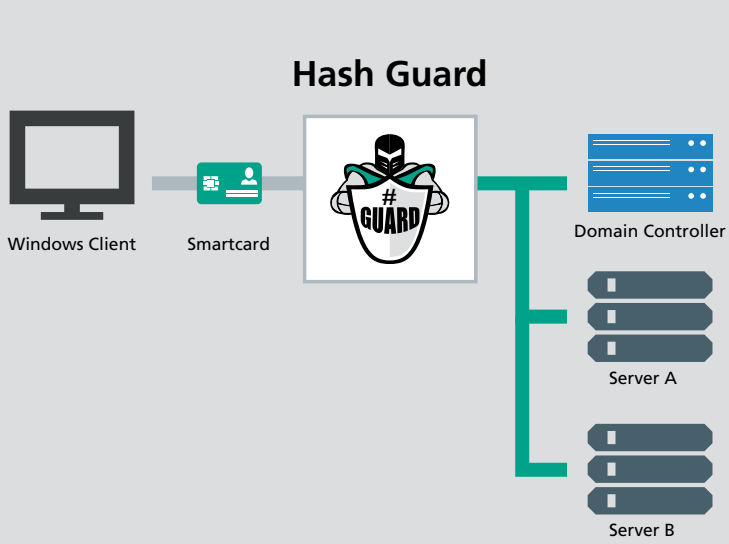
Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE



Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Dr. Frank Weber
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-176
Fax 06151 869-224
frank.weber@sit.fraunhofer.de
www.sit.fraunhofer.de

HASH GUARD

BESSERER SCHUTZ VOR ADVANCED PERSISTENT THREATS

Pass-the-hash ist eine der gefährlichsten Sicherheitslücken in Unternehmensnetzen. Angreifer nutzen diese Technik, um die Server-Authentifizierung zu umgehen und in den Besitz von geheimen Informationen zu kommen. Fraunhofer SIT und Arkoon Netasq, eine Tochtergesellschaft der Airbus Defence and Space, haben mit Hash Guard eine Lösung entwickelt, die Unternehmen vor den Folgen weit verbreiteter Pass-the-Hash-Angriffe schützt. Hash Guard steht vor der Marktreife und kann in bestehende Netzwerksicherheitslösungen integriert werden.

Herausforderung

Jedes Mal, wenn sich ein Benutzer an einem Windows-Netzwerk anmeldet, wird sein Passwort genutzt, um daraus eine Reihe von Sicherheitstokens, also Hashes, zu erzeugen. Die Hashes werden verwendet, um den Computer des Nutzers mit verschiedenen Servern und Anwendungen innerhalb des Firmennetzwerks zu verbinden. Dieser Windows-single sign on-Authentifizierung fehlt ein Mechanismus, der sicherstellt, dass ein Hash nur von seinem rechtmäßigen Besitzer genutzt wird. Folglich können Angreifer Hashes stehlen und sie nutzen, um Zugang zu sensiblen Bereichen der Unternehmens-IT-Infrastruktur zu bekommen, um etwa Kontrolle über das Netzwerk zu erlangen (lateral movement). Auch das Abschirmen von Hashes gegen unberechtigten Zugriff bietet keinen Schutz, da durch das Vortäuschen einer legitimen Verwendung selbst ein derart geschützter Hash missbraucht werden kann.

Lösung

Hash Guard liefert diesen fehlenden Schutzmechanismus: Ähnlich wie eine Firewall ist es vor dem Unternehmens-Server gelagert und überwacht dort Authentifizierungs-Nachrichten im Netzwerkverkehr. Hash Guard überprüft, ob ein Hash vom rechtmäßigen Eigentümer und nur für den vorgesehenen Zweck verwendet wird – wenn nicht, wird die Verbindung sofort automatisch gekappt. Die Lösung unterstützt Authentifizierung über Smartcards, wobei Nutzer lediglich beim Einloggen ihre PIN eingeben müssen. Von da an prüft Hash Guard regelmäßig alle eingehenden Verbindungsanfragen zu den Servern. Für jede Authentifizierungsanfrage an einen Server gewährleistet Hash Guard die Legitimität der Verbindung, indem er prüft, ob die Smartcard des Nutzers an dem Computer eingesteckt ist, der die Anfrage sendet. Hash Guard schützt Protokolle, die bei LAN Manager- (LM) oder NT LAN Manager-(NTLM) sowie Kerberos-Authentifizierungen zum Einsatz kommen, einschließlich des Server Message Blocks, (SMB), Internet Message Acces Protocol (IMAP), Simple Mail Transfer Protocol (SMTP) und mehr. Eine Anpassung dieser Protokolle ist nicht erforderlich.

Partner

Arkoon und Netasq sind hundertprozentige Tochtergesellschaften von Airbus Defence and Space. Sie führen die Marke Stormshield und verkaufen weltweit innovative Ende-zu-Ende-Sicherheitslösungen. Arkoon Netasq implementiert Hash Guard in Stormshield-Produkte.

Nutzwert

- Wirksamer Schutz für Windows-Domänen
- Einfache Integration
- Hohe Benutzerfreundlichkeit/single sign on
- Standardkonforme Smartcard-Protokolle (ISO/IEC 7816)