DIGITTRADE 2-Stufen-Authentifizierung

17.09.2009, 12:21 | IT, New Media & Software

Pressemitteilung von: *DIGITTRADE GmbH*
Presseagentur: *Borgmeier Public Relations*

Doppelter Schutz mittels Smartcard und PIN-Eingabe in externen Speichermedien mit hardwarebasierter Verschlüsselung

Einige externe Speichermedien verfügen über Schutzmechanismen, die unbefugte Zugriffe auf Daten verhindern. Die Qualität der Datensicherheit eines externen Speichermediums wird durch drei wichtige Faktoren bestimmt: die Verschlüsselungsmethode der Daten, der Schutz des Sicherheitsschlüssels sowie die Authentifizierungsmethode. Eine hohe Sicherheit kann nur dann erreicht werden, wenn jeder dieser drei Faktoren entsprechende Anforderungen erfüllt.

Eine gute Authentifizierungsmethode ist nur dann ohne eine entsprechende Datenverschlüsselung wirksam, so lange sich der Datenträger in dem dafür vorgesehenen Gehäuse befindet. Nach dem Entfernen des Speichermediums aus dem Sicherheitsgehäuse besteht die Möglichkeit, auf die Daten zuzugreifen, wenn diese auf dem Speicherträger nicht ausreichend verschlüsselt sind. Demgegenüber kann auch die beste Verschlüsselung die relevanten Informationen nicht vor unbefugten Zugriffen schützen, wenn die Authentifizierungsmethode Sicherheitslücken aufweist. Das sicherste Verfahren zur Überprüfung der Authentizität und die sicherste Verschlüsselungsmethode können umgangen werden, wenn der Sicherheitsschlüssel nicht ausreichend geschützt ist.

Derzeitige Speichermedien mit hochgradiger hardwarebasierter Verschlüsselung, wie zum Beispiel nach AES 128 oder 256 Bit, verfügen über einstufige Authentifizierungsmechanismen wie etwa Fingerprint, Token oder PIN-Code. Für die Authentifizierung benötigt der Anwender dabei nur einen Faktor. Der Sicherheitsschlüssel des Kryptosystems wird auf dem Speichermedium oder im Sicherheitsgehäuse abgelegt.
Mit dieser Problemstellung beschäftigte sich auch die DIGITTRADE GmbH. Seit 2005 arbeitet sie an der Entwicklung und Produktion moderner elektronischer Artikel. Einen besonderen Teil des Angebots machen mobile verschlüsselte Speicher wie USB-Security-Sticks, RFID-Security- und High-Security-Festplatten sowie TV und DVB-T-Medien aus. Mit Entwicklung der High-Security-Festplatten entstand auch das Konzept der zum Patent angemeldeten 2-Stufen-Authentifizierung.

Aktuelle Lösungen mit einstufigen Authentifizierungsmechanismen weisen zwei wesentliche Probleme auf:
Einerseits kann der Sicherheitsschlüssel durch verschiedene Methoden ausgelesen werden, da dieser auf dem Speichermedium oder im Sicherheitsgehäuse gespeichert wird. Der Zugriff auf den Speicherort des Schlüssels kann in diesem Fall niemals ausreichend gesichert werden. Zur Erhöhung der Datensicherheit ist es wichtig, den Zugriff auf den Sicherheitsschlüssel bedeutend zu erschweren oder bestenfalls komplett zu verhindern.

Andererseits werden bei aktuellen Lösungen in der Regel alle zur Nutzung des Speichermediums notwendigen Komponenten zusammen aufbewahrt, wie beispielsweise Sicherheitsgehäuse und Token. Dies ist erforderlich, da für die Nutzung des Speichermediums zwangsläufig beide Komponenten notwendig sind. Es genügt, in den Besitz dieser Komponenten zu gelangen, um den Zugriff auf die Daten ohne Weiteres freizuschalten. Zur Erhöhung der Sicherheit ist es wichtig, einen zusätzlichen Authentifizierungsfaktor nicht materieller Art zu verwenden.

Diese beiden Probleme werden durch die Implementierung der „2-Stufen-Authentifizierung“ mittels Smartcard und PIN-Eingabe in externen Speichermedien mit hardwarebasierten Verschlüsselungsmechanismen gelöst. Der Vorgang ist nach dem Prinzip „Besitzen und Wissen“ konzipiert und sorgt dafür, dass der Sicherheitsschlüssel sicher gespeichert wird und dessen Verwendung einer Genehmigung bedarf.
In der ersten Stufe des Authentifizierungsvorgangs („Besitzen“) prüft das System, ob der Nutzer eine gültige Smartcard besitzt, und in der zweiten Stufe („Wissen“), ob der Nutzer die passende PIN kennt und somit berechtigt ist, die Smartcard zu benutzen.

Der für den Zugriff auf das externe Speichermedium notwendige Sicherheitsschlüssel wird auf einer Smartcard, getrennt vom Sicherheitsgehäuse und dem Speichermedium, abgelegt. Die Auslagerung des Speicherortes des Sicherheitsschlüssels auf die Smartcard verhindert das Auslesen des Schlüssels, falls ein Unbefugter in Besitz des Speichermediums mit Sicherheitsgehäuse gelangt. Es besteht somit auch keine Angriffsfläche für etwa Brute-Force-, Cold-Boot- und USB-Sniffer-Attacken sowie für andere Methoden, durch welche der Sicherheitsschlüssel ausgelesen werden könnte.
Der Schlüssel wird erst in der ersten Authentifizierungsstufe durch das Einlegen der Smartcard in das Gehäuse physisch mit dem Speichermedium verbunden. Dabei überprüft das System, ob eine gültige Smartcard eingesetzt wurde.

Durch die Eingabe einer PIN erfolgt in der zweiten Stufe des Authentifizierungsprozesses die Freigabe zur Übertragung des Sicherheitsschlüssels von der Smartcard an das Sicherheitsgehäuse, in welchem sich das Speichermedium befindet. Die Ver- und Entschlüsselung der Daten erfolgt mithilfe des übertragenen Sicherheitsschlüssels. Auf diese Weise wird bestätigt, dass der Besitzer der Smartcard auch die Berechtigung für deren Nutzung hat und somit auf das Speichermedium zugreifen darf.
Die „2-Stufen-Authentifizierung“ mittels Smartcard und PIN-Eingabe in externen Speichermedien mit hardwarebasierter Verschlüsselung verfügt außerdem über einen Schutzmechanismus, welcher unberechtigten Zugriff auf die Smartcard und den Sicherheitsschlüssel verhindert. Dieser Schutzmechanismus sperrt die Smartcard unwiderruflich und vernichtet den auf ihr gespeicherten Sicherheitsschlüssel, sobald eine bestimmte Anzahl an Fehlversuchen bei der PIN-Eingabe erreicht ist.

Die Notwendigkeit einer PIN-Eingabe unterbindet die Verwendung von Brute-Force-, Cold-Boot-, USB-Sniffer-Attacken und anderen Methoden zum Auslesen des Sicherheitsschlüssels. Durch die begrenzte Anzahl an Fehlversuchen bei der PIN-Eingabe wird der Einsatz von Backtracking-Methoden zum Auslesen des Sicherheitsschlüssels wirksam verhindert. Der Zugriff auf die Smartcard und somit den Sicherheitsschlüssel, ohne die korrekte PIN zu kennen, ist dadurch nicht möglich.

Die „2-Stufen-Authentifizierung“ mittels Smartcard und PIN-Eingabe in externen Speichermedien bietet durch entsprechende Authentifizierungsmethoden für Speichermedien mit hochgradiger hardwarebasierter Verschlüsselung, wie zum Beispiel nach AES 128 oder 256 Bit, den derzeit höchsten Standard für Datensicherheit. Daher sind hochverschlüsselte externe Speichermedien mit Sicherheitsgehäusen, die diese Authentifizierungsmethode verwenden, für die Speicherung hochsensibler Daten besonders geeignet.

DIGITTRADE realisierte dieses Prinzip in der externen High-Security-Festplatte HS128. Mit 2-Stufen-

Authentifizierung und Fulldisk 128-Bit-Verschlüsselung nach AES gehört diese Festplatte in die erste Reihe mobiler Speichermedien.

Portrait

Seit 2005 arbeitet DIGITTRADE GmbH mit Sitz in Holleben/Teutschenthal an Entwicklung und Produktion moderner elektronischer Artikel. Grundgedanke ist die Herstellung von Computer- und Home-Entertainment-Produkten, die den Anforderungen und Bedürfnissen deutscher und europäischer Kunden entsprechen. Dabei versorgt DIGITTRADE mit einfach zu bedienenden Lösungen alle Kunden und Betriebssysteme. Flexibel programmieren Mitarbeiter tagesaktuell Softwareupdates, testen und optimieren kontinuierlich das Sortiment. Einen besonderen Teil des Angebots machen mobile verschlüsselte Speicher sowie TV und DVB-T-Medien aus. Enge Beziehungen verbindet DIGITTRADE mit dem Grafikkartenhersteller AXLE 3D. Gemeinsam entwickelten sie i-DSS, ein Programm, das ermöglicht, nVidia Grafikprozessoren bei Bedarf automatisch und kontrolliert bis zu 50 Prozent zu übertakten. Seit Herbst 2008 finden Käufer auch Notebook-Taschen der Marke Hugger, die als Tragetasche, Umhängetasche und Rucksack verwendbar sind, im eigenen Shop unter digittrade.de. Ergänzt wird das Portfolio durch „Juzt-Reboot“ PCI-Recovery-Karten. Sie bieten optimalen Schutz und Sicherheit im Umgang mit PCs und sorgen als reine Hardwarelösung für Datensicherung und Systemwiederherstellung.

News-ID: 350835 • Views: 893 (Stand: 06.05.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/350835/DIGITTRADE-2-Stufen-Authentifizierung.html