

Network Security - TACS

www.tacs.eu

[TACS-Facebook](#)

Network security

Network security is defined as "the protection of a computer network and its services from unauthorised modification, destruction, or disclosure".

TACS

June 2014

Network security

- Network security is defined as ***"the protection of a computer network and its services from unauthorised access, modification, destruction, or disclosure"***.
- Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- Network security involves the authorization of access to data in a network, which is controlled by the network administrator.
- Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.
- Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network security concepts

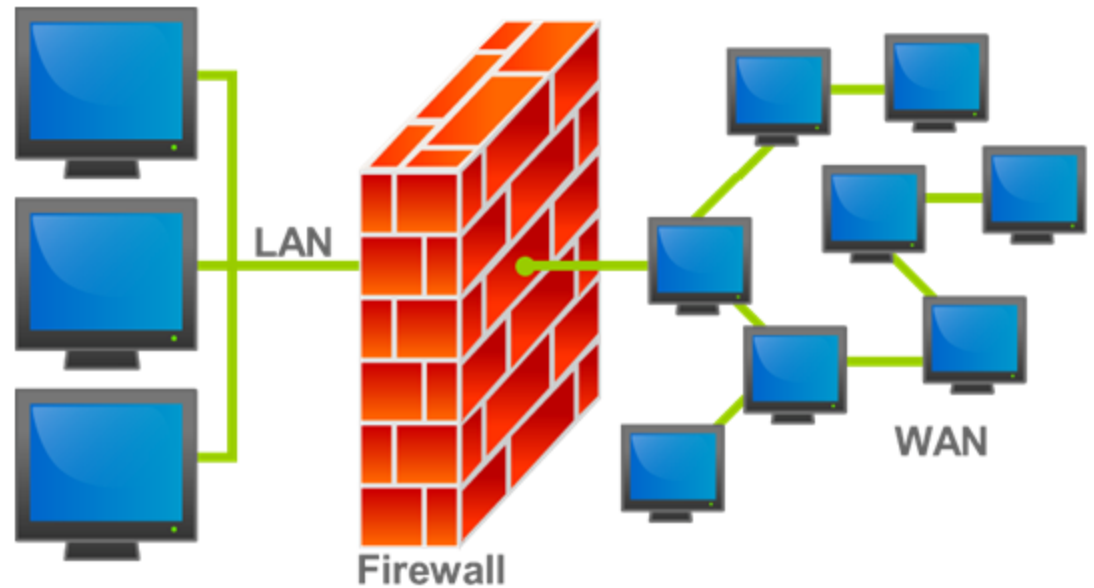
- **Access Control Systems**
- **Application security**
 - Antivirus software
 - Secure coding
 - Security by design
 - Secure operating systems
- **Authentication**
 - Two-factor authentication
 - Multi-factor authentication
- **Authorization**
- **Firewall (computing)**
- **Intrusion detection and prevention systems**

Network Security management

- Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

Firewall

- In computing, a firewall is a software or hardware-based network security system that controls the incoming and outgoing network traffic based on applied rule set.
- A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.
- Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet.
- Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.



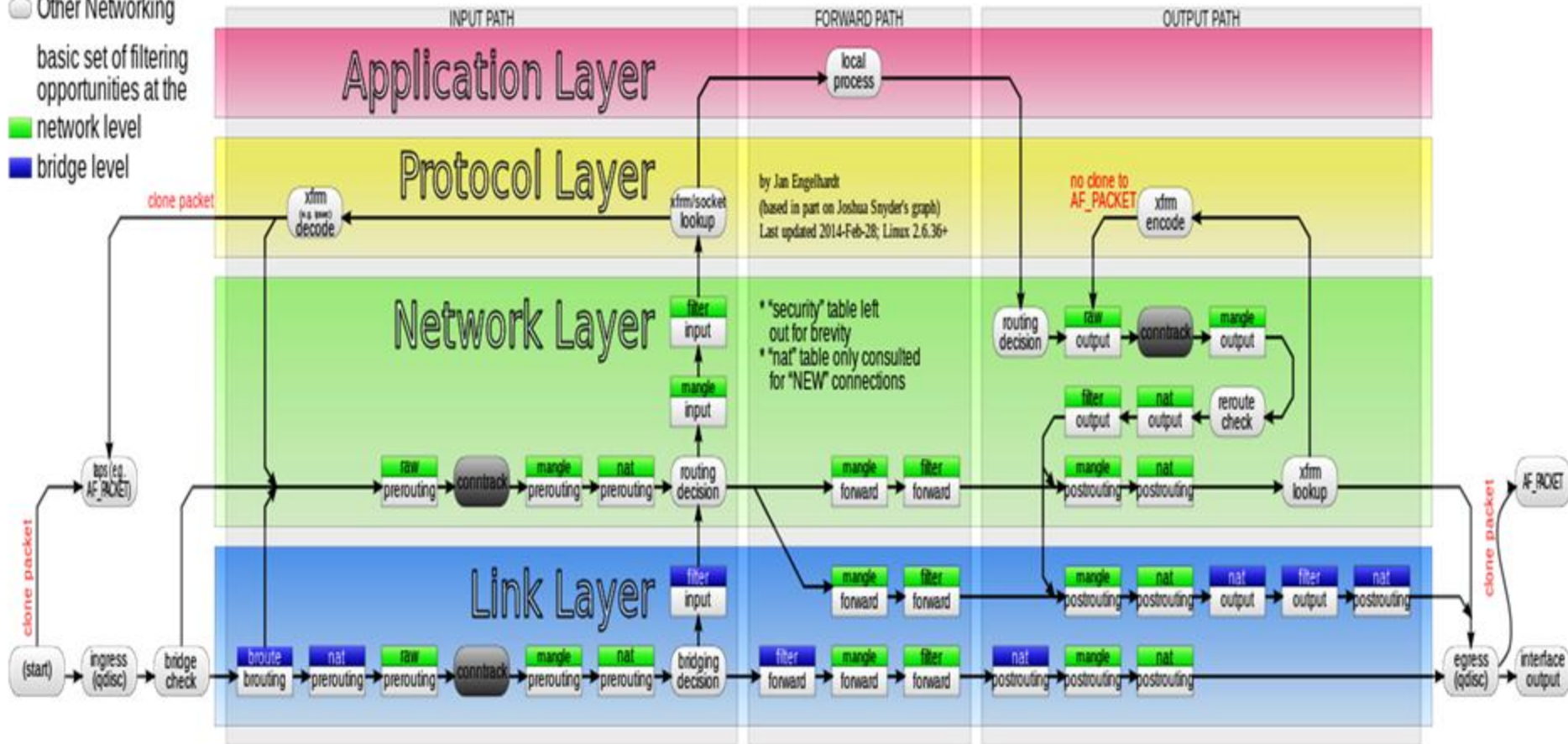
Firewall Types

- Network layer or packet filters
- Application-layer
- Proxies
- Network address translation (NAT as a firewall)

An illustration of flow of network packets through Netfilter (Firewall)

Packet flow in Netfilter and General Networking

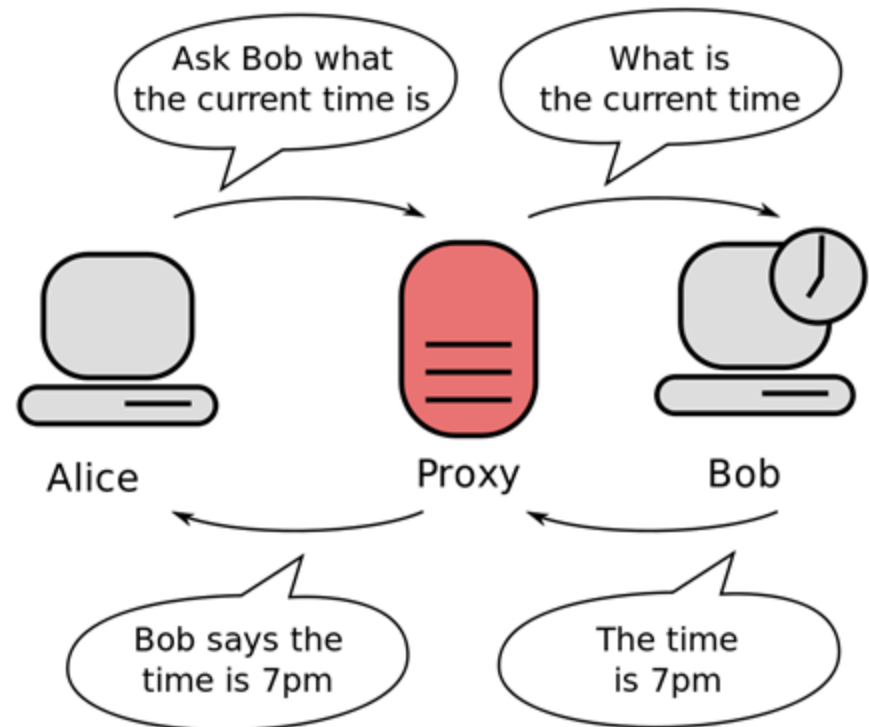
- Other NF parts
- Other Networking
- basic set of filtering opportunities at the
- network level
- bridge level



Proxy server

- In computer networks, a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web and providing anonymity.

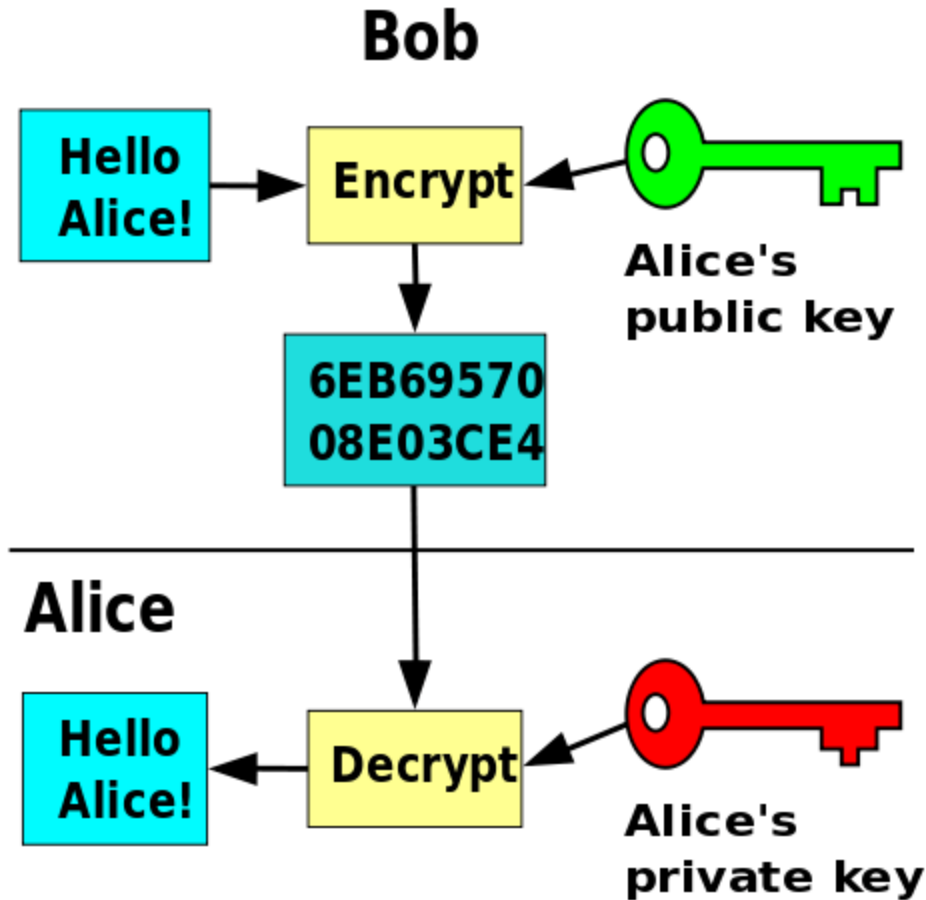
- A proxy can keep the internal network structure of a company secret by using network address translation, which can help the security of the internal network. This makes requests from machines and users on the local network anonymous. Proxies can also be combined with firewalls.



Network address translation (NAT)

- NAT is a methodology of modifying network address information in IP datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another.
- The NAT function was originally developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization.
- However, Firewalls often have network address translation {NAT} functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range". Firewalls often have such functionality to hide the true address of protected hosts.
- Hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

Encryption

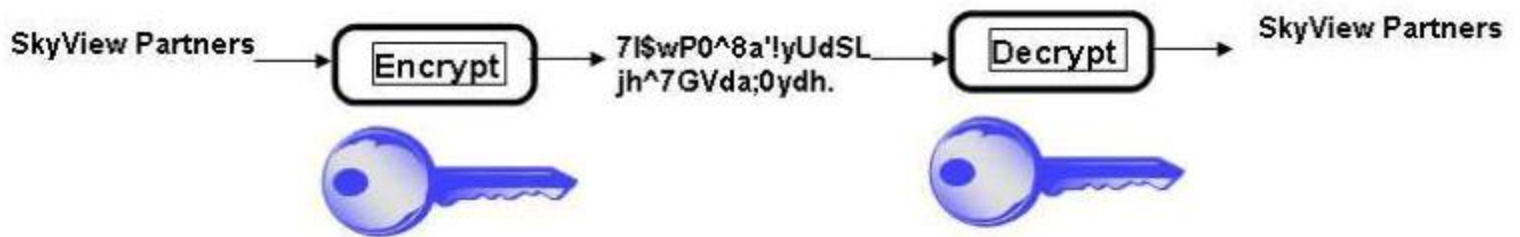


Types of Encryption

DES
TripleDES
AES
RC5

Symmetric Keys

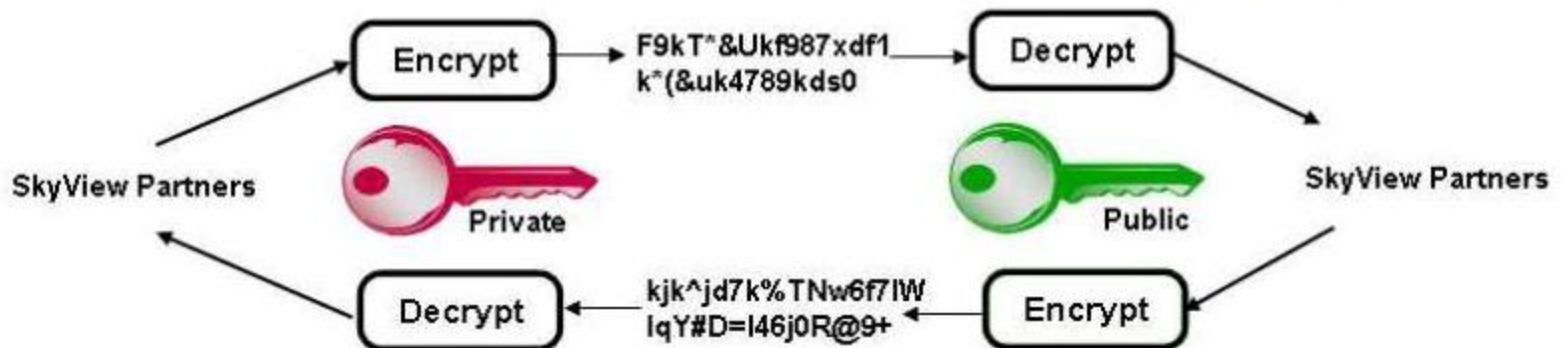
- ◆ Encryption and decryption use the **same key**.



RSA
Elliptic
Curve

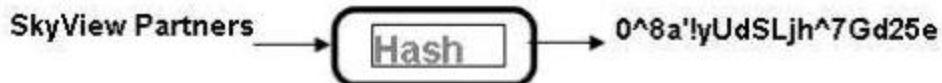
Asymmetric keys

- ◆ Encryption and decryption use different keys, a **public key** and a **private key**.



MD5
SHA-1

One-way hash



Security Architecture

Three Interconnected Layers for SDP (CheckPoint)

Software-Defined Protection (SDP) Architecture

MANAGEMENT LAYER: Integrates security with business process

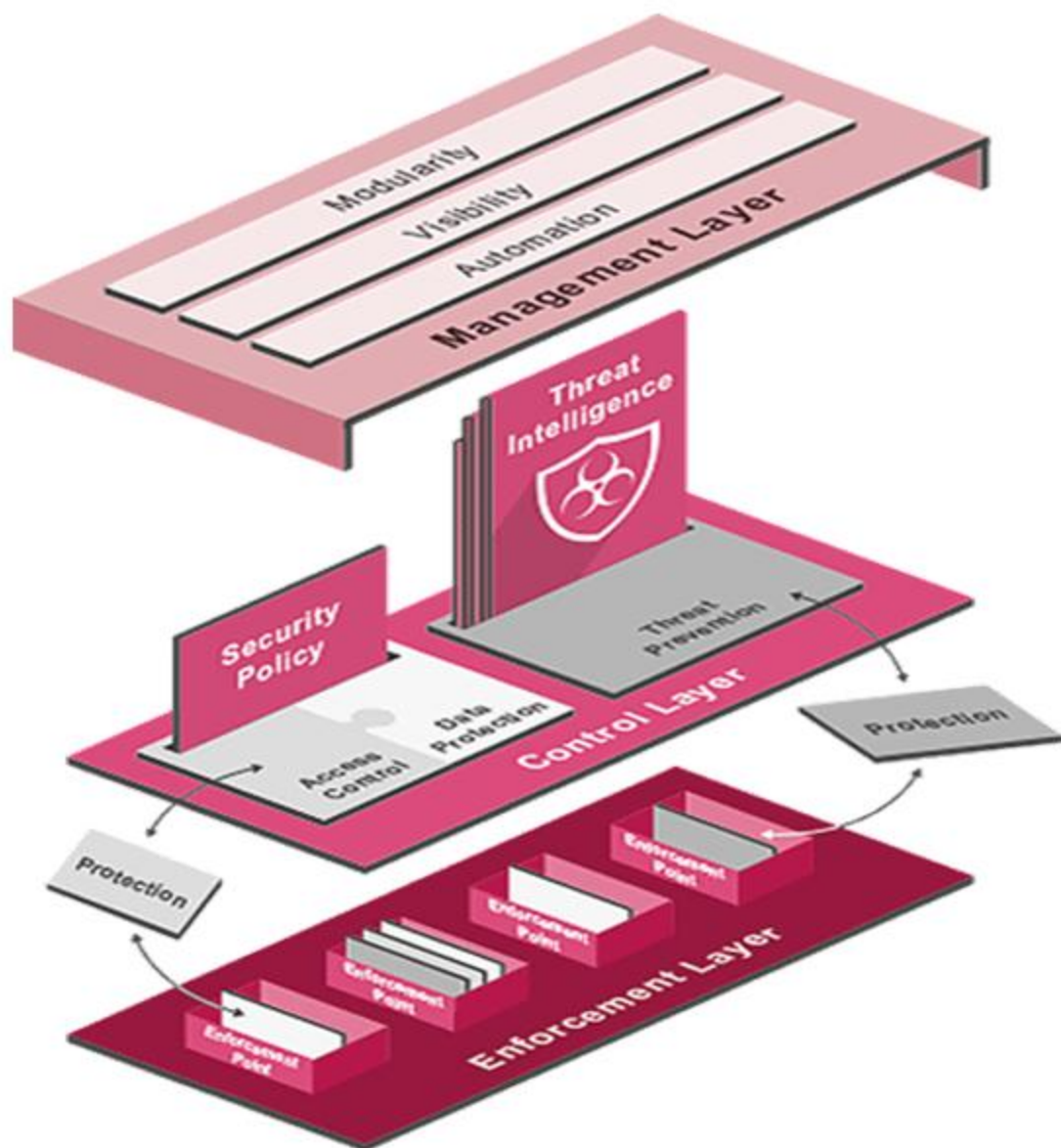
- Modularity
- Centralized visibility
- Automation and orchestration

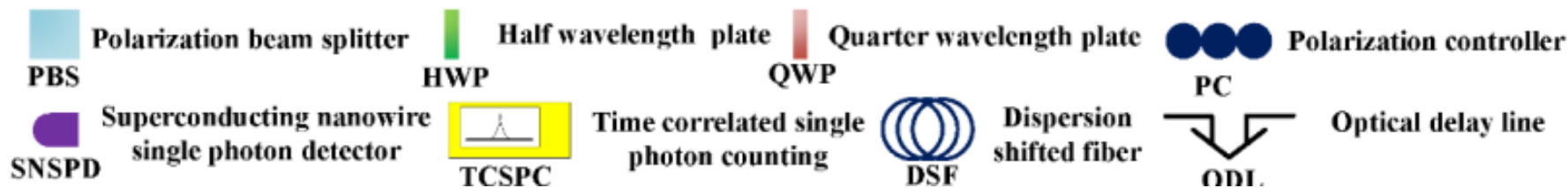
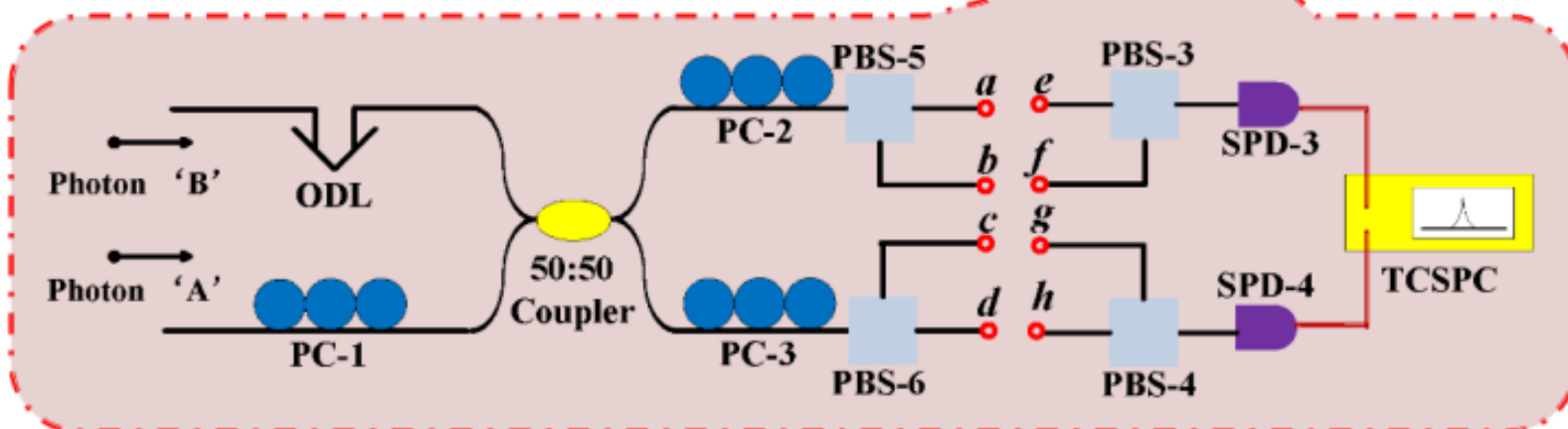
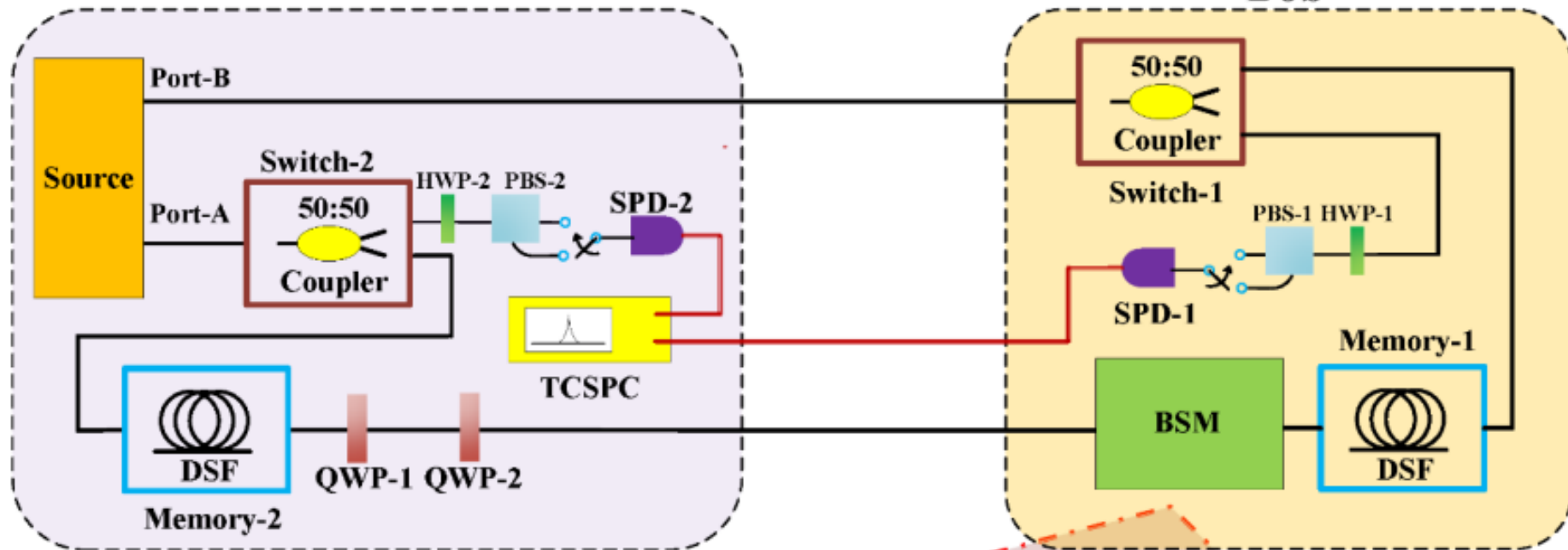
CONTROL LAYER: Delivers real-time protections to the enforcement points

- Threat intelligence
- Access control
- Data protection based on classification

ENFORCEMENT LAYER: Inspects traffic and enforces protections in well-defined segments

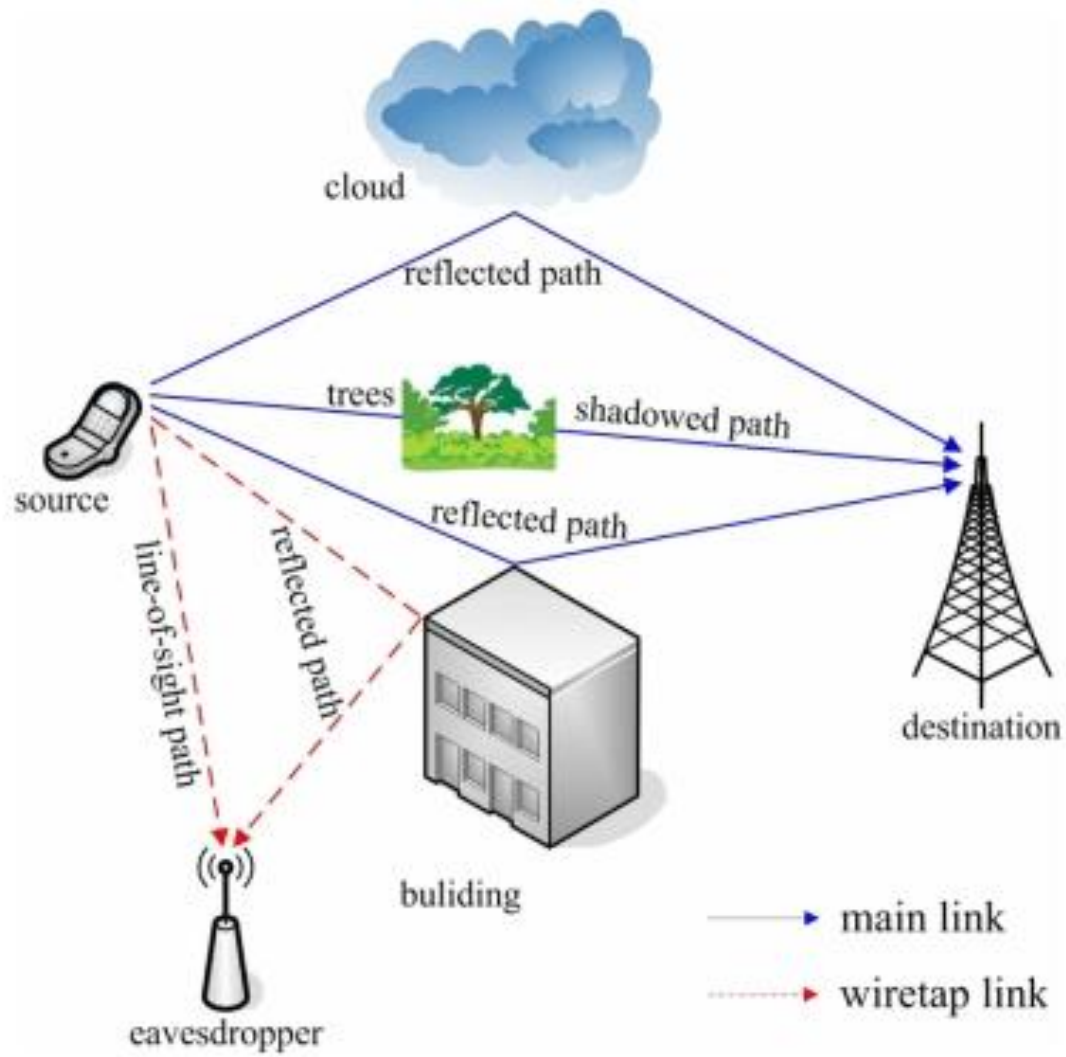
- Segmentation
- Centralized control
- Infection prevention

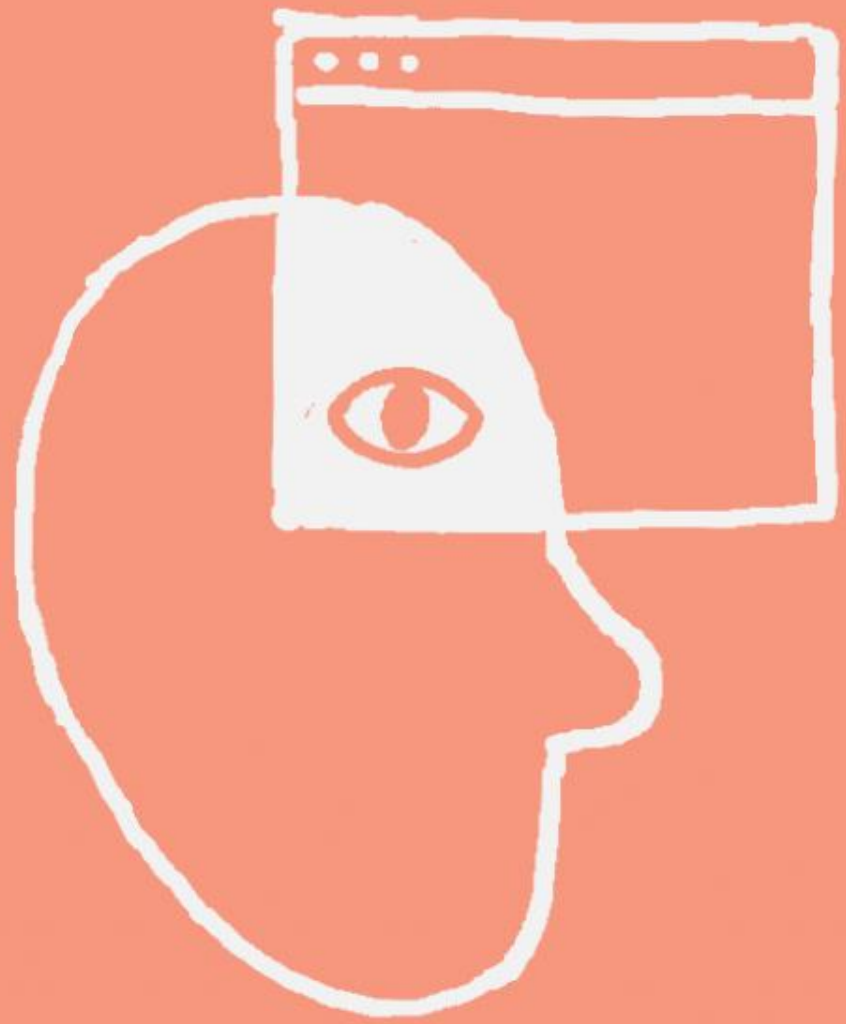


Alice**Bob**

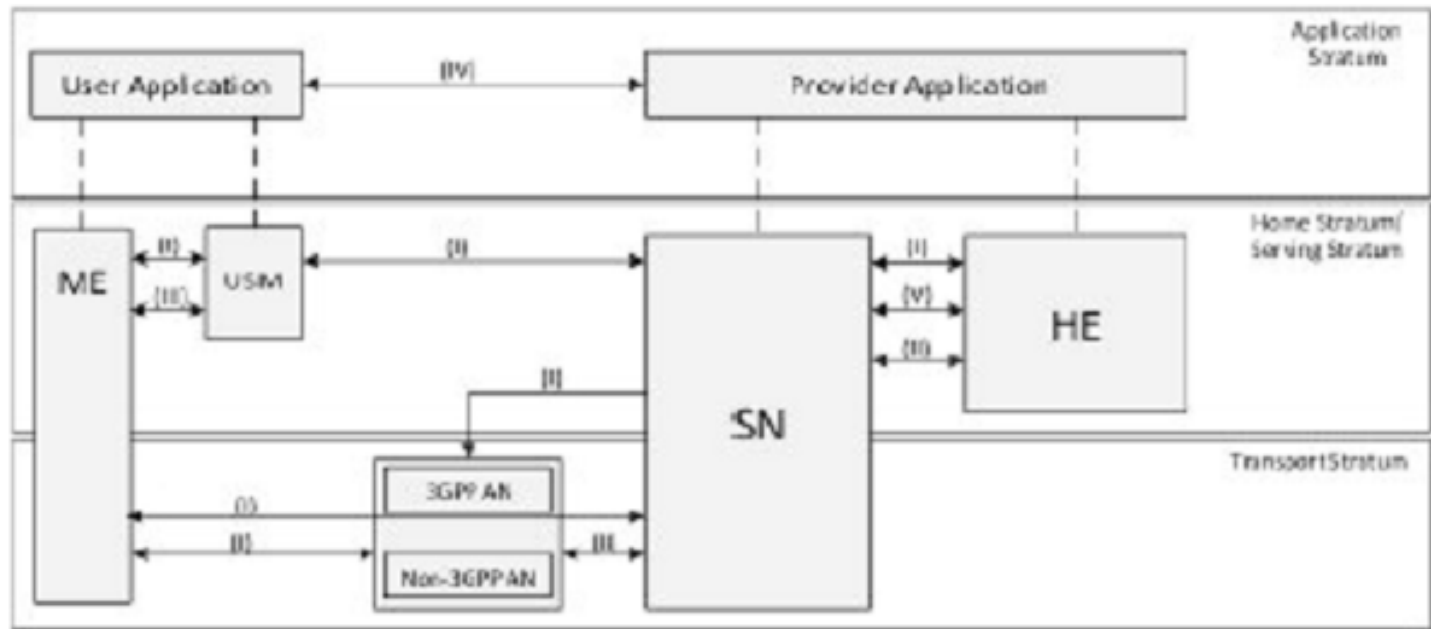
WPA3

The image features the text "WPA3" in a bold, white, sans-serif font. Each letter is decorated with red Wi-Fi symbols (three curved lines radiating from a central dot) placed at various points: top-left of 'W', top-center of 'P', top-right of 'A', and bottom-right of '3'. The background is black, with a large, thick red arc spanning the top and a solid red circle at the bottom center. Additional red Wi-Fi symbols are scattered around the letters, some overlapping the red arc.





3GPP 5G SECURITY ARCHITECTURE



The Evolution of Security in 5G- *5G Americas White Paper*

NEW 5G SECURITY SAFEGUARDS



ENCRYPTION



AUTHENTICATION



INTEGRITY



PRIVACY



AVAILABILITY

5G SECURITY ENHANCEMENTS



Unified authentication framework

that enables seamless mobility across different access technologies and support of concurrent connections



User privacy protection

for vulnerable information often used to identify and track subscribers (for example, SUPI, IMSI, and IMEI)



Secure Service-Based Architecture and slice isolation

optimizing security that prevents threats from spreading to other network slices



Native support for secure steering of roaming (SoR)

allowing operators to steer customers to preferred partner networks – improving the customer experience, reducing roaming charges, and preventing roaming fraud.



Improved SS7 and Diameter

protocols for roaming




Improved rogue base station detection and mitigation



Proprietary operator and vendor analytics

solutions offer even more layers of security



A photograph of two men in a server room. The man on the left is wearing a dark jacket and is looking down at a laptop. The man on the right is wearing a light-colored shirt and is also looking down at the laptop. The background shows server racks and a laptop keyboard.

Cisco on Cisco /

Fighting Malware to the End: How We Tested and Deployed AMP for Endpoints



Sensing/Actuation layer

Biological

Optical

Haptic

Acoustic

RFID

Infrared

Thermal

Communication layer

ZigBee

VAN

Bluetooth

NFC

WiMAX

BSN

4G, 5G

WAN

WLAN

Ethernet

Modbus

Profibus

CAN

Data Center, Cloud Computing

System application layer

Smart
Traffic Infrastructure

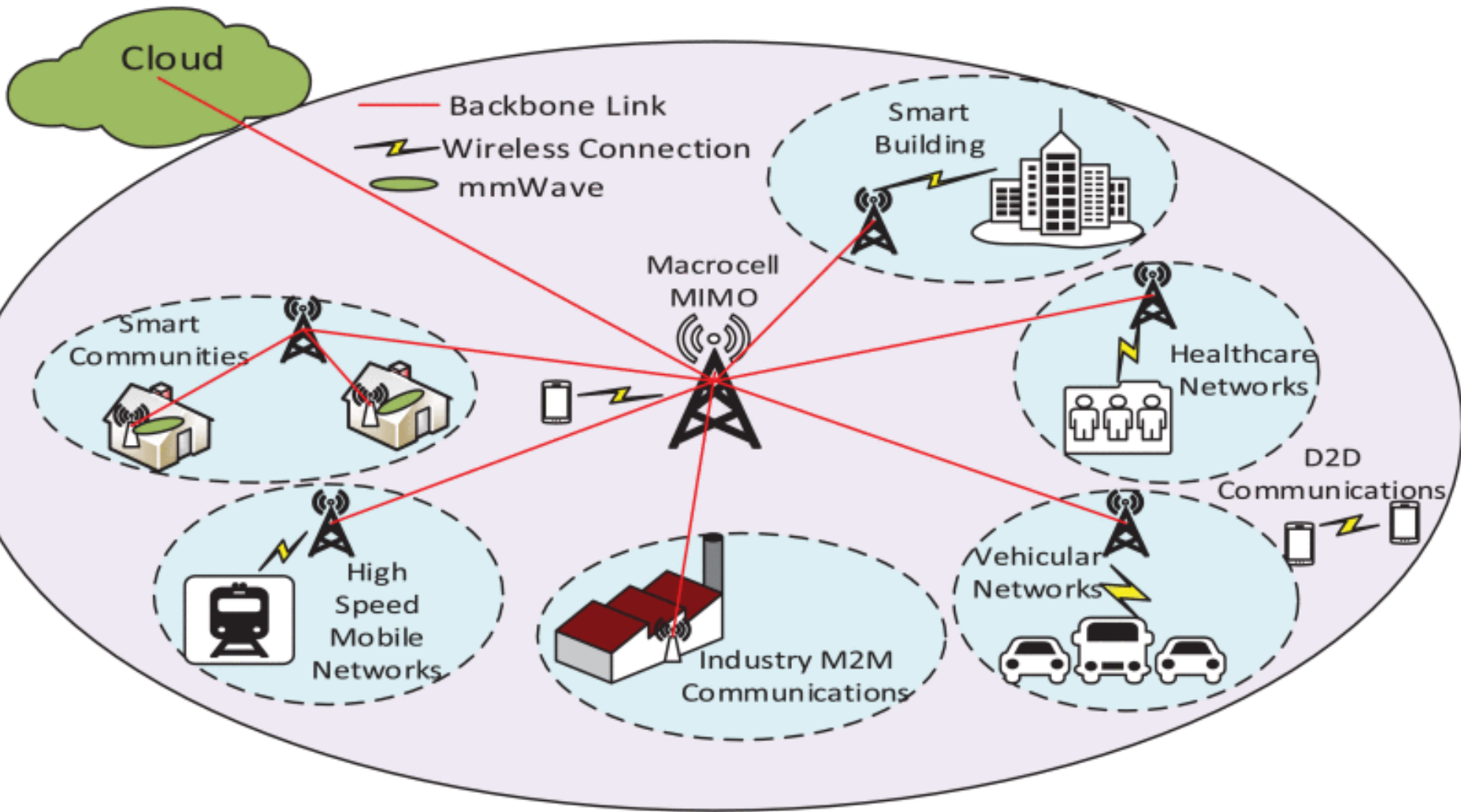
Personalized
Healthcare

Autonomous
Vehicle

Smart
Grid

Industrial
Control Systems

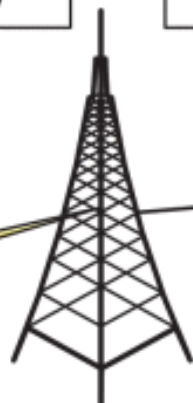
Smart
Manufacturing



Authentication/authorization; Key agreement

Security negotiation;
Key hierarchy;
Enhanced control plane;
Robustness;
Enhance subscriber privacy

NFV/SDN security;
Network slicing
security



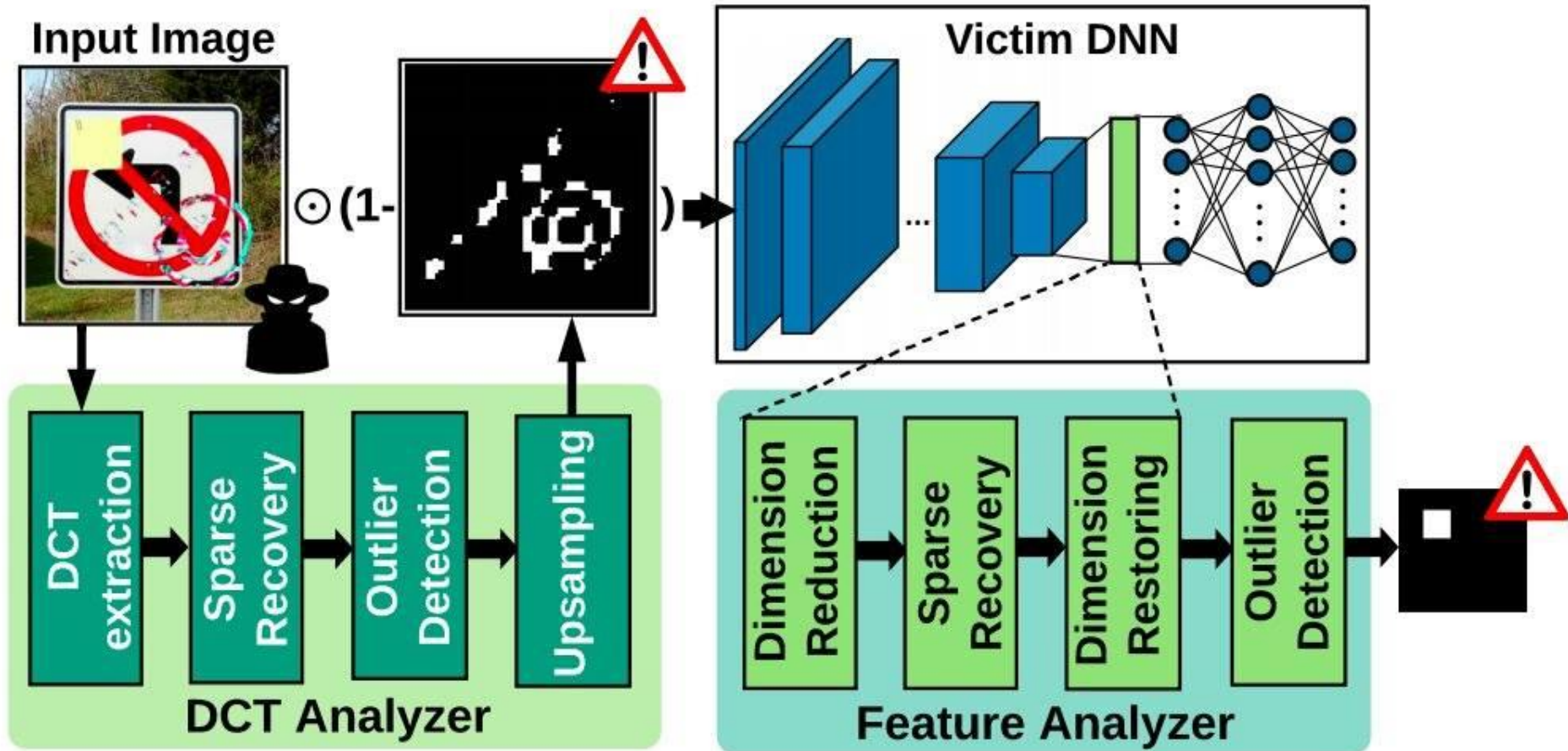
Edge Cloud

Central Cloud

Crypto algorithms;
Physical layer
security;
Jamming protection

Security management and
orchestration;
Security assurance for NFV
environments;
Self-adaptive, intelligent
security controls





Network security

Network security is defined as "the protection of a computer network and its services from unauthorised modification, destruction, or disclosure".

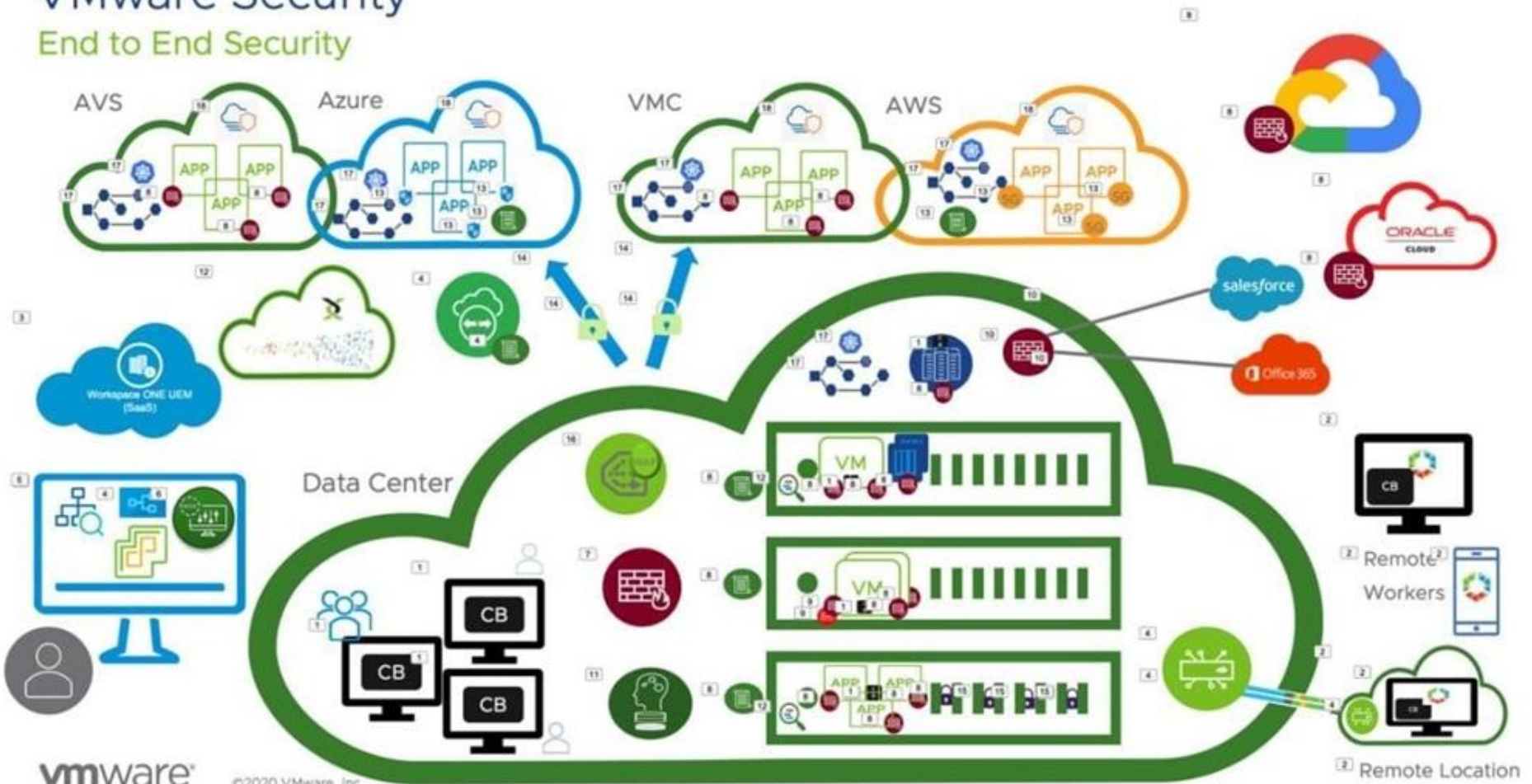
TACS

June 2014



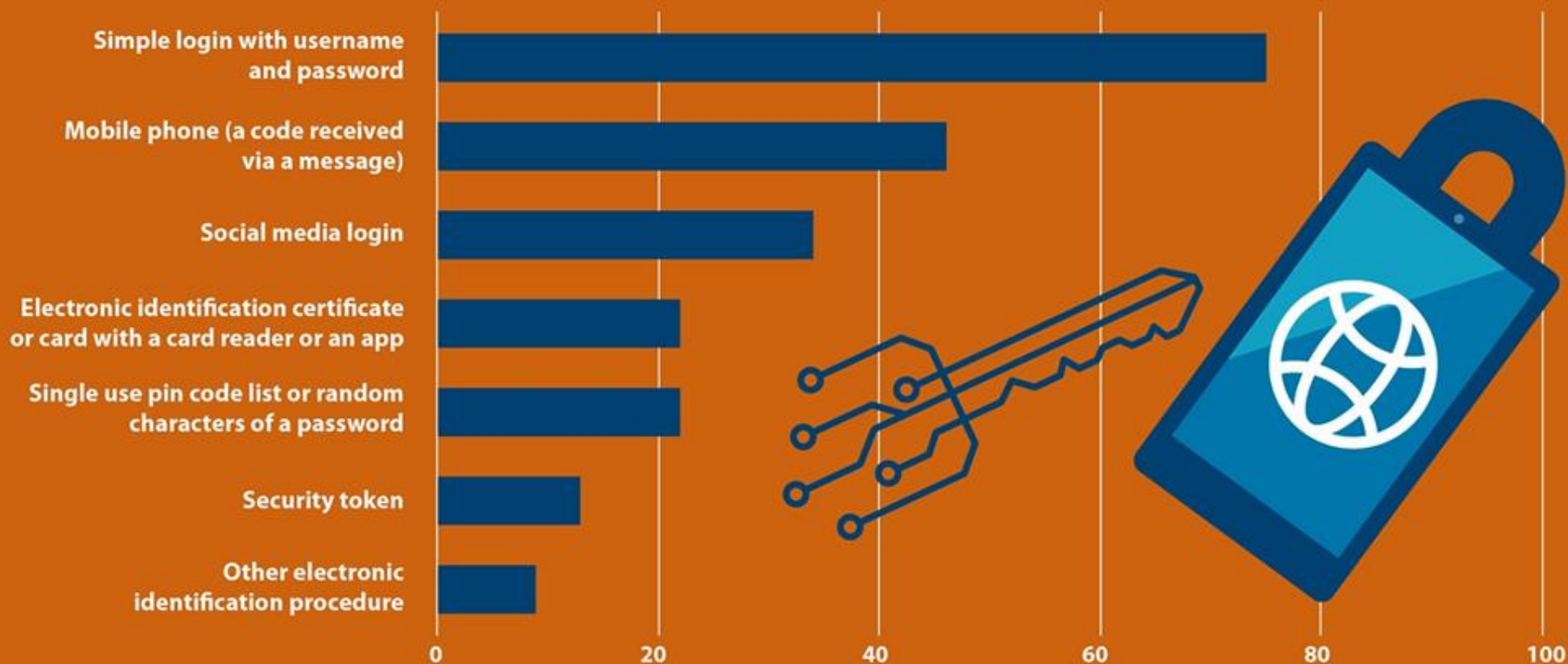
VMware Security

End to End Security



Identification procedures used for online services in the EU, 2020

(% of people aged 16-74, estimated)



People who used a mobile phone for receiving a code via a message to access online services, 2020

(% of people aged 16-74)

France, Italy: 2020 data not available.
EU value has been estimated.

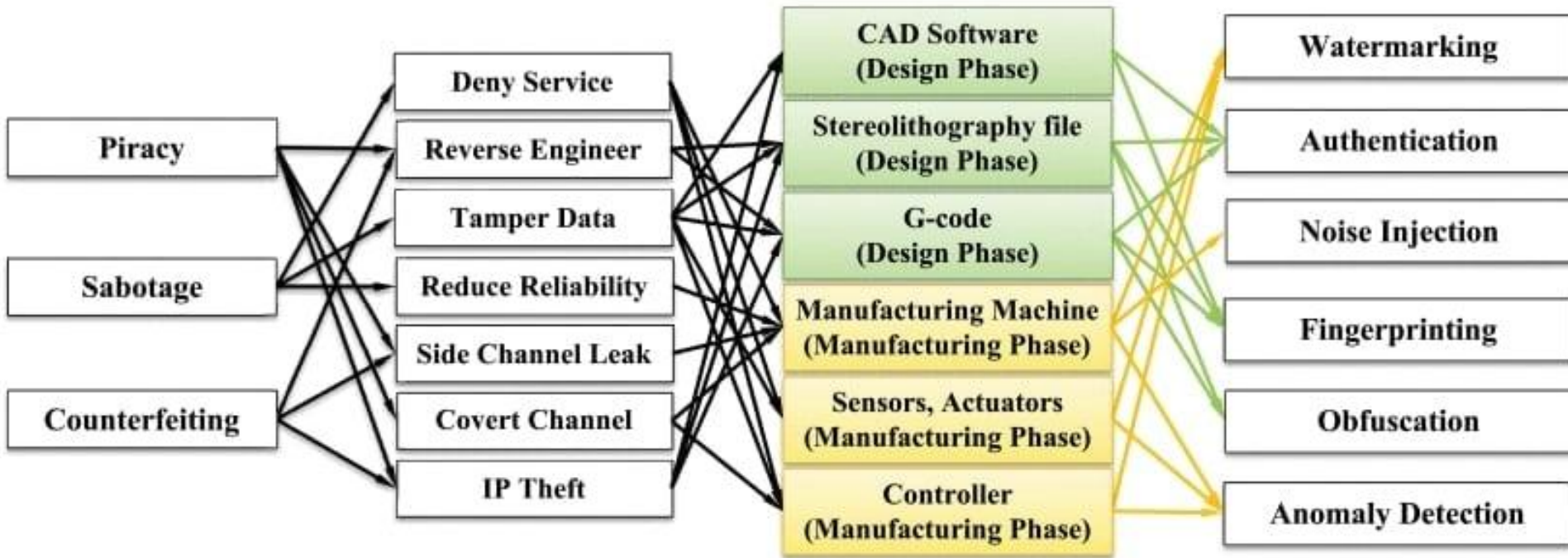


Attack Goals

Attack Methods

Attack Targets

Countermeasures



5 Cybersecurity Threats to Be Aware of in 2020