD Packet Filter (BPF) と呼ばれる疑似レジスタマシンが用いられ、また、正規表現を実装する方法の一つとして、非決定性有限オートマトンを模倣する疑似レジスタマシンが用いられる事もある。

そこで、本 PBL では、ネットワークトラフィックに対してパターンマッチを行うための疑似レジスタマシンの設計と実装を行い、ネットワークトラフィック処理技術について理解を深める。

また、より高度な課題として、本演習で実装した疑似レジスタマシンを、netmap 等に代表されるカーネルバイパス技術の上に適用し、実践的なネットワークトラフィック処理機構の実装を行う。

カーネルバイパス技術を用いると、専用ハードウェア無しに、一般的なコンピュータを用いてソフトウェア処理のみで、高速にネットワークトラフィック処理を行えるようになる。

[学習目標]

(1) レジスタマシン理解

レジスタマシンについて理解しコンピュータの基礎的な構造について学ぶ

(2) バイトコードインタプリタの設計と実装

BPF や正規表現のバイトコードインタプリタを設計・実装することで、パターンマッチングの基盤技術を習得する

(3) コード生成学習

Low Level Virtual Machine (LLVM) を利用したマシン語の生成を行うことで、高速な言語処理系について学習する

[成績評価]

レポートによる評価を行い、評価基準は以下の通りとする。

最優: 下記に加え、BPF および正規表現を実行する、Just-in-time コンパイル可能な疑似レジスタマシンを実装することができる

優: BPF を実行する疑似レジスタマシンのインストラクションセットを完全に実装することができる

良: BPF を実行する疑似レジスタマシンの一部機能を実装することができる

可: BPF と疑似レジスタマシンについて理解し論じることができる