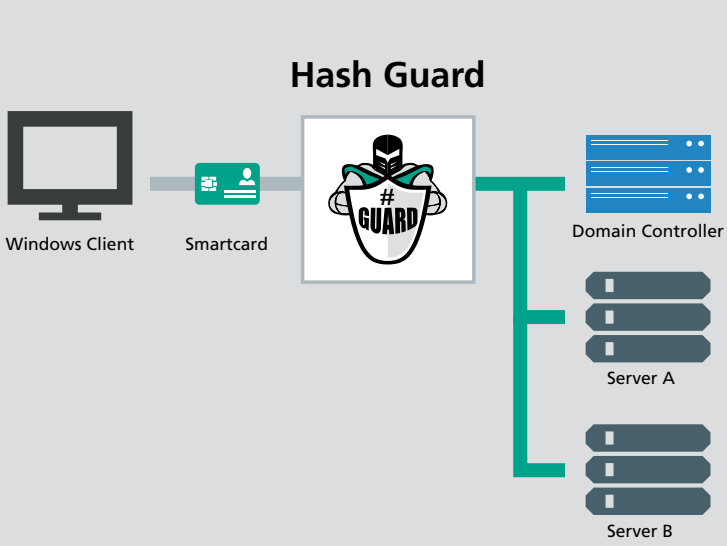
Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY




*Fraunhofer Institute For Secure Information Technology SIT*

*Contact:*
*Dr. Frank Weber*
*Rheinstrasse 75*
*64295 Darmstadt*
*Germany*

*Phone +49 6151 869-176*
*Fax +49 6151 869-224*
*frank.weber@sit.fraunhofer.de*
*www.sit.fraunhofer.de*

# HASH GUARD

## NEXT LEVEL PROTECTION AGAINST ADVANCED PERSISTENT THREATS

Pass the hash is one of the most dangerous network security vulnerabilities. Hackers use this technique to circumvent server authentication and gain access to secret information and sensitive applications. The Fraunhofer Institute for Secure Information Technology SIT and Arkoon Netasq, a subsidiary of Airbus Defence and Space, have jointly developed Hash Guard, a solution for protecting enterprises against widespread pass-the-hash attacks. Hash Guard is ready for the market and can be integrated into existing network security solutions.

### Challenge

Every time a user logs in to a Windows domain network, the domain controller uses the password to generate a number of security tokens a.k.a. hashes. These are used to connect the user's computer with the different servers and applications inside the company network. Due to its design, Windows single sign-on authentication is lacking a mechanism to ensure that a hash is only used by the rightful owner. Consequently, attackers can steal hashes and use them to access sensitive parts of the enterprise's IT infrastructure, steal valuable information or take control over the network.

### Solution

Hash Guard provides the missing safeguarding mechanism: similar to a firewall it is situated in front of the enterprise's servers and monitors the network traffic for authentication messages, verifies whether a hash is used by its rightful owner and if not it automatically terminates the connection. The solution supports smartcard authentication, where the user only has to enter the PIN when logging in to the computer. From there on Hash Guard regularly checks incoming connections to the servers. For each authentication request to a server Hash Guard will assure the legitimacy of the connection by verifying the presence of the user's smartcard at the requesting computer.

Hash Guard protects protocols that employ the LAN Manager (LM) or NT LAN Manager (NTLM) as well as Kerberos authentication including Server Message Block (SMB), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP) and more. Modifying these protocols is not necessary.

### Partner

Arkoon and Netasq, fully owned subsidiaries of Airbus Defence and Space, run the Stormshield brand and offer innovative end-to-end security solutions worldwide to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security). Arkoon Netasq implements Hash Guard in Stormshield products.

### Benefits

- Effective protection against one of the most dangerous and common sort of targeted attacks on windows domain networks
- Easy to integrate into enterprise networks
- Ease of use/single sign-on
- Standard conform smartcard protocols (ISO/IEC 7816)