Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Smart Attacks require Smart Defence

Moving Target Defence

Prof. Dr. Gabi Dreo Rodosek

Executive Director of the Research Institute CODE

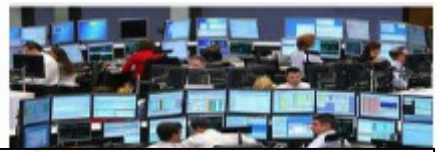
Virtual, Connected, Smart World

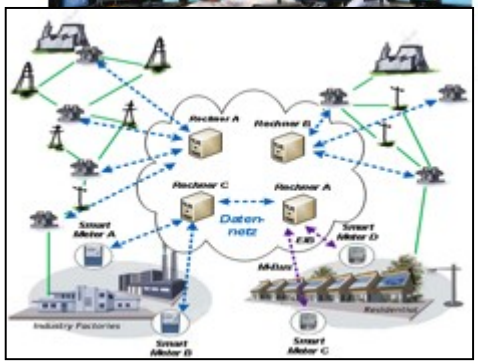
FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

- **Real World**
  - Billions of connected devices
  - 163 Zettabyte of data until 2025
  - Systems are getting “smarter” (with AI) and autonomous

Paradigm Shift

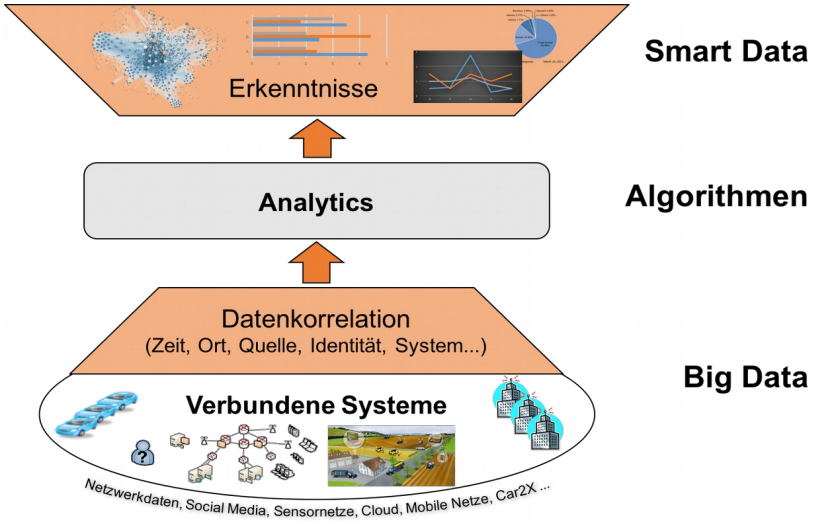
Smart Grid, Connected Car / Connected Plane, Financial Sector, e-Health, Industry 4.0, Military (connected) operations, ...

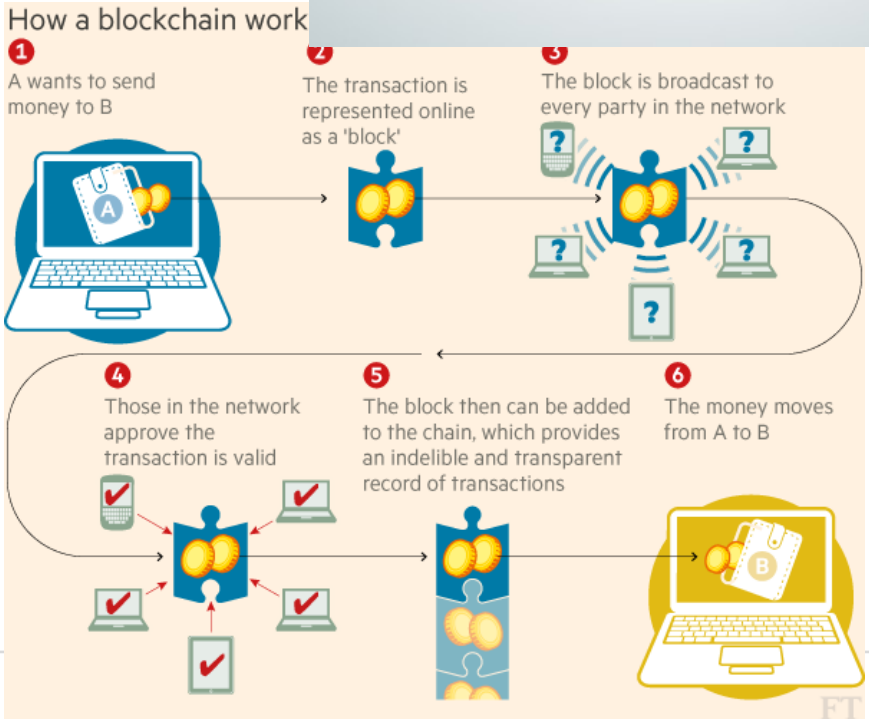




ICT is the key technology of the digital society!
Cyber security is fundamental for digital society!

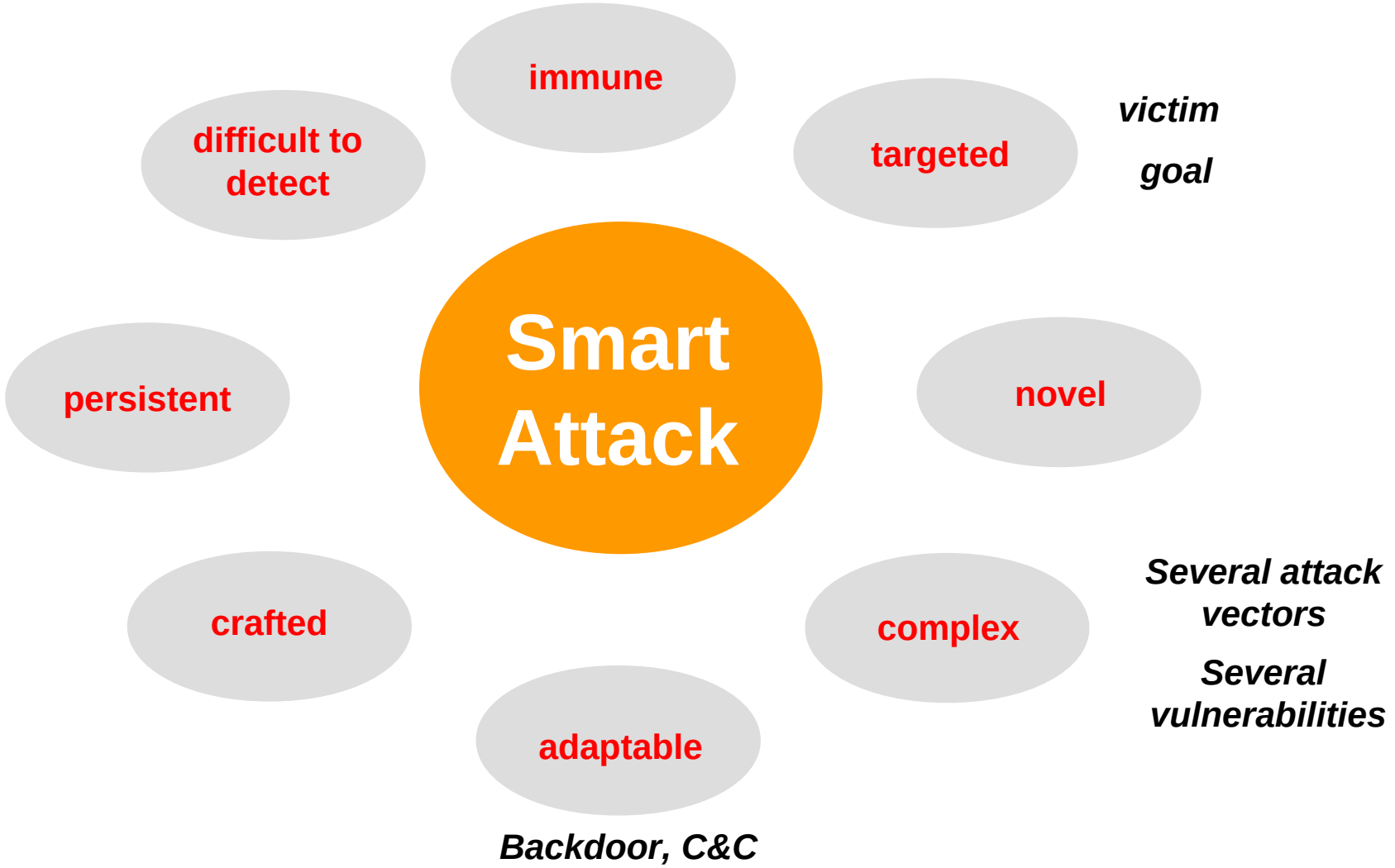
ICT is developing with tremendeous speed





Smart Attacks:
Advanced Persistent Threats (APT)

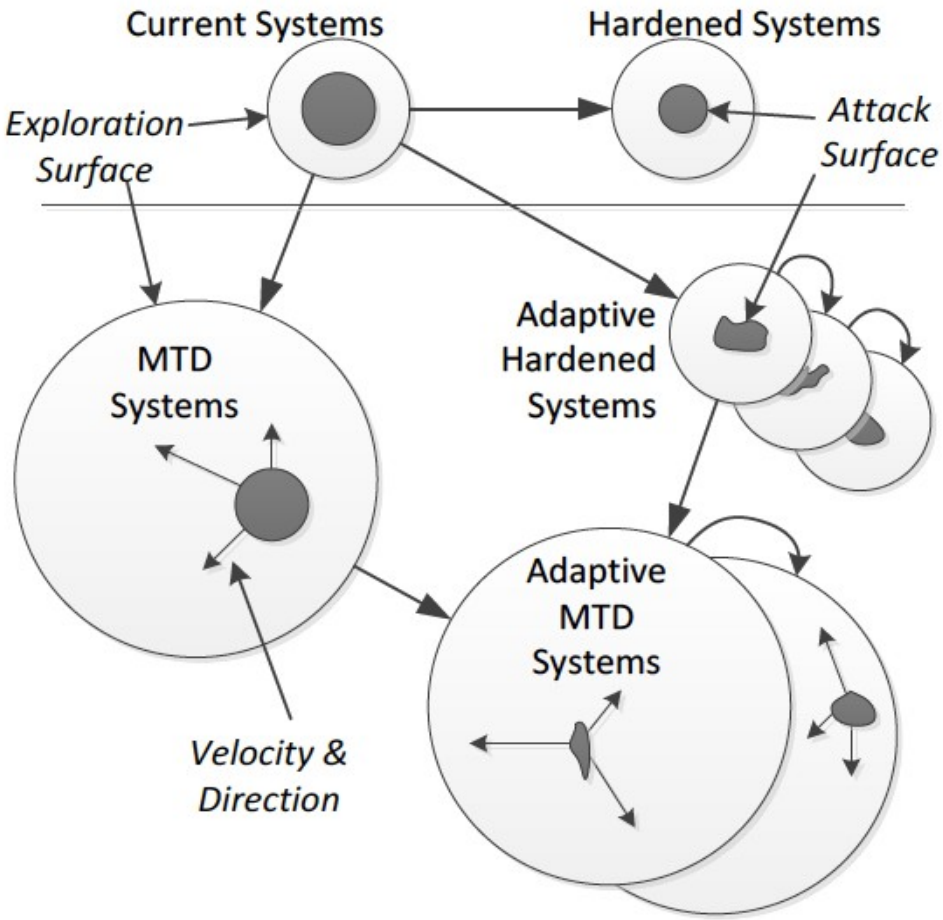
FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München



Current State of Cyber Defence

- **Attackers have natural advantage**
  - "Static" attack surface
  - Near-unlimited time for reconnaissance / preparation
  - Access to 0-day vulnerabilities
  - Attacker only needs to find a single vulnerable entry point
  - Adversaries have an **asymmetric advantage** in that they have the time to study a system, identify its vulnerabilities, and choose the time and place of attack to gain the maximum benefit

Attack Surface



Cyber Kill Chain

1. Reconnaissance: The attacker collects useful information about the target

2. Access: The attacker tries to connect or communicate with the target to identify its properties (versions, vulnerabilities, configurations, etc.)

3. Exploit Development: The attacker develops an exploit for a vulnerability in the system in order to gain a foothold or escalate his privilege

4. Attack Launch: The attacker delivers the exploit to the target. This can be through a network connection, using phishing-like attacks, or using a more sophisticated supply chain or gap jumping attack (e.g., infected USB drive)

5. Persistence: The attacker installs additional backdoors or access channels to keep his persistence access to the system

Towards Moving Target Defence

Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

Changing the Paradigm:

- Aim to substantially increase the cost of attacks by deploying and operating networks/systems to makes them less deterministic, less homogeneous, and less static
- Continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency
- Dynamically altered in ways that are manageable by the defender yet make the attack space appear unpredictable to the attacker
- Introduce asymmetric uncertainty that favors defender over attacker
- Attackers do not have adequate time to find vulnerabilities / create exploits

MTD Categories

- **Very diverse, specialized against specific attack vectors, yet mostly isolated**

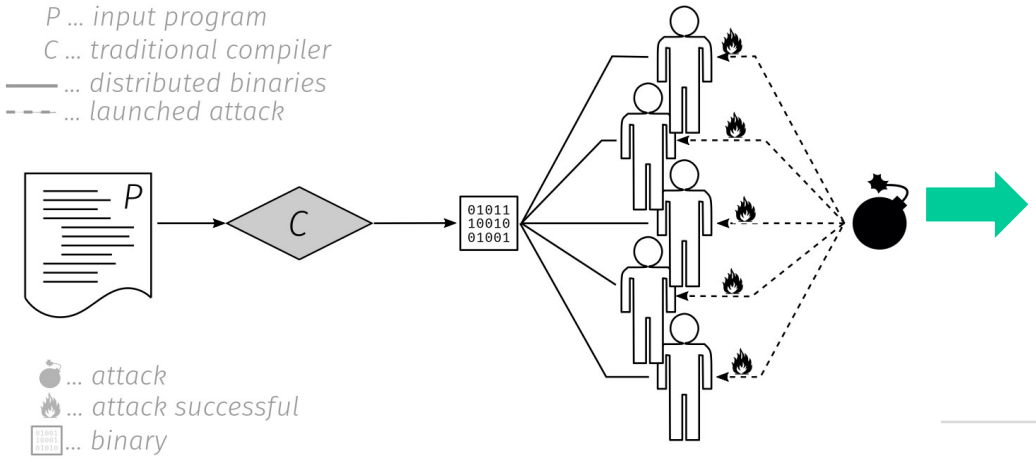
- **System-based MTD**
  - Software-based
    - Application, OS, Data
  - Hardware-based: processor, FPGA
- **Network-based MTD**
  - MAC layer: changing MAC address
  - IP layer: IP randomization
  - TCP (Traffic) layer: changing network protocol
  - Session layer

Software-based MTD

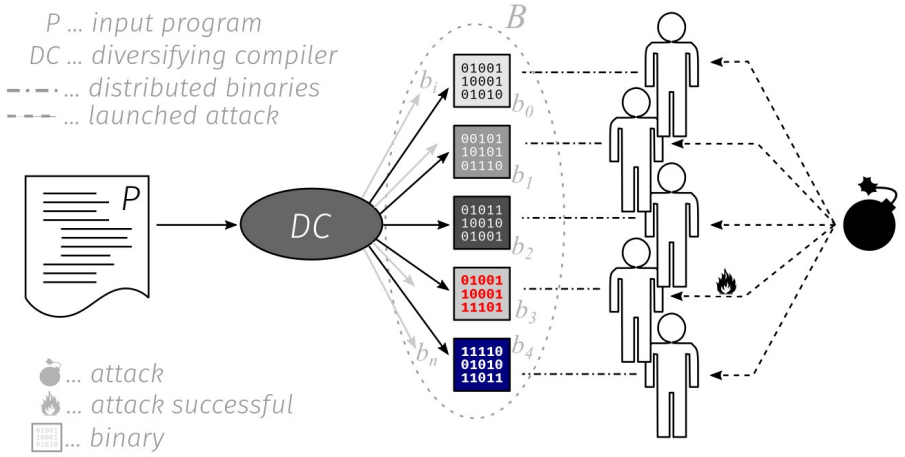
FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

- **Goals**
  - Prevent unwanted modification, protect software against analysis
- **Types**
  - Dynamic Runtime Environment: Address Space Layout Randomization (ASLR), Instruction Set Randomization
  - Dynamic software: In-place code randomization, Compiler-based Software Diversity

Software Monoculture



Software Diversity



Network-based MTD

- **Network reconnaissance is the first step for attackers to collect network and host information and prepare for future targeted attacks**

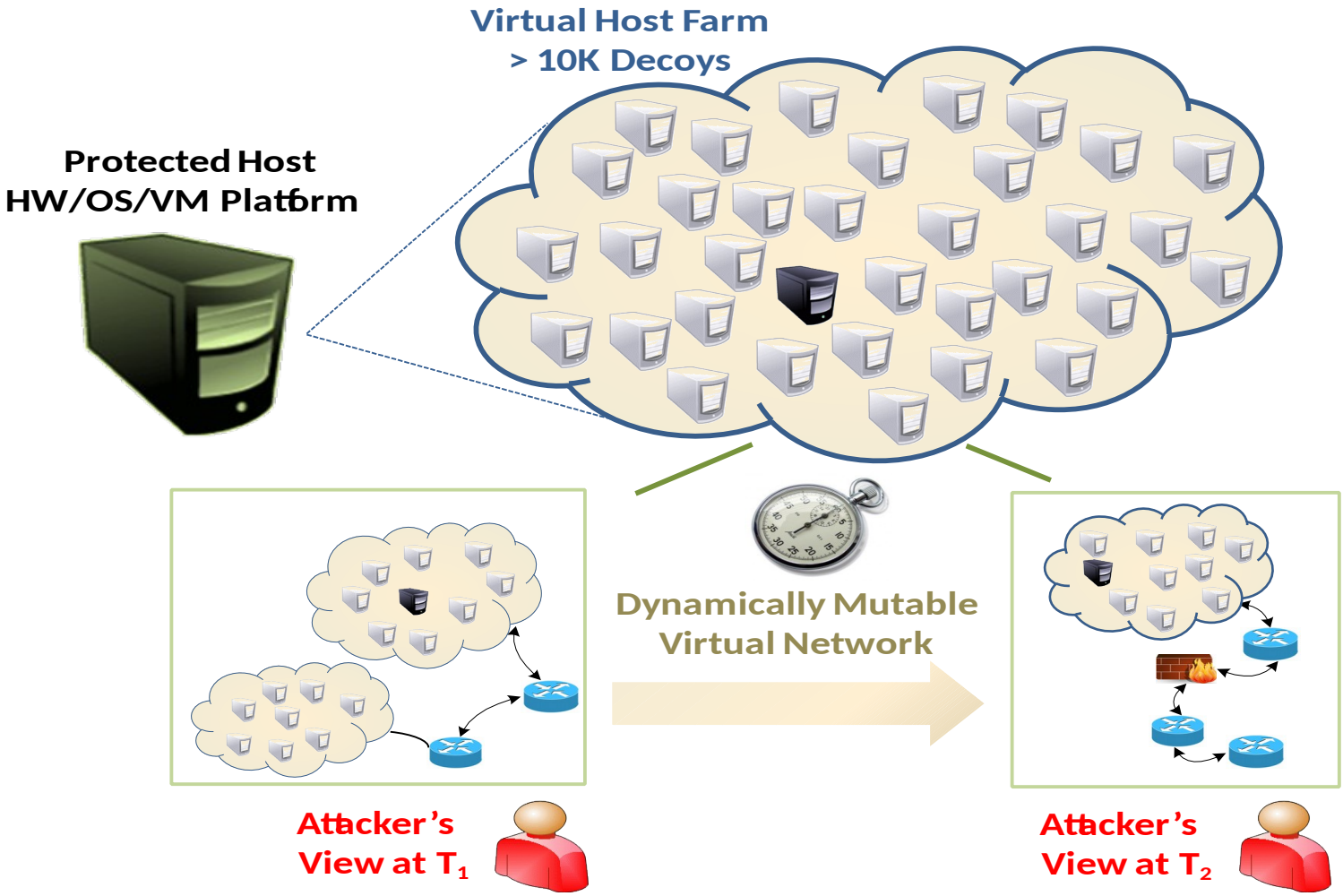
- **Goal: make the scanning results expire soon or give the attacker a different view of the target system**
  - IP address randomization, Port randomization

Threat Model

- **Data leakage attacks**, **e.g., steal crypto keys from memory**
- **Denial of Service attacks**, **i.e., exhaust or manipulate resources in the systems**
- **Injection attacks**
  - Code injection: buffer overflow, ROP, SQL injection
  - Control injection: return-oriented programming (ROP)
- **Spoofing attack**, **e.g., man-in-the-middle**
- **Authentication exploitation**: **cross-cite scripting (XSS)**
- **Scanning**, **e.g., port scanning, IP scanning for targeted attack**
- **Physical attack**: **malicious processor**

Dynamic Virtualized Network Topology

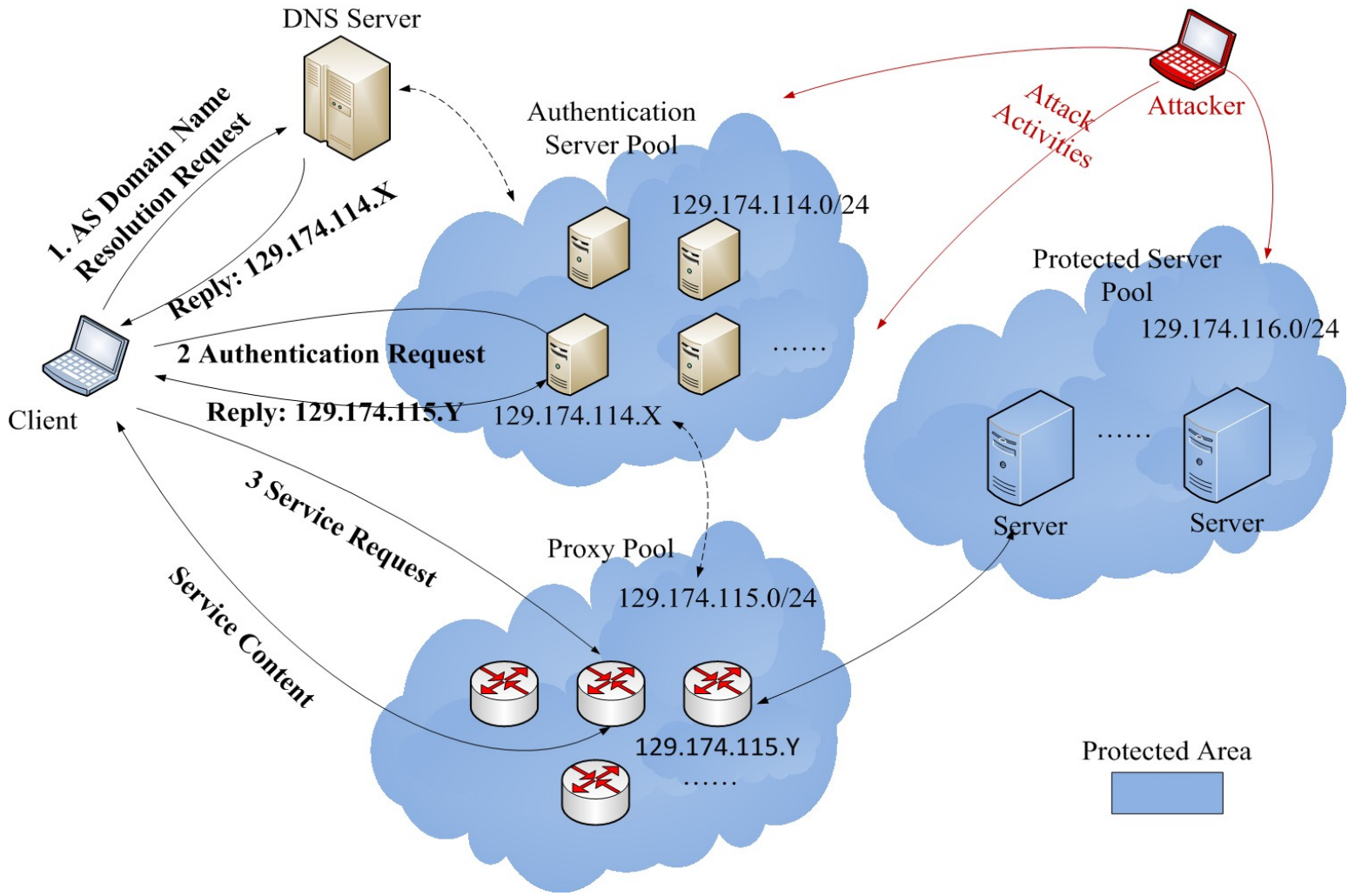
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München



Two Challenges in Network-based MTD

1. **Service availability**
   - Authenticated clients should always know the new IP address/port number
   - When the IP and port changes, the connection still maintained, minimizing service downtime
2. **Service security**
   - Only the authenticated users can access the service
   - How to mitigate insider attacks?
3. **Service Quality**
   1. Meeting Service Level Agreements

Three layer protection: Decoys in each layer

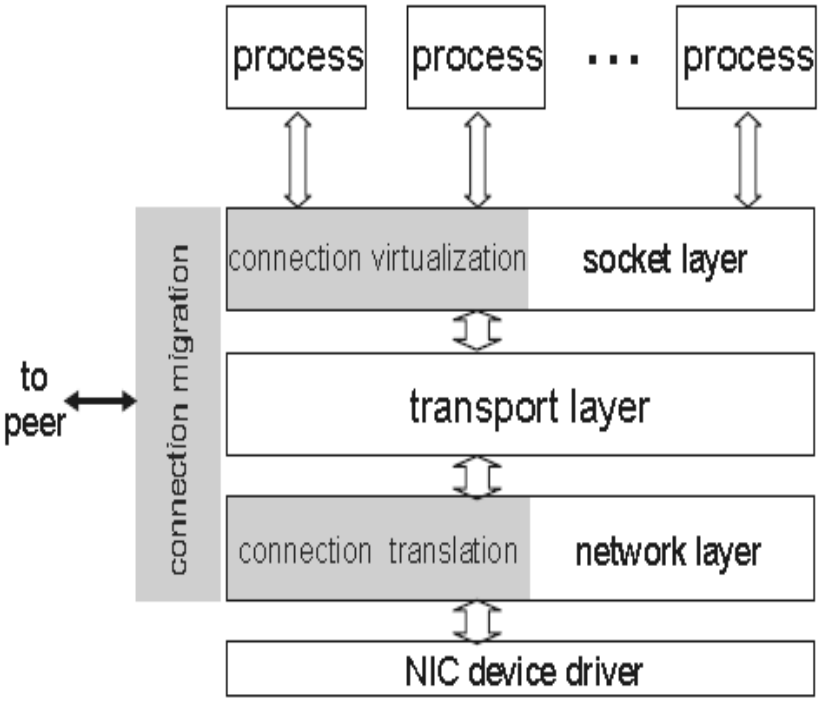


Seamless TCP Connection Migration

FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

- **Keep end-to-end transport connection alive through separating transport endpoint identification from network endpoint identification.**

- **Three components**
  - Connection virtualization
  - Connection translation
  - Connection migration



Connection Virtualization

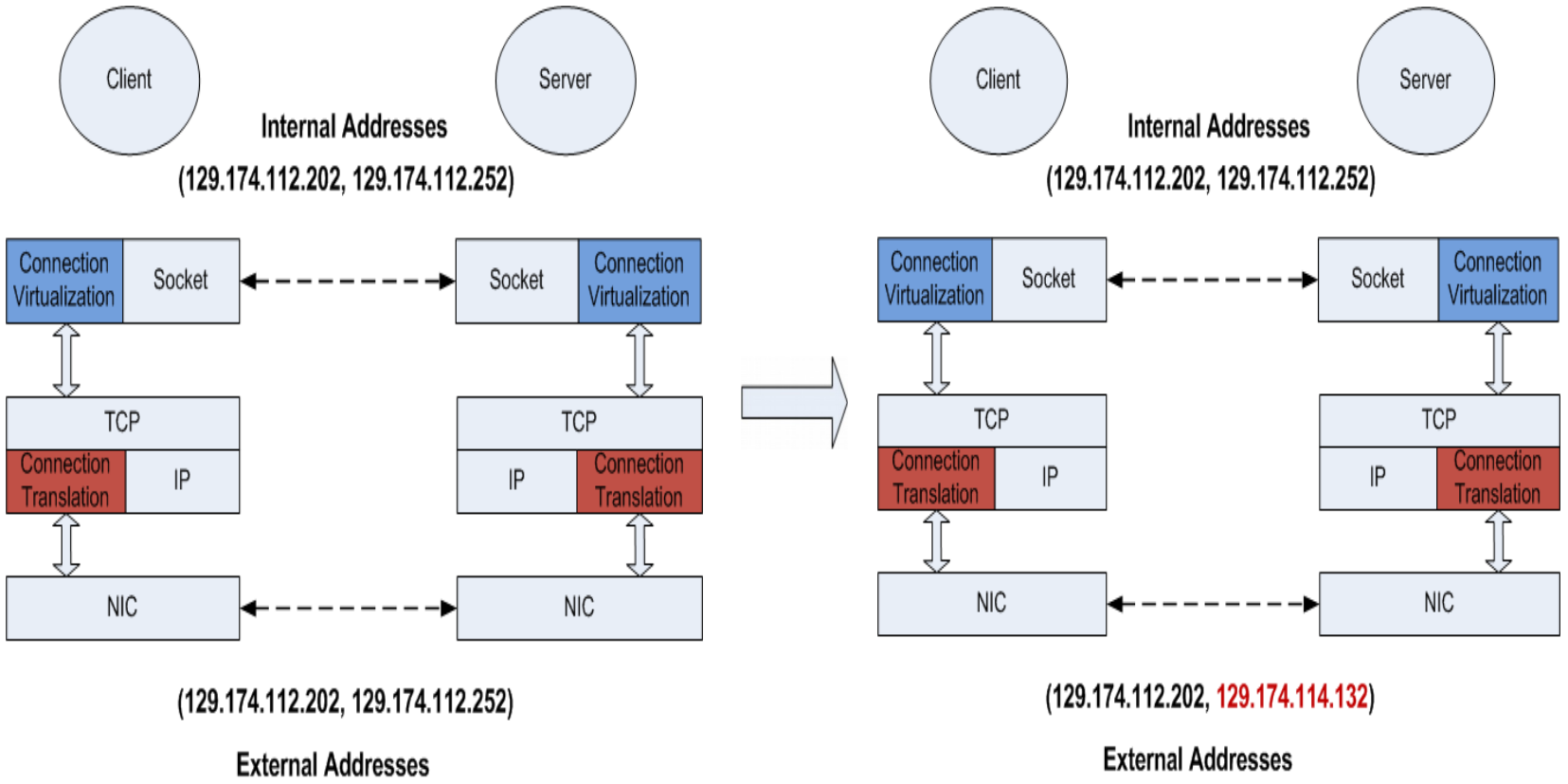
- **Internal address for applications**
  - IP address and Ports
  - never changes for one connection
- **External address for communications**
  - IP addresses and Ports
  - may change according to MTD requirements
- **A map to translate between Internal address and External address**

Connection Translation

FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

At beginning,
internal address = external addresses

Server changes its IP address



Network Migration

- **After the server changes its IP address and port, it will inform the client to update the internal-external address mapping**
- **Migration Steps: protected by a shared secret key**
  - Suspend a connection
    - Keep connection alive
  - Resume a connection
    - Update internal-external endpoints mappings
    - Server sends UPDATE packet
    - Client sends UPDATE_ACK packet
- **Both endpoints need to know the same internal address pair**

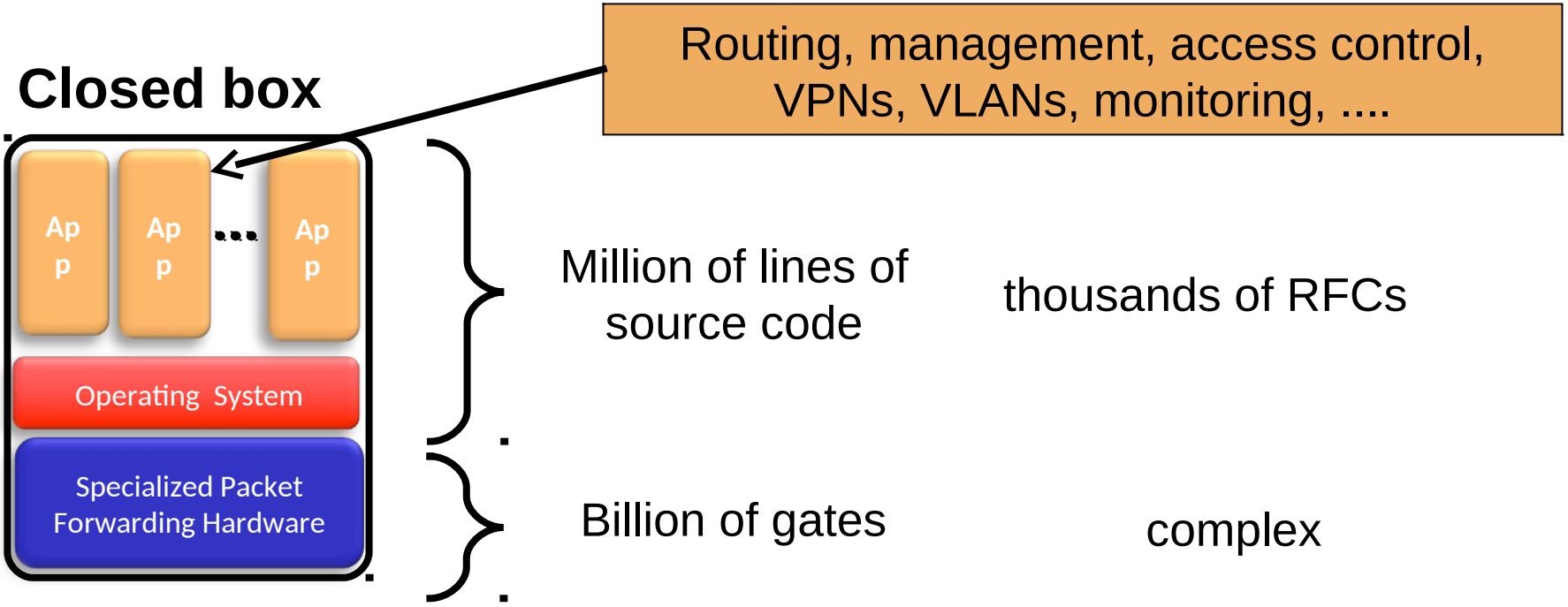
We need more flexibility on the network layer

HOW?

Software-Defined Networking (SDN)

Software Defined Networking

Situation today: closed „boxes“

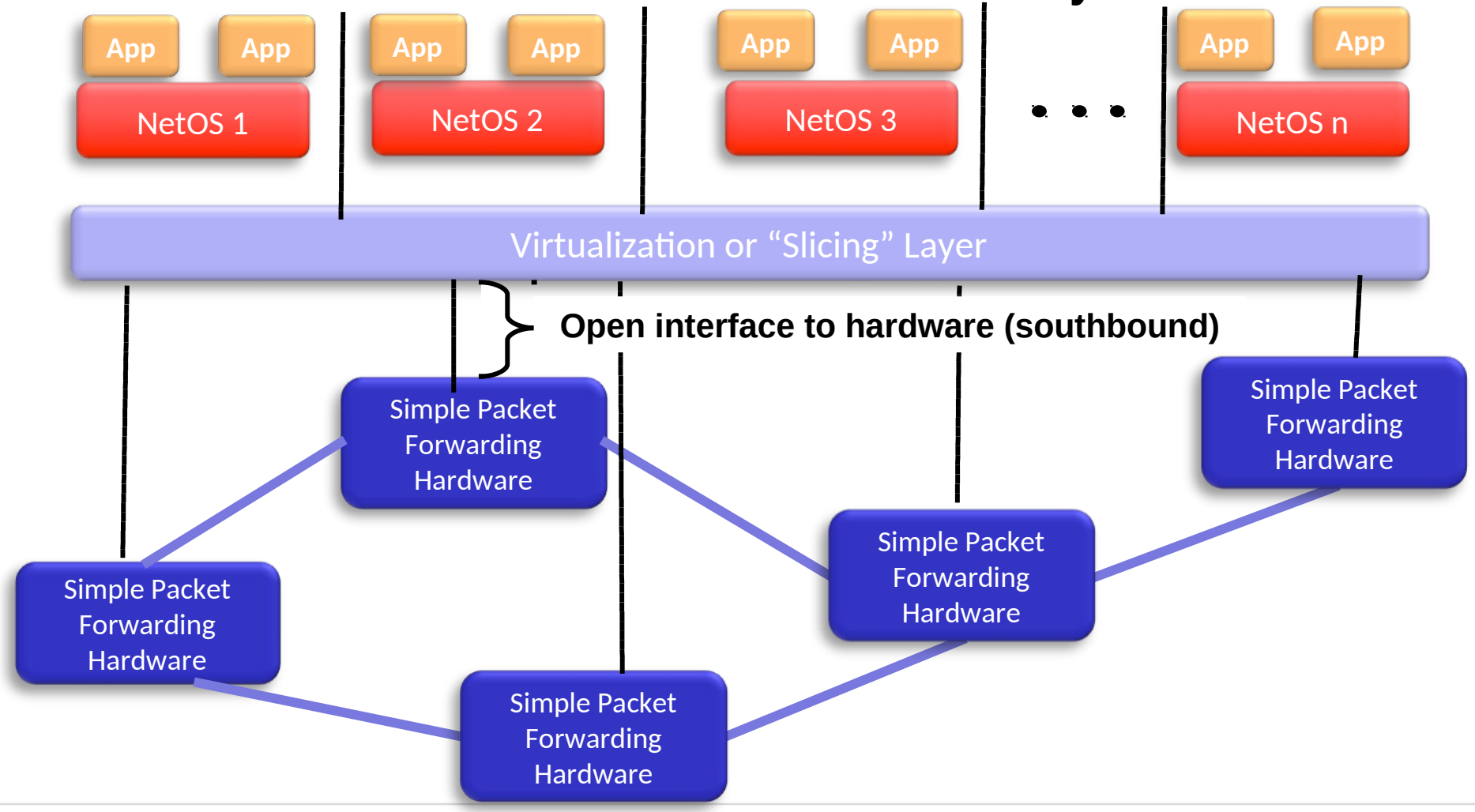


- Closed, vertically integrated
- Many complex functions baked into infrastructure (OSPF, firewalls, NAT, ...)

The idea: Separate “Control“ from „Switching“

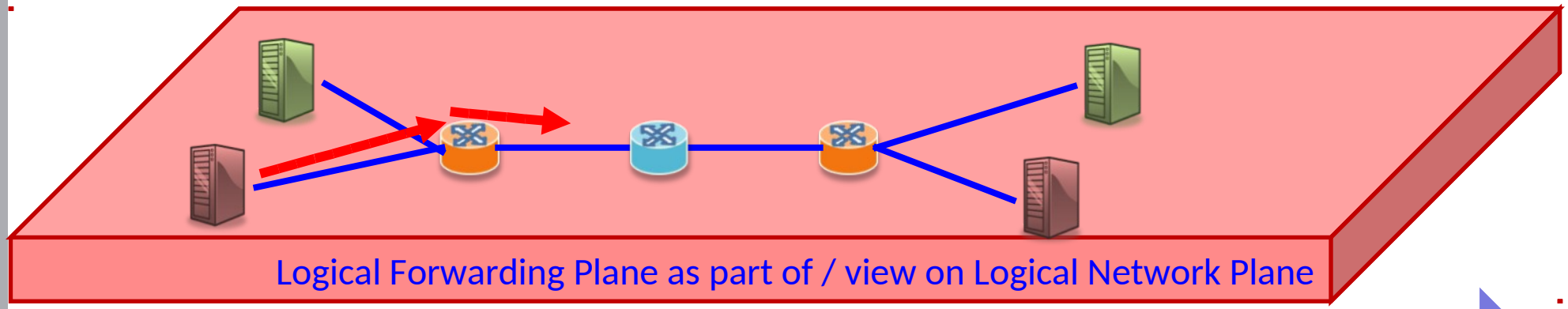
FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

- Serveral NetOS → virtualized centralized Layer

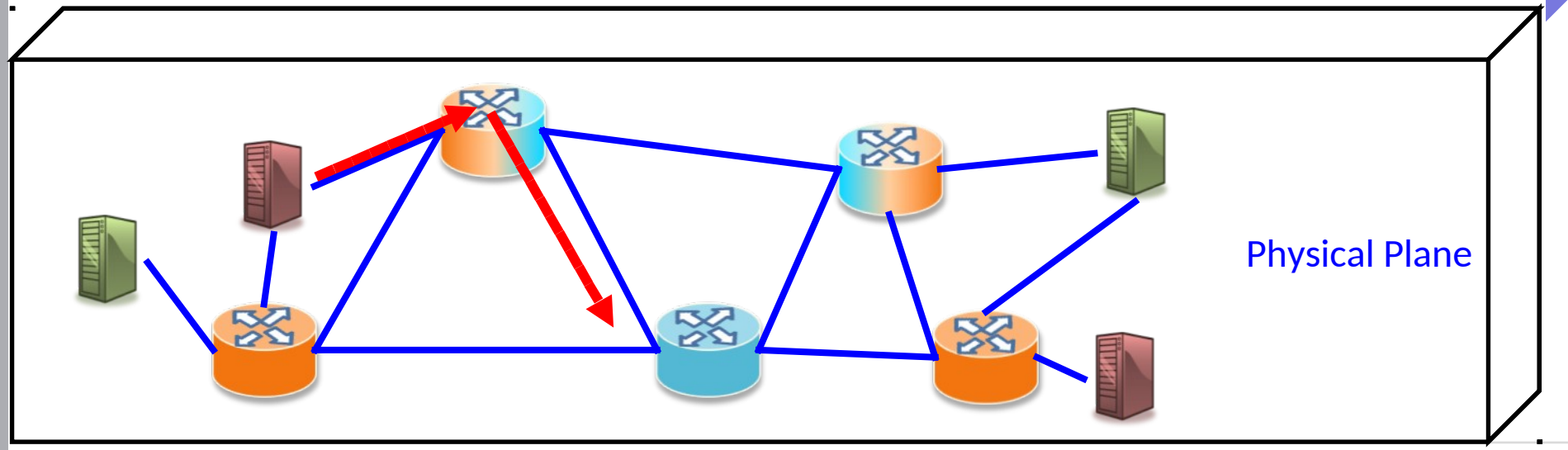


SDN Controller vs SDN Switch

FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

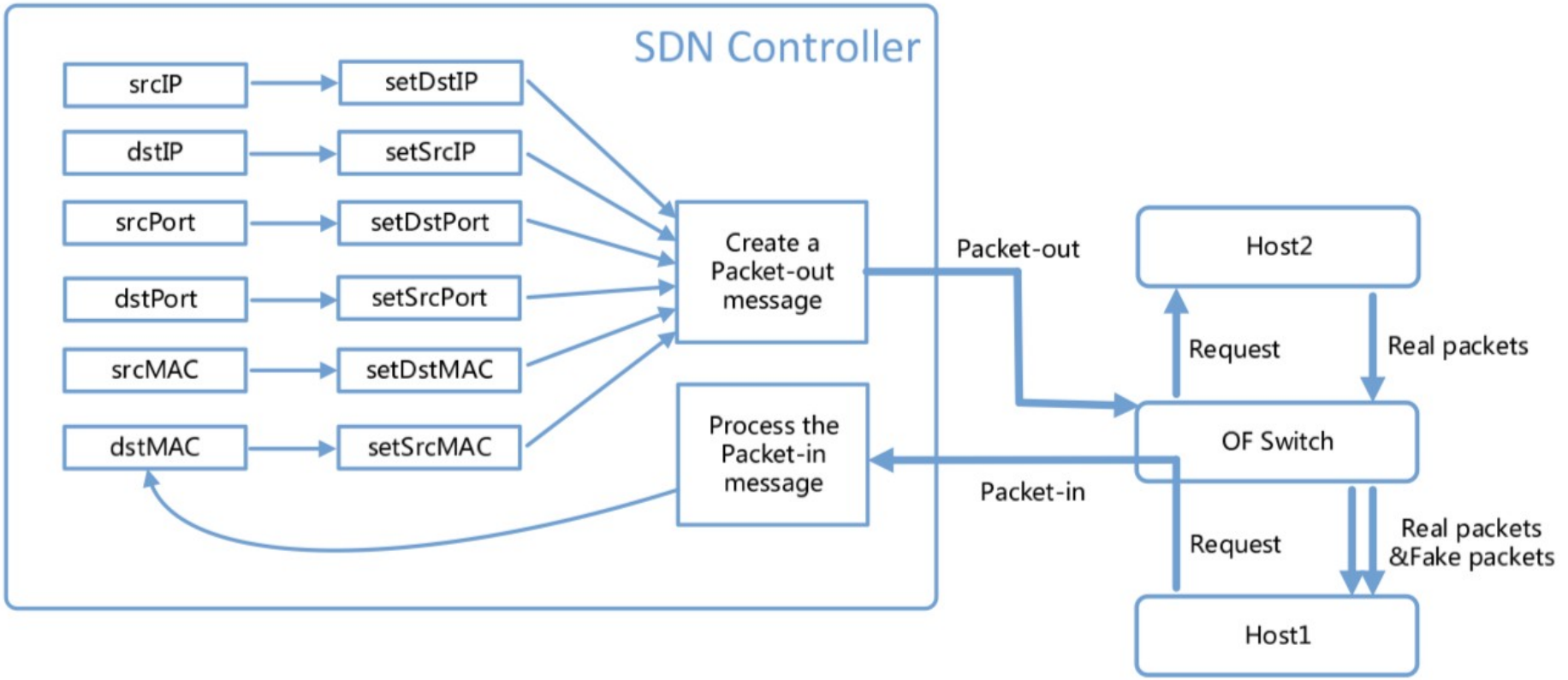


Packets traversing the network = Moving in logical + Physical Plane



Port Obfuscation (MTD) with SDN Controller

FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München



MTD: a Game Changer

- **A promising approach with several techniques and open questions**
  - **Definition of the attack surface and the possible transformations**
  - **Redundancy**
  - **Actuality**
    - What part (critical) should be changed at a specific time? What are the most important transformations at a time? What happend if a transformation is not successful?
  - **Functional equivalency**
  - **Cooperation between different MTD techniques**
  - **Integration with existing tools, like Intrusion Detection / Prevention Tools, Firewalls, ...)**
  - **...**