マルチテナント環境におけるセキュリティと機能の最適配置を考慮した NFC 機構

攝待 大輔, 近藤 賢郎, 寺岡 文男　{ed, latte, tera}@inl.ics.keio.ac.jp

目的｜安全で高性能な NFC 基盤構築

ネットワーク機能のソフトウェア化 (NFV)

サーバ仮想化技術を用いて実現

マシンの高性能化に伴い NF 集約率が向上

NFV基盤のマルチテナント利用

単一マシンで複数テナントのフローを処理

○資源利用率向上, 運用コストの低下

×悪意ある機能/バグを含むNFの混在により他テナントデータの盗聴/改竄, 資源占有

NFV フレームワークの比較.

	1	2	3	4	5
VM-based	×	○	○	○	High
NetVM	△	○	×	○	High
Container-based	×	○	○	○	Low
OpenNetVM	△	×	×	○	Low
Flurries	○	○	×	○	Low
Function-based	○	×	×	×	Very Low
NetBricks	○	○	○	×	Very Low
FastPaaS	○	○	○	×	Very Low

1. Packet Zerocopy
2. Memory Isolation
3. Packet Isolation
4. Resource Isolation
5. Resource Overhead

提案｜アーキテクチャ

機能の最適配置による安全な集約率, 性能の向上

NF の特徴に合わせて動作環境を決定

単純な NF は XDP/eBPF (in kernel) による安全で軽量な実行

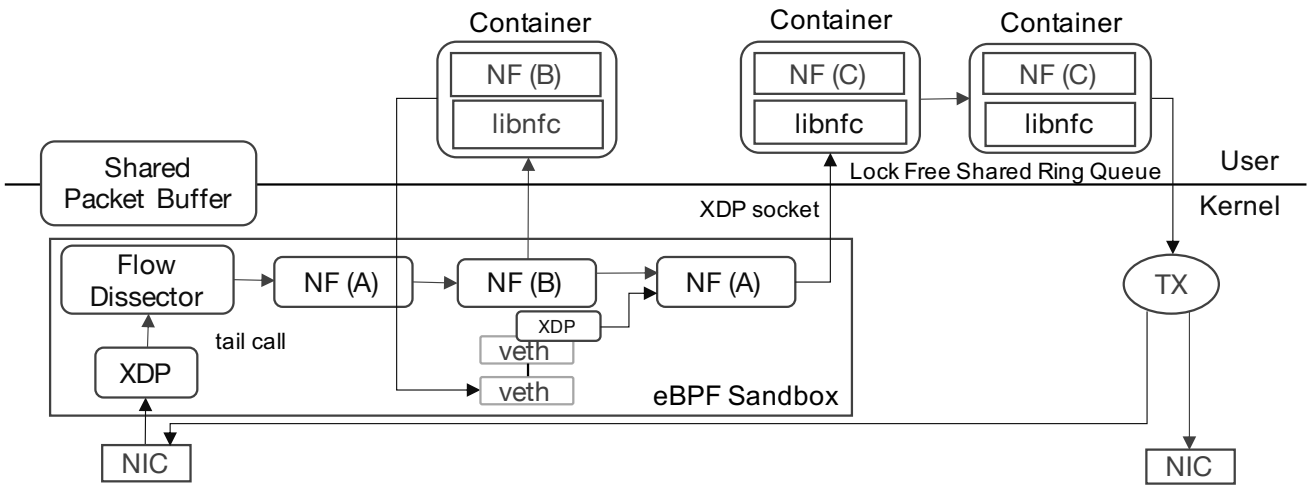
複雑な NF はユーザ空間のコンテナサンドボックス環境にて実行

*ユーザ名前空間を含む全名前空間を分離した非特権コンテナ

保護された共有パケットバッファによる安全なゼロコピーNFC

全ての NF・デバイスでメモリを共有し, パケットコピーなしでチェイニング

共有メモリを管理するライブラリを Intel MPK により分離し安全性を確保



マルチテナント環境におけるセキュリティと機能の最適配置を考慮した NFC 機構

攝待 大輔, 近藤 賢郎, 寺岡 文男　{ed, latte, tera}@inl.ics.keio.ac.jp

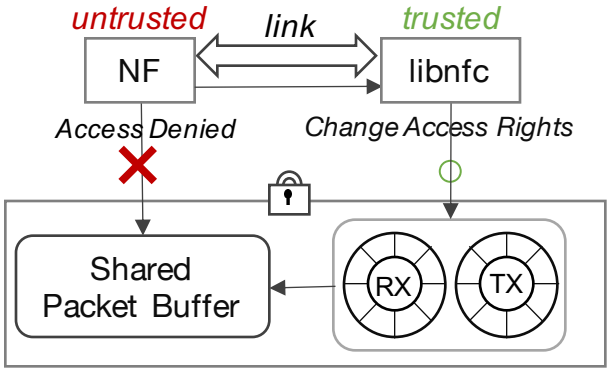
提案｜共有メモリ保護

Intel Memory Procetion Keys

PTEに4bit keyを設定したメモリマップのアクセスを単一の非特権レジスタで制御

Intel MPK によるアクセス制御

任意コードが動く User NF は不信頼
信頼できる libnfc を介してパケット操作



Intel MPK の安全性保証

バイナリ検査/書換, システムコールフィルタリング, DEP により安全性保証

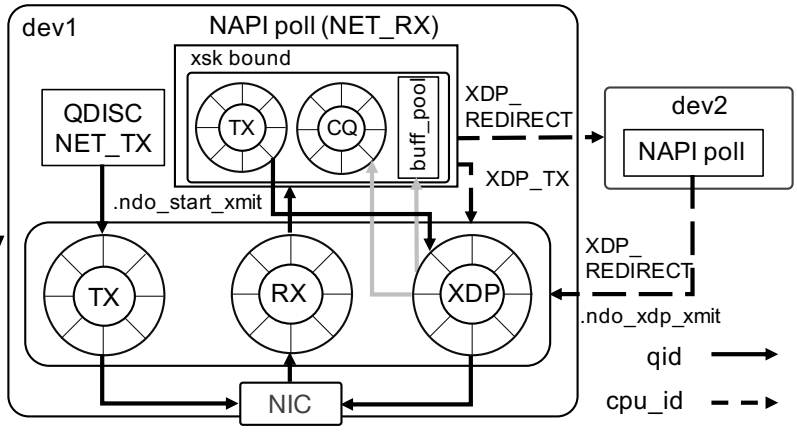
課題｜AF_XDP ZC 環境下のXDP フレームワークにおける制限

1. XDP_REDIRECT先に利用不可

XDP_REDIRECT/XDP socket TX間にて使用するXDP Ringの競合問題

2. XDP_TX/REDIRECT memcpy

異なるNAPIコンテキストからのバッファ回収による CQ/buff_pool 競合問題



解決策｜問題 1

XDP Ring を RX Ring 数とコア数分用意し XDP_REDIRECT 受動用と XDP_TX/XDP socket TX 能動用に分離

解決策｜問題 2 Zerocopy XDP_TX

NAPI コンテキスト内の XDP Ring を使い, 送信完了時は buff_pool に回収

解決策｜問題 2 Zerocopy XDP_REDIRECT

送信先とメモリを共有していることを判別し, ndo_xdp_xmit にてバッファ ID を受け渡し, 回収用に buff_pool に percpu な list_head を用意