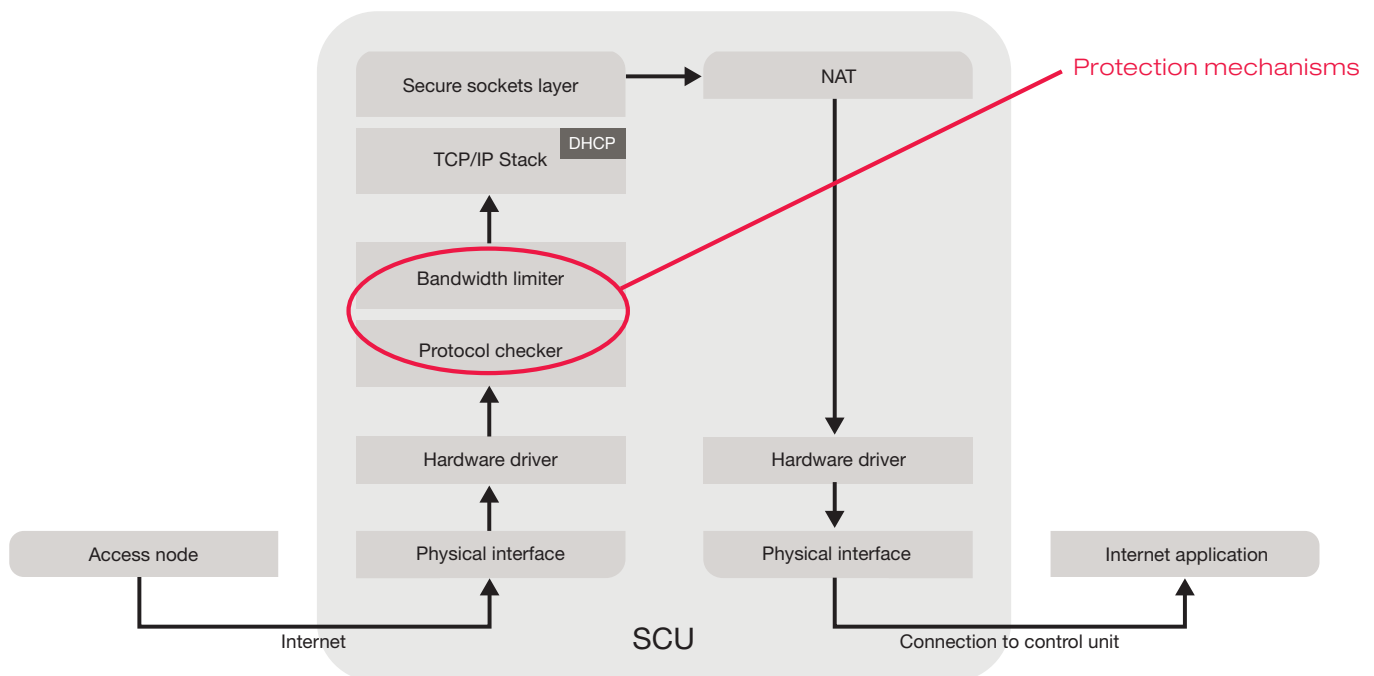


# secunet

## Embedded Security

### Secure Online-Access in Vehicles via a Secure Communication Unit (SCU)



Internet access has nowadays become a reality in modern cars. On this account vehicle security requirements to protect against online attacks are growing. This was secunet's motivation to develop an architecture which effectively secures online interfaces in vehicles against major types of web-based attacks.

#### Protection against attacks at network layer

The Secure Communication Unit (SCU) is a technique which ensures the availability of incoming and outgoing communication channels. 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. Monitoring the bandwidth protects against denial-of-service attacks; checking the IP packet size prevents buffer overflow attacks at protocol level. This provides a successful protection against Internet attacks.

#### Your advantages:

- Reliable online-access in vehicles
- Protection against DoS attacks
- Protection against buffer overflow attacks

### 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 denial-of-service attacks

In order to protect against denial-of-service attacks, the bandwidth is limited by peak (number per second) and average number of IP packets per time window. 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.

Protection against buffer overflow attacks at IP level

If the size of an IP packet does not match the information in the IP header, the buffers for the intermediate storage of the content of an IP packet may overflow. Malicious program code can be executed this way. The protocol check compares the size specifications in the IP header against the size of the respective IP packet. If the sizes are different, the Internet connection is auto reloaded. This ensures that only correctly formed IP packets are forwarded to the higher-level protocol layers. The risk of exploiting implementation errors in the TCP/IP stack is therefore reduced.

Configuration of the SCU

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 currently 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. The next step is to implement the SCU functionality in programmable hardware. Since hardware is resistant to software attacks, this solution allows fully protected online access in the vehicle.

### secunet Security Networks AG

IT security and its trend-setting usage is the core competence of secunet Security Networks AG. The development and implementation of IT security solutions for sensitive data turn secunet into a specialist in great demand. Excellent technological understanding is reflected in our consulting services and modulated products. Progressive digitalization of processes and communication channels of all kind pose new challenges for secunet day-to-day. Due to our large know-how we set standards in the IT security market. Our extensive clientele comprises national and international companies and affiliated groups as well as the public sector. About 250 highly qualified and experienced employees at seven branch offices in Germany as well as at further offices in subsidiaries in Switzerland and the Czech Republic are engaged in the creation of innovations, the optimal settlement of projects and our twenty-four-seven support.

Editor:

**secunet**

secunet Security Networks AG  
Kronprinzenstraße 30  
45128 Essen, Germany  
Phone: +49 - 201 - 54 54 - 0  
Fax: +49 - 201 - 54 54 - 123  
E-mail: [info@secunet.com](mailto:info@secunet.com)  
[www.secunet.com](http://www.secunet.com)