

Sicherheitsaspekte – Internet-Technologie Seminar

Vortrag: Armen Lalayan

Leitung: Prof. Dr. Herbert Göttler, Thomas Gottron

Ausarbeitung

Einleitung

Das Ziel des Vortrags und dieser Ausarbeitung ist eine kurze Erläuterung der Sicherheitsmaßnahmen, Techniken und Mechanismen, die ihren Einsatz in der Absicherung der Rechner und der Daten in Netzwerken finden. Es wird ein kurzer Blick auf die Programm-Technische Sicherheitslösungen geworfen, sowie einige „sichere“ Protokolle erläutert.

Grundbegriffe der Netzwerksicherheit

Um die Sicherheitsaspekte in Netzen im weiteren Sinne in Betracht zu ziehen, ist es notwendig die Grundbegriffe der Sicherheit im Rechenwesen zu klären. Im Großen und Ganzen sind es drei: die Bedrohung, die Anfechtbarkeit und der Angriff. Unter dem Begriff „Bedrohung“ der Sicherheit eines Computersystems ist ein potenziell möglicher Vorfall zu verstehen (ob absichtlich oder nicht), der einen unerwünschten Einfluss auf das System und/oder auf die Daten im System haben kann.

Mit Anfechtbarkeit bezeichnet man eine „schwache“ Charakteristik des Systems, die erst die Bedrohungen möglich macht. Mit anderen Worten, die Anfechtbarkeit ist eine Schwachstelle des Rechensystems, die zur Bedrohung führen kann. Es ist üblich drei Haupttypen hierbei hervorzuheben: Die Bedrohung der Offenlegung der Information, die Bedrohung der Integrität der Daten und die DoS Bedrohungen.

Die Offenlegung besteht darin, dass die Information im System denen bekannt wird, die normalerweise keinen Zugriff auf diese haben dürfen. Die Bedrohung der Offenlegung kommt dann zustande, wenn nicht autorisierte Personen

sich Zugriff auf vertrauliche Informationen im Rechensystem oder im Netzwerk verschaffen. Die Bedrohung der Integrität beinhaltet eine beliebige Änderung oder Zerstörung der Daten im Rechensystem oder im Netz. DoS Bedrohungen kommen immer dann zustande, wenn durch bestimmte Handlungen der Zugriff auf bestimmte Ressourcen des Rechensystems blockiert wird.

Und letztlich der Angriff auf ein Rechensystem ist eine Handlung eines „Missetäters“, die darin besteht den einen oder den anderen Anfechtbarkeitspunkt im System zu finden, um sich dadurch den Zugriff aufs System oder auf darin befindlichen Daten zu ergattern. Somit kann man den Angriff als Realisierung der Bedrohung bezeichnen.

Jetzt noch kurz zur Definition des Begriffs Netzwerksicherheit. Eine feste Begriffserklärung ist hier schwer zu geben. Unter Netzwerksicherheit sind die Maßnahmen zur Planung, Ausführung und Überwachung der Sicherheit in Netzwerken zu verstehen. Dies beinhaltet nicht nur die technischen Aspekte und Mechanismen, die der Sicherheit der Daten in Netzwerken dienen, sondern auch organisatorische Maßnahmen, so wie der Ansatz bestimmter Policies (Regeln) innerhalb einer Organisation und/oder Abteilung. Dabei müssen die Datensicherheit und der Datenschutz gewährleistet sein. Unter Datensicherheit versteht man den Schutz der Daten vor Verlust, Manipulationen und Offenlegung, dabei muss aber die Verfügbarkeit der Daten nicht beeinträchtigt und die Integrität dieser gewährleistet sein. Als Datenschutz bezeichnet man den Schutz eigener Daten vor dem Missbrauch, das beinhaltet die Bewahrung der Privatsphäre, die Übertragungssicherheit in Netzwerken und die Gewährleistung der Vertraulichkeit.

Zur Garantie des Datenschutzes und der Datensicherheit setzt man die Zugriffssteuerungsmechanismen ein. Die wichtigsten Begriffe hierbei sind: die Authentifizierung (Sicherstellung einer Identität anhand eines bestimmten Merkmals) und die Autorisierung (Ermächtigung einer Person oder einer Gruppe auf die Ausführung gewisser Aktionen in dem Datenverarbeitungssystem). Erst nach der erfolgreichen Authentifizierung wird die Person oder z.B. ein Rechner autorisiert auf bestimmte Daten zuzugreifen oder diese zu ändern. Zur Sicherstellung der Authentizität werden heutzutage folgende Mechanismen/ Technologien eingesetzt:

Das einfachste ist die Authentifizierung durch Eingabe einer Kennung und dazugehörigem Passwort (ist üblich bei Personen), eine Chipkarte, Einsatz sogenannter digitaler Signaturen und Zertifikate (üblich wenn sich die Rechner im Netz gegenseitig authentifizieren, PGP- Systeme oder bei E-Mail Nachrichten) und biometrische Daten (Fingerabdruck usw.). Im Weiteren wird nur der Begriff Digitaler Signatur (Zertifikate) näher erläutert.

Die Technologie der Zertifikate bietet folgende Vorteile zur Gewährleistung der Sicherheit. Die Echtheit des Zertifikates kann überprüft werden, das Zertifikat kann man nicht fälschen, vom Zertifikat kann man nicht „abschwören“. Die Zertifikate werden häufig eingesetzt, um die Zugehörigkeit eines kryptografischen Schlüssels zu einer Person/Firma/Institution (z.B. bei der PGP- Verschlüsselung von Dateien oder E-Mails) einer Maschine (z.B. bei der SSL- Verschlüsselung) zu bestätigen¹. Dies ist auch noch dadurch ermöglicht, dass die Zertifikate von bestimmten autorisierten Zertifizierungsstellen vergeben werden und damit als vertraulich gelten. Die abgelaufenen Zertifikate oder solche, deren Schlüssel nicht mehr sicher sind, werden in den so genannten Zertifikatssperllisten aufgelistet. Die Echtheit eines Zertifikats wird durch die digitale Signatur einer vertraulichen Organisation bestätigt.

An dieser Stelle ist ein Rückblick auf die Kryptographie angebracht. In der Welt der Rechner und Rechnernetzwerken werden symmetrische und asymmetrische Block- und Strom-Verschlüsselungsverfahren eingesetzt. Als symmetrisch bezeichnet man dabei die Verschlüsselungsalgorithmen, bei denen ein und derselbe geheime Schlüssel sowohl für Ver- als auch für die Entschlüsselung benutzt wird. Der Vorteil dabei ist der geringe Rechenaufwand bei Ver- und Entschlüsselung. Nachteilig ist die Notwendigkeit eines sicheren Kanals, um die Schlüssel austauschen zu können.

Die asymmetrischen Chiffrieralgorithmen verwenden zwei unterschiedliche Schlüssel. Der eine so genannte öffentliche Schlüssel wird für die Verschlüsselung benutzt und ist jedem bekannt, der andere (geheime Schlüssel) wird bei der Entschlüsselung eingesetzt und muss geheim gehalten werden. Nachteil dabei ist der extrem große, im Vergleich zu den symmetrischen Verfahren, Rechneraufwand.

Die bekanntesten Verschlüsselungsverfahren, die ihre Verwendung im Re-

¹ Digitales Zertifikat: de.wikipedia.org/wiki/Zertifikat_%28Informatik%29. Stand: 20.02.2006

chenwesen finden, sind: DES, AES, IDEA, RC4 den symmetrischen und RSA und Rabin von den asymmetrischen.

Sichere Protokolle

Um die Netzwerksicherheit auf der Protokollebene zu gewährleisten, werden unterschiedliche sichere Netzwerkprotokolle eingesetzt, die es ermöglichen die Pakete möglichst sicher durch die unsicheren Netze zu transportieren.

Erwähnenswert sind:

DNSSEC – ist eine Weiterentwicklung des DNS Protokolls und bietet neben der schon in DNS bestehenden Leistungen noch die Authentifizierung und die Sicherstellung der Integrität der Information auf dem DNS-Server mittels der Digitalen Signaturen an. DNSSEC als solcher gewährleistet nicht die Vertraulichkeit der Information und bietet keine Zugriffssteuerungsmechanismen an.

Des Weiteren betrachten wir den bedeutenden oder besser den meist verbreiteten, besonders in Verbindung mit HTTP und FTP Protokollen, das SSL-Protokoll. Dieses wurde von Netscape im Jahre 1991 entwickelt. Der große Vorteil, der ihm seine Popularität verschaffen hat, besteht darin, dass er oberhalb der Transportebene im OSI- Modell sitzt, demzufolge einen sicheren Kanal für alle Anwendungsprotokolle bietet und völlig transparent für die letzteren ist. Der seitens SSL zur Verfügung gestellte Kanal ist privat (alle Pakete werden chiffriert), der Kanal ist authentifiziert (der Server authentifiziert sich immer gegenüber dem Client, Umkehrweg ist optional), der Kanal ist sicher (die Integrität der Daten wird durch den Einsatz der Hasch-Algorithmen gewährleistet)

SSL selbst besteht aus vier Teilprotokollen, dem Handshake Protokoll – dessen Rolle in der gegenseitigen Authentifizierung der kommunizierenden Rechnern (hierfür werden Zertifikate eingesetzt) und dem Aushandeln eines symmetrischen Chiffrierverfahrens für die weitere Kommunikation besteht. Das Record-Protokoll bietet sicheren Datenaustausch mit dem von Handshake ausgehandelten symmetrischen Chiffrierverfahren. Das Cipher Spec - Unterprotokoll wird zum Schlüsselaustausch verwendet und das Alert - Unterprotokoll nimmt die Fehlerbehandlung auf sich.

Als Vergleich zu dem SSL-Protokoll wird ein kurzer Blick auf den SHTTP Protokoll angeboten. Dieser setzt auch Datenverschlüsselung und Zertifizierung ein, um sichere Kommunikation herzustellen und ist einfach in bestehende Systeme zu integrieren, beschränkt sich jedoch nur auf HTTP und dadurch ist kaum verbreitet. Es wird auch von keinem der bekannten Web-Browser unterstützt.

SNMPv3 – ist eine Weiterentwicklung des SMTP- Protokolls und setzt sowohl die Authentifizierung von Personen und Rechnern als auch die Verschlüsselung von Nachrichten ein.

PPTP (Point- to- Point Tunneling Protocol) und IPSec (IP Secure) werden zum Aufbau eines VPN (Virtual Private Network) verwendet. Der PPTP ermöglicht das Tunneling des PPP durch IP-Netzwerke, IPSec gewährleistet die Integrität der Daten, bietet Authentifizierung und sichert die Vertraulichkeit.

Programm-Technische Absicherung

Die Grundmethodik der Programm-Technischen Absicherung eines bestimmten Segments des IP-Netzes ist die Firewall. Firewall bietet folgende Hauptfunktionalitäten an: Mehrschichtige Filtrierung des Traffiks, Proxy-Schema mit zusätzlicher Identifikation und Authentifikation, Trennung des Netzes in das private und das öffentliche Bereiche.

Filtrierung des Traffiks findet in der Regel in den Sicherheits-, Netzwerk-, Transport- und Anwendungssichten des OSI Modells statt. Filtration des Netzwerktraffiks ist die Hauptfunktion der Firewall und ermöglicht dem Netzwerkadministrator den zentralisierten Einsatz der nötigen Policies in bestimmten Abschnitten des Netzwerkes.

Man unterscheidet drei Arten von Firewall: Paket-Filter, Application Proxy und Kombinierte.

Die Filtration des Traffiks findet zunächst in den Routern statt, damit bilden die Firewall quasi die zweite Schicht der Programm-Technischen Absicherung des Netzes. Die Pakete werden in beiden Richtungen filtriert, damit ist es möglich so-

wohl den Zugriff auf bestimmte Dienste der Hosts im von der Firewall geschützten Netzwerk aus dem öffentlichen Netz zu kontrollieren als auch den Zugriff der Benutzer des Inneren Netzes zu bestimmten Ressourcen des öffentlichen Netzes zu gewährleisten oder zu blockieren.

Das Proxy-Schema bietet eine zusätzliche Authentifizierung beim Zugriff auf geschützte Hosts und verbirgt die Rechner im inneren Netzwerk hinter sich. Die öffentlichen Rechner kommunizieren dabei mit dem Proxy-Server ohne zu wissen, dass der Adressat sich hinter dem Proxy versteckt.

Ein typisches Beispiel für Firewall ist auf der Folie 21 des Vortrages abgebildet. Dabei sind:

Perimeter network - Grenznetzwerk zwischen den Innen- und Außennetzen. Beinhaltet normalerweise öffentliche Server.

Bastion host – ein oder mehrere Server, die den Traffic zwischen dem öffentlichen und dem privaten Netzwerken kontrolliert.

Exteriour router – Außenrouter. Schützt das Innennetzwerk vor dem öffentlichen.

Interiour router – Innenrouter. Leistet einen zusätzlichen Schutz des Innennetzwerkes im Falle eines Servereinbruchs.

Internal network – Inneres geschütztes Netzwerk.

Demilitarisierte Zone (DMZ) ist eine Möglichkeit die private Information vor der öffentlichen zu schützen. Die DMZ's werden meistens zur Abgrenzung der „öffentlichen“ Hosts (z.B. Web-, DNS-, Mail-Server) vom übrigen Organisationsnetzwerk eingesetzt. Dadurch wird das Innere Netz vor z.B. DoS Attacken, Packet-sniffing, Port scans, usw. geschützt, die Verbindung zu nicht autorisierten Hosts im öffentlichen Netz limitiert und protokolliert. Man kann die DMZ's auch z.B. für die Isolierung eines bestimmten Abschnittes vor dem übrigen Organisationsnetzwerk einsetzen.

Sicherheit in WWW

Der Web-Server selbst ist die Software, die die Wechselwirkung mittels HTTP- Protokolls mit Browsern realisiert: Annahme von Anfragen, Suche der ge-

brauchten Dateien und Transport deren Inhalte, Ausführen der CGI Skripte und Übergabe deren Ergebnisse an den Clienten. Damit stellt die Sicherheit eines Web-Servers nur eine kleine Komponente des gesamten Sicherheitssystems des Hosts dar.

Die Sicherheitslücken in den WWW Servern, die Bedrohungen darstellen können, sind meistens entweder auf fehlerhafte Administration oder schlecht programmierte dynamische Komponente (sowie z.B. CGI Skripte), Plug-ins usw. zurückzuführen. Dabei werden folgende Fehlerklassen unterschieden:

Fehler, die zur Verlust der Vertraulichkeit führen,
Fehler die zu den Attacken vom DoS Typ führen und
Fehler die zur Ausführung nicht autorisierter Programmcodes führen.

Dies kann zum Beispiel zur folgenden Angriffarten führen:

Umgehen der Authorisation:

Brute Force Methode – basiert auf einem automatisierten Vorgang in dem durch einfaches Ausprobieren die Kennung und das dazugehörige Passwort eines Benutzers „erraten“ wird.

Insufficient Authentication – kommt dann zustande, wenn der Web-Server ohne dazugehörige Authentifikation dem Angreifer den Zugang zur wichtigen Information gewährt.

Umgehen der Authorization:

Insufficient Authorization – unzureichende Autorisation ist dann der Fall, wenn der Server dem Angreifer Zugriff auf die Daten ermöglicht, auf die er normalerweise keinen haben sollte.

Ausführen von Kommandos:

OS Commanding – Attacken dieser Klasse sind auf das Ausführen der Kommandos des Betriebssystems auf dem Web-Server durch die Manipulation mit Eingabedaten zurückzuführen.

SSI Injection – Attacken dieser Klasse ermöglichen dem Angreifer, einen ausführbaren Code auf dem Web-Server zu starten.

Offenlegung der Information:

Web Server/Application Fingerprinting – ist eine Bestimmung der Softwareversionen mit dem Ziel, Informationen über die verwendeten Betriebssysteme, Web-Servern und Browsern zu bekommen.

Information Leakage – Diese Anfechtbarkeiten kommen dann zu Stande, wenn von der Server Seite irgendwelche wichtige Informationen über das System publiziert werden.

Logical Attacks:

Abuse of Functionality – Diese Art von Attacken ist auf die Nutzung der Funktionalität der Web- Anwendungen gerichtet, mit dem Ziel, die Zugriffssteuerungsmechanismen zu umgehen.

Insufficient Process Validation – Anfechtbarkeiten dieser Klasse kommen dann zu Stande, wenn der Server nicht gründlich genug die Reihenfolge der Ausführung von Operationen prüft.

Am Ende ist noch kurz zu erwähnen, dass die meisten Sicherheitslücken auf der Client- Seite auf die Einstellungen der benutzten Browsern, die Plug- in's, die diese Browser benutzen, die dynamischen Elementen (MS ActiveX, Java- Applet, Java Script usw.) und Cookies zurückzuführen sind.

Benutzte Literatur:

- Allan Liska: The Practice of Network Security: Deployment Strategies for Production Environments. Prentice Hall PTR. 2002
- Prof. R. Kröger. Skript zur Veranstaltung „Verteilte Systeme“. 2005
- Priscilla Oppenheimer: Top-Down Network Design Second Edition. Cisco Press. 2004
- Chris McNab: Network Security Assessment. O'Reilly. 2004
- Chris Hare, Karanjit Siyan: Internet Firewalls and Network Security. New Riders Publishing. 1996
- *Илья Медведевский, Павел Семьянов: Атака на Интернет. ДМК. 2004*
- Соколов А.В., Степанюк О.М.: Защита от компьютерного терроризма. БХВ - Петербург. 2002
- www.wikipedia.org