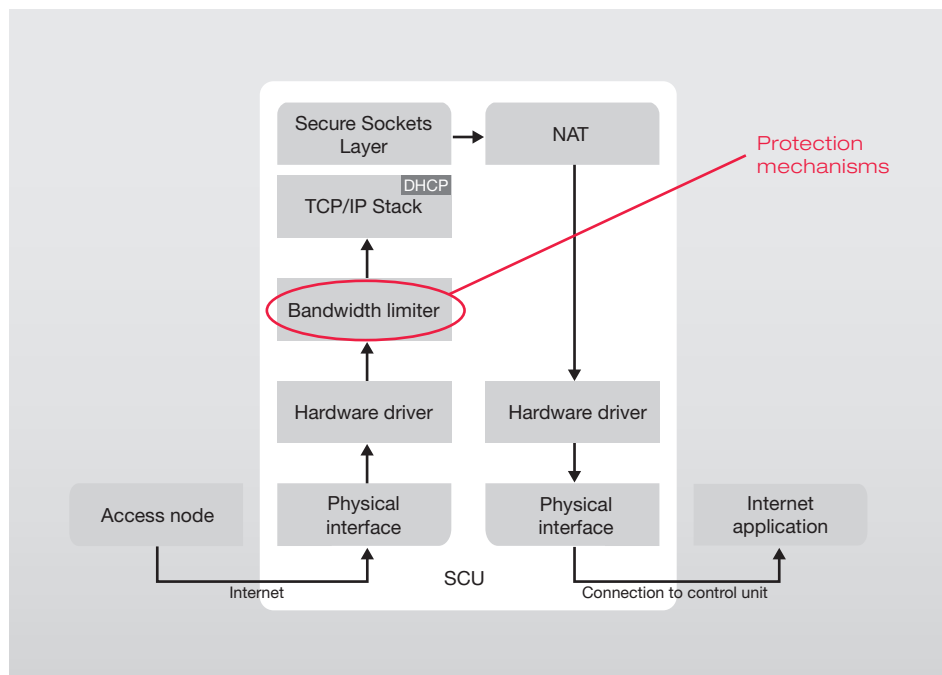


The Secure Communication Unit Provides Secure Online Access in Vehicles



Benefits:

- » **Reliable online access in the vehicle**
- » **Protection against flooding attacks**
- » **Protection against Bot-net**
- » **Increased availability of online applications**

Free Internet access in modern cars has now become a reality; and the future scope of this access will grow dramatically. As a result of this connectivity and the risk of untrustworthy software being downloaded, vehicle security requirements have increased. It is imperative that the vehicle's onboard network be protected against online attacks.

This is what motivated secunet to develop a process to effectively secure online interfaces in vehicles against web-based attacks.

Protection against attacks at network layer

The Secure Communication Unit (SCU) is a technique which ensures the availability of communication channels from and to the vehicle. In the event that the communication interface of the vehicle is attacked, the SCU ensures that the remaining vehicle applications can continue to run without being compromised. The SCU protects online access by monitoring the bandwidth of the Internet connection and the size of the transmitted IP packets. By doing so, flooding attacks are neutralised, bot-net attacks are blocked successfully.

Architecture of the Secure Communication Unit

The above-mentioned protection measures are located at the interface between the physical layer and the TCP/IP stack. Thus the protection measures are active at the lowest level and affect all higher-level software layers. All protocols required for IP operation (ARP, DHCP, TCP/IP and ICMP) are pooled in the TCP/IP stack block. The router provides the NAT (Network Address Translation) functionality.

Overview of Secure Communication Unit functions

Establishing an Internet connection

In order to establish communication to the Internet from the vehicle, a dynamic IP address is obtained by the access node. This is done automatically via the Dynamic Host Configuration Protocol (DHCP). The assigned dynamic IP address is then mapped to an internal static IP address via NAT. The Internet application is accessed via this static IP address.

Protection against flooding attacks (Bandwidth Limitation)

The bandwidth is limited by peak (number per second) and average number of IP packets per time window to protect against flooding attacks. The time window can be variably defined. This so-called bandwidth limiter works at IP level, without specific consideration of the protocols ICMP, ARP, DHCP, IP HTTPS, IP HTTP, etc., in order to enable simple and sustainable implementation of the SCU in the hardware. As soon as the bandwidth exceeds a certain threshold, the SCU terminates the logical IP connection. The downstream Internet application remains unaffected and cannot be caused to crash. Subsequently, the Internet connection is re-established with a new IP address (auto reload). As a result of the new

IP address, the SCU and the vehicle are no longer visible to the attacker. Bandwidth limitation also ensures that the SCU always has enough processing power to carry out the auto reload.

Configuration of the SCU (Diagnosis)

The SCU is currently configured using SNMP (Simple Network Management Protocol) commands. The following commands are available:

- Set and read the threshold value for the bandwidth limiter
- Set and read the static IP address in connection with NAT
- Get the current bandwidth usage
- Get status information whether an auto reload has occurred

Availability of SCU functions

The SCU functions are implemented in software. A Freescale MPC5200 embedded processor running Linux serves as the base platform. WLAN is used as an access node, which is connected to the processor board via USB. The Internet application is connected to the SCU via Ethernet.

Why secunet?

secunet offers OEMs and suppliers a critical competitive advantage in the form of time to market for the launch of online platforms: OEMs and suppliers concentrate on developing their platform's customer functions; we deliver the necessary security mechanisms. This means lower costs and faster launches.

Our experts in the business unit Automotive Security combine many years of project experience in the automotive world with valuable expertise in extratraditional IT and telecommunications.

For the development of adapted security mechanisms for the protection of online platforms, we have achieved excellence in the following projects:

- Introduction of secure payment transactions via mobile end devices in the telecommunications sector
- Introduction of protection mechanisms for remote maintenance access in the automotive sector
- Analysis of browser security in head units and of the security modules for a toll system's onboard units
- Network security for the implementation of multi-level firewall concepts and the operation of managed security services

Animation and Whitepaper:
www.secunet.com/en/onlinesecurity