A9N Manual

Version 0.2.1

Contents

1. Introduction

1.1. A9N Microkernel Overview

A9N は HAL を用いて移植容易性を実現する Capability-Based Microkernel です.

1.2. Capability

A9N Kernel は Object-Capability Model による強固なセキュリティ機構を実現します.
Capability とは, 偽造不可能かつ譲渡可能な Token です. User による特権的呼び出しは Kernel Object への Capability を介した操作としてモデル化されます.

1.3. Capability の使用

基本的に, User からの特権的呼び出しである Capability Call は `capability_call()`メカニズムを用いて,

```
capability_call(capability_descriptor, ... )
```

のように行われます.
しかしながら, この `capability_call()`は最も Primitive な API であるため, 実際の使用にはそれらをラップする `liba9n` ライブラリを使用することが推奨されます.
例えば, Generic Capability に対する Convert 操作には,

```
generic_result<> convert(
    generic_descriptor,
    type,
    size,
    count,
    node_descriptor,
    node_depth,
    node_index
)
```

のようなライブラリ関数が用意されます.
同様に, 他すべての Capability に対する操作へライブラリ関数が用意されます.

2. Capability Node

2.1. Introduction

Capability Node は, Capability を格納するためのコンテナとして使用される Capability です.

この Node は2^{radix}個の Slot を持つ Radix Tree です.

子として Node が保持可能であり, 複数階層の Capability Tree を作成できます.

2.2. Addressing

Node 内の Capability は Descriptor によって, 以下のように Addressing されます :

1. Descriptor の先頭 8bit を取り出し, `depth_bits` とします
   - `depth_bits` は探索可能 bit 数の最大値を表します
   - 例えば, 64bit Computer では64 − 8の 56bit が標準の `depth_bits` となります
2. Node 内の `radix_bits` から Index に使用する Bit を決定します
3. Descriptor から 2 で得た Index 分の bit を取り出し, 子を取得します
4. 子に対して, Descriptor を使い切るか終端に到達するまで再帰的に探索を行います

Node と Descriptor は Page Table と Virtual Address のような構造をしています.

2.3. Node API

2.3.1. **`copy`**

2.3.2. **`move`**

2.3.3. **`remove`**

2.3.4. **`revoke`**

3. Generic

3.1. Introduction

Generic は, メモリを抽象化する Capability です.
A9N カーネルはヒープを持たないため, カーネルオブジェクトのようなシステム内で使用するメタデータのメモリは, ユーザーが明示的に割り当てる必要があります.
生の物理メモリをユーザーに直接使用させるのはセキュリティ上のリスクが発生するため, `convert()`メカニズムを用いて安全な割当ポリシーを実現します. `convert()`は対象 Generic を切り出し, カーネルオブジェクトを作成します. 作成したオブジェクトは親 Generic の Dependency Node に登録され, 初期化処理などに使用されます.

3.2. Generic API

3.2.1. **convert**

```
common::error convert(
    a9n::capability_descriptor generic_descriptor,
    library::capability::capability_type       type,
    library::common::word                      size,
    library::common::word                      count,
    library::capability::capability_descriptor node_descriptor,
    library::common::word                      node_index,
)
```

name	description
`generic_descriptor`	対象 Generic への Descriptor
`type`	作成する Capability の Type
`size`	作成する Capability の Size
`count`	作成する Capability の個数
`node_descriptor`	格納先 Node への Descriptor
`node_index`	格納先 Node の Index