HOB GmbH & Co. KG
Schwadermühlstr. 3
90556 Cadolzburg

Tel: 09103 / 715-0
Fax: 09103 / 715-271
E-Mail: support@hob.de
Internet: www.hob.de

WhitePaper

HOBCOM und HOBLink J-Term/Terminal Edition

Single Sign-On mit Kerberos und RACF-PassTicket am 3270-Mainframe

April 2010

Technology
Future
Communication

In unserer heutigen IT-Welt benutzen Anwender täglich eine Vielzahl von unterschiedlichen Systemen. Für den Zugang zu Windows Remote Desktop Services, das Abrufen von E-Mails oder das Arbeiten mit Webanwendungen ist fast immer eine gesonderte Anmeldung zum Nachweis der Identität notwendig. Aus Sicht der Benutzer eine mehr als unbefriedigende Tatsache, die nicht nur die Produktivität senkt, sondern auch Schwachstellen bei der Sicherheit erzeugt. Ein Anwender, der zehn oder mehr Passwörter parat haben muss, wird dazu neigen, sich diese auf kleinen gelben Zetteln am Monitor zu notieren und entsprechend einfache Benutzerkennungen auszuwählen. Hier ist es für die IT-Verantwortlichen natürlich sehr schwer, das Einhalten von bestimmten Mindeststandards durchzusetzen. Durch den erhöhten administrativen Aufwand entstehen aber auch zusätzliche (vermeidbare!) Kosten.

Die typische IT-Systemlandschaft ist historisch gewachsen und daher in hohem Maße heterogen. Im Rechenzentrum steht der Mainframe neben dem Server mit Windows Remote Desktop Services, ein Telnet-Server empfängt noch Passworte im Klartext, während die Webanwendung SSL-verschlüsselt überträgt. Gerade die Vielfalt der Datenformate und die mangelnde Interoperabilität zwischen den kommunizierenden Komponenten sind mitverantwortlich für die oben beschriebene Situation einer uneinheitlichen Authentifizierung. Darüber hinaus muss in den meisten Client-Server-Umgebungen nur der Anwender, nicht aber der Server oder Dienst seine Identität beweisen. Gerade bei Webanwendungen, die mit gefälschten 'Phishing'-Adressen versuchen an Benutzerpasswörtern zu gelangen, ein nicht zu unterschätzendes Sicherheitsrisiko.

Hier stehen die IT-Verantwortlichen vor der schwierigen Aufgabe, einerseits die Ergonomie für den Benutzer durch den Einsatz von 'Single Sign-On'-Systemen zu steigern, aber auch anderseits die Sicherheit im Datenverkehr mit einheitlichen kryptografischen Standards zu erhöhen. Übersetzt man 'Single Sign-On' mit Einmalanmeldung, so bedeutet das für den Anwender einen einmaligen Nachweis seiner Identität z.B. durch Kennwort-Eingabe oder über Zertifikate (Smartcards, Token), um Zugriff auf alle Anwendungen und Dienste, für die er berechtigt ist, zu erhalten. Diese nachfolgenden Zugriffe werden über das 'Single Sign-On'-System automatisch authentifiziert.

Die Vorteile eines solchen Systems lassen sich einfach nachvollziehen:

- Die Forderung nach längeren und sicheren Passwörtern lässt sich leichter gegenüber den Benutzern durchsetzen, da diese alle anderen ersetzen.
- Der 'Single Sign-On'-Mechanismus sorgt für einen einheitlichen Standard bei der Authentifizierung und bringt somit auch hier einen wichtigen Beitrag zu höherer Sicherheit.
- Steigerung der Produktivität durch die einmalige Kennwort-Eingabe.
- Für jeden Anwender existiert nur noch ein Benutzerkonto. Aus Sicht der IT-Administration ein Sicherheitsgewinn, da jede Änderung nun zentral erfolgt. Ein Löschen dieses Kontos z.B. beim Ausscheiden des Mitarbeiters hat auch ein sofortiges Erlöschen aller seiner Berechtigungen zu Folge.

Aber ist es nicht ein Nachteil, dass bei Verlust der Identität eines Anwenders dem missbräuchlichen Benutzer damit alle Anwendungen und Dienste, auf die der Anwender Zugriff hat, zur Verfügung stehen? Ohne 'Single Sign-On' benutzen die meisten Anwender ohnehin das selbe Passwort für ihre Anwendungen und Dienste, so dass das Schadenspotential kaum höher liegt. Im Verlustfall lässt sich ein 'Single Sign-On'-Konto schnell sperren. Eine gute Firmen-'Policy' sieht den regelmäßigen Wechsel der Passwörter vor.

Ein vielversprechender Ansatz, diese Ziele zu erreichen, findet sich in dem Konzept von Kerberos, das bereits vor über 20 Jahren am Massachusetts Institute of Technology (MIT) entwickelt wurde. Kerberos vereinigt das Konzept eines einheitlichen kryptografischen Standards (z.B. AES) bei der Übertragung von Daten mit einem standardisierten Authentifizierungsmechanismus, nicht nur zur Authentifizierung am System sondern auch an Diensten. Microsoft erkannte zu Recht das Potential dieses Protokolls als ein echtes 'Single Sign-On'-Systems, ohne Übertragung der Passwörter oder ihrer Speicherung auf den Endgeräten. Seit dem Release von Windows 2000 ist Kerberos ein fester Bestandteil der MS Active Directory Server und weiterer Produkte von Microsoft.

Die Firma HOB GmbH & Co. KG hat ihre Produktpalette um die Kerberos-Funktionalität erweitert, um den IT-Verantwortlichen, aber auch den Anwendern Produkte an die Hand zu geben, die den Umstieg zu mehr Sicherheit und Komfort erst ermöglichen. Speziell der IBM-Mainframe, der in vielen Firmen immer noch eine unverzichtbare Säule der IT-Struktur ist, steht mit seinen 3270-Anwendungen (CICS, TSO, usw.) in einer Kerberos-Umgebung nicht länger abseits, sondern wird nun als vollwertiges Mitglied integriert.

Im Gegensatz zu anderen 'Single Sign-On'-Konzepten, die z.B. Passwörter lokal speichern und bei Bedarf die Benutzereingabe ersetzen, arbeitet Kerberos mit so genannten Tickets, die Zugriffe erlauben. Es wird zwischen dem TGT (Ticket Granting Ticket), das bei der ersten Authentifizierung gegenüber Kerberos ausgestellt wird, und den Service-Tickets für den Zugriff auf Dienste und Anwendungen unterschieden. Da die Protokolle für die Anforderung von Tickets und die Struktur der Tickets standardisiert sind, können die Tickets auch plattformübergreifend angefordert und ausgetauscht werden. Diese Interoperabilität in heterogenen Netzwerken (z.B. Windows / Unix) ist ein wichtiger Vorteil auf dem Weg zu einer einheitlichen Verwaltung aller Strukturen. Kerberos trifft aber noch eine weitere entscheidende Annahme: Endgeräte, aber auch Dienste sind als potentiell unsicher anzusehen und müssen sich sowohl gegenüber einer vertrauenswürdigen Instanz, dem Key Distribution Center (KDC), als auch gegenseitig ('mutual authentication') ausweisen.

So kann sich der Anwender sicher sein, seine Daten im richtigen Web-Portal und nicht auf einer gefälschten Webseite einzugeben. Als Voraussetzung dafür, dass ein Benutzer Tickets beim Kerberos Key Distribution Center anfordern kann, muss diese Komponente den Benutzer kennen. Dazu arbeitet ein KDC mit einem Verzeichnisdienst zusammen, im Fall von Microsoft Windows mit dem ActiveDirectory. Das 'Ticket Granting Ticket' (TGT), das anstelle der Passwörter oder zertifikatsbasierenden PKI zur weiteren Verwendung abgespeichert wird, ermöglicht für eine genau definierte Gültigkeitsdauer von z.B. 8 Stunden oder bis der Benutzer sich ausloggt, die Nutzung von Anwendungen und Diensten im Kontext des Anwenders. Das Service-Ticket, das über das TGT für eine Applikation angefordert wird, beinhaltet für jeden Benutzer genau die Zugriffsberechtigungen, die dieser hat, und unterstützt somit die enge Einbindung der Anwendungen.

Der Einsatz von Kerberos setzt je nach Komplexität der Netzwerkstrukturen mitunter eine aufwendige Planung und Konfigurationsarbeit voraus. Es müssen verschiedene Systemumgebungen integriert werden.

Die administrativen Herausforderungen beginnen bei der Vergabe von differenzierten Berechtigungen in allen Bereichen und gehen hin bis zu einem anwendungsübergreifenden Benutzermanagement. Aber auch die Software-Entwickler müssen jede einzelne Anwendung zur Unterstützung des Kerberos-Protokolls explizit anpassen (kerberisieren). Aber nach allen Anstrengungen steht ein System mit einem deutlich höheren Sicherheitsstandard und Anwenderkomfort zur Verfügung.

Leider bietet der IBM-Mainframe für häufig benutzte 3270-Applikationen wie z.B. CICS, TSO, und andere keine Kerberos-Unterstützung, so dass der Anwender nach wie vor gezwungen ist, nach Starten seiner 3270-Terminalemulation, Benutzernamen und Passwort in die Hostmaske einzugeben. Hier bietet die Firma HOB mit der Hostsoftware HOBCOM und der 3270-Terminalemulation HOBLink J-Term bzw. HOBLink Terminal Edition eine komfortable Methode, diese Applikationen in die Kerberos-Infrastruktur einzubinden. HOBLink J-Term ist eine überaus leistungsfähige Web-to-Host Lösung mit einem großen Funktionsumfang. So werden neben 3270-, auch 5250-, VT525-, HP700-, 97801-, oder 9750-Anbindungen, so-wie der RDP-Zugriff auf Windows Remote Desktop Services unterstützt. Die Benutzer können mit HOB Enterprise Access zentral administriert und konfiguriert werden. Als plattformunabhängige Java-Anwendung läuft HOBLink J-Term unter Windows, Linux, Mac OS X oder anderen. Ebenso möglich ist der Einsatz von HOBLink Terminal Edition, das auch eine leistungsfähige 3270-Emulation für Windows enthält.

Beim Einsatz in einer Kerberos-Infrastruktur arbeitet HOBCOM als ein zentraler Authentifizierungsserver zum Beispiel gegenüber CICS oder anderen Anwendungen. HOBCOM speichert die Authentifizierungsnachweise (Name/Passwort oder RACF PassTickets) für verschiedene Applikationen und übergibt diese im Hintergrund an die Anwendungen. Durch diesen 'Workaround' erfolgt nun die Anmeldung an die Hostapplikation ebenfalls als 'Single Sign-On' ohne weitere Benutzereingabe.

Der Benutzer startet auf seinem Windowssystem wie gewohnt seine 3270-Emulation (HOBLink J-Term oder HOBLink Terminal Edition), die nun das Service-Ticket an die Hostanwendung HOBCOM weiterleitet. Das verschlüsselte Service-Ticket enthält alle benötigten Informationen, wie zum Beispiel Benutzernamen ('principal') oder Service. Eine Hostanwendung wie CICS, die über HOBCOM gestartet wird, erhält dann in der erscheinenden Login-Maske sofort automatisch den richtigen Benutzernamen und das richtige Passwort. Dies geschieht über die Funktion 'Screen Mask', die es ermöglicht auch komplexe Prozeduren zu erstellen. Sollte RACF zum Einsatz kommen, so ist das Anmelden über *RACF PassTicket* sehr einfach zu realisieren. Somit lässt sich hier eine Verbindung der Kerberos-Infrastruktur mit RACF-Definitionen schaffen.

Mit Hilfe von 'Screen Mask' können verschiedene Bildschirminhalte (oder Teile davon) abgefragt und entsprechend dem Bild bestimmte Eingaben veranlasst werden. Dabei können nicht nur die Zeichen in der Bildschirmanzeige überprüft werden, sondern auch die Attribute. Innerhalb eines 'Screen Mask'-Eintrags können mehrere Bildschirminhalte

nacheinander beschrieben werden, so dass man auch über mehrere Bildschirmmasken hinweg den Ablauf automatisieren kann. Durch die Möglichkeiten mehrere Vergleichsoperationen zu verknüpfen bzw. komplexe Operationen zu programmieren, ist sichergestellt, dass es zu keinen falschen Eingaben kommt.

Somit brauchen die Anwender auch beim Arbeiten mit dem Mainframe nicht auf den gewohnten Komfort und die Sicherheit einer Kerberos-Infrastruktur zu verzichten.

09.12.08 JL
akt. 20.04.10 JL/KWi