Erschreckende Sicherheitsdefizite bei Internet-Anwendungen

Seeming Secure Layer

Dominique Petersen, Norbert Pohlmann

Etliche Internet-Anwender legen mittlerweile Wert darauf, verschlüsselt zu kommunizieren – zumindest mit der Banking-Website, schon seltener mit ihrem Mailserver. Die für die Sicherheit wesentliche Art und Weise der Verschlüsselung ist jedoch den meisten egal – mit möglicherweise fatalen Folgen.

Das Internet ist selbstverständlicher Teil des privaten und beruflichen Lebens, und wir füttern es bereitwillig mit persönlichen Daten wie Adressen, Passwörtern, Kontonummern und PINs. Längst interessieren sich kriminelle Vereinigungen, die hier das große Geld wittern, für derlei Informationen. Diverse Fälle illegalen Datenhandels mit Millionen Kunden- und Kontodaten zeigen, welch blühender und lukrativer Geschäftszweig hier entstanden ist. Firewall-Programme und Virenscanner auf PCs bieten nicht den geringsten Schutz dagegen. Eine verschlüsselte Kommunikation bei der Übertragung sensibler Daten gilt als obligatorisch. Doch verschlüsselte Verbindungen sind keineswegs immer sicher.

Den Transport von Webseiten und E-Mails verschlüsselt meist das Protokoll Transport Layer Security (TLS), eine standardisierte Weiterentwicklung des Secure Sockets Layer (SSL) 3.0 von Netscape. Aus diesem Grund sind die Begriffe TLS und SSL praktisch synonym in Gebrauch. Beide Protokolle gehören zu den hybriden Verschlüsselungsverfahren: Sie bestehen aus einer Kombination von symmetrischen Algorithmen wie AES, (Triple-)DES oder IDEA und asymmetrischen Verfahren (Public Key) wie RSA oder Elgamal, um deren jeweilige Vorteile zu vereinen. Den Verbindungsaufbau schützt das Public-Key-Verfahren, die eigentliche Datenübermittlung erfolgt symmetrisch verschlüsselt.

Verschlüsselung mit TLS/SSL

Den Aufbau einer gesicherten Verbindung verdeutlicht das Beispiel, dass ein Benutzer mit seinem Browser (Client) auf eine verschlüsselte Webseite (Server) zugreift (siehe Abb. 1). Der Client besorgt sich vom Server das öffentliche Zertifikat der Webseite. Es enthält Informationen über den Namen des Servers und des Zertifikatausstellers, eine Gültigkeitsdauer und den öffentlichen Schlüssel.

Der Client prüft das Zertifikat auf Gültigkeit und kann so die Integrität und Authentizität der Webseite verifizieren. Da gültige Zertifikate nur von vertrauenswürdigen Instanzen stammen und sich nicht ohne Weiteres verändern lassen, bietet diese Vorgehensweise dem Benutzer einen grundlegenden Schutz vor Angriffen wie Phishing und Pharming – vorausgesetzt er handelt verantwortungsbewusst und akzeptiert keine fragwürdigen Zertifikate. Beim Phishing gerät der Benutzer über falsche Links auf manipulierte Server, während Pharming-Angreifer die Hostnamen-Auflösung per DNS-Spoofing fälschen. Manipulationen an Zertifikaten decken kryptografische Prüfsummen (Hashes) wie SHA oder MD5 auf.

Akzeptiert der Client das Zertifikat, generiert er eine Zufallszahl, den Session Key, und übermittelt sie – verschlüsselt mit dem öffentlichen Schlüssel des Servers – an die Webseite. Nur der richtige Server kann mit seinem geheimen Schlüssel den Session Key entschlüsseln. Damit steht die Verbindung, und die eigentlichen Nutzdaten wie die Formulardaten des Benutzers und der Inhalt der Webseiten gehen fortan mit dem Session Key symmetrisch verschlüsselt und mittels Hash-

Verfahren auf Integrität verifiziert über die Leitung.

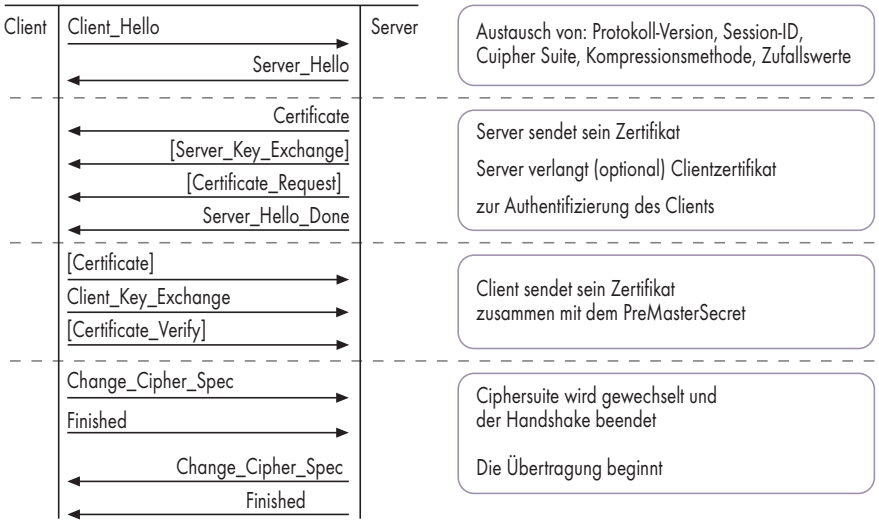
Entscheidende Unterschiede

Wenigen Anwendern ist bewusst, wie sehr sich die verwendeten Verschlüsselungsverfahren hinsichtlich ihrer kryptografischen Leistungsfähigkeit voneinander unterscheiden. Zwar sind alle Kryptosysteme mit genügend Rechenkraft knackbar, aber der Aufwand für Angreifer hängt stark von zwei beeinflussbaren Variablen ab. Zunächst von der Schlüssellänge, die den theoretischen Aufwand für das Ausprobieren aller möglichen Kombinationen festlegt. Hinzu kommen jedoch Schwachstellen, die ein Krypto-Algorithmus aufweisen kann. Sie verringern den theoretischen Aufwand bisweilen stark und bilden eine reale Bedrohung.

Die tatsächlich genutzte Kombination aus asymmetrischer und symmetrischer Verschlüsselung handeln die Clients mit den Servern aus. Dazu schickt etwa der Webbrowser eine Liste der ihm zur Verfügung stehenden Verfahren an den Server, der eines davon selektiert. Wenn nur eine der Parteien keinen sicheren Algorithmus anbietet, entsteht eine Sicherheitslücke.

Nach Angaben verschiedener Standardisierungsorganisationen und namhafter Kryptografieexperten [a, b, 1] gelten etwa die Verschlüsselungsverfahren RC4 sowie DES und das Hash-Verfahren MD5 mit zu geringer Schlüssellänge heutzutage als unsicher (siehe Tabelle). Vertrauenswürdig sind hingegen die Verschlüsselungen Triple-DES, AES und die Prüfsumme SHA mit langen Schlüsseln.

Bei der Benutzung von TLS/SSL gibt es also eine Vielzahl an Kombinationsmöglichkeiten für die verwendete Verschlüsselung, die enorme Unterschiede in der Sicherheit aufweisen. Als Extrembeispiel sei angeführt, dass es sogar erlaubt ist, den Datenaustausch



Beim Onlinebanking und anderen Internet-Anwendungen ist SSL alias TLS unverzichtbar. Es kann jedoch den Benutzer in trügerischer Sicherheit wiegen.

selbst ohne Session Key zu verschlüsseln, was einer Übermittlung im Klartext gleichkommt. So wären lediglich die Integrität und Authentizität des entfernten Servers sichergestellt, obwohl der Browser dem Benutzer mittels eines Schloss-Symbols eine sichere Sitzung suggeriert. Es stellt sich die Frage, ob überhaupt ein Website-Betreiber solch unsichere „Verschlüsselungen“ nutzt.

Sicherheitstrends im Internet

Um Licht ins Dunkel der Netzwerkkommunikation zu bringen, entwickeln und optimieren die Autoren am Institut für Internet-Sicherheit [d] seit über vier Jahren das Internet-Analyse-System (IAS, [e]), eine Kernkomponente der Internet-Frühwarnsysteme (IFS, [f]). Das IAS beobachtet den Datenverkehr paketorientiert und passiv und zählt anonymisierte, vorher definierte Protokoll-Header-Informationen (Deskriptoren). Damit lassen sich Statistiken generieren und grafisch auswerten.

Die verwendeten Deskriptoren identifizieren ausschließlich datenschutzrechtlich nicht relevante Kommunikationsparameter der OSI-Schichten 2 (Sicherungsschicht) bis 7 (Anwendungsschicht), zum Beispiel einen gesetzten TCP-Syn-Flag beim Verbindungsaufbau oder einen speziellen Browser-Typ. Derzeit sind über 870 000 verschiedene Kommunikationsparameter im Datenstrom identifizierbar.

Da die im Internet verteilten Sensoren des IAS seit mehreren Jahren laufen, lassen sich Statistiken auch über längere Zeiträume generieren. So ist festzustellen, dass der verschlüsselte Verkehr auf Webservern (HTTPS) im Fachbereich Informatik der FH Gelsenkirchen und bei den Partnern des if(is) nur rund 5 bis 15 % ausmacht, dementsprechend sind 85 bis 95 % ungeschützt (HTTP). Diese Verteilung hat sich im Laufe der letzten Monate nicht signifikant verändert.

Im Fachbereich Informatik der FH Gelsenkirchen ist bei den verwendeten Verschlüsselungsverfahren (siehe Abbildung 1) hingegen ein deutlicher Trend vom unsicheren RC4/MD5 zum sicheren AES/SHA zu verzeichnen, auch wenn nach wie vor RC4 einen nicht unerheblichen Anteil ausmacht. Andere Verschlüsselungsverfahren und Kombinationen machen weniger als ein Prozent des Gesamtverkehrs aus.

RC4 mit MD5 oder SHA machte im Jahr 2007 noch insgesamt 67 % aus, 2008 nur noch 35 %. Dafür steigerte sich AES/SHA mit seinen unterschiedlichen Ausprägungen hinsichtlich der verwendeten Schlüssellängen (128 bis 256 Bit) und des optional zusätzlich genutzten Schlüsselaustauschprotokolls Diffie-Hellman (DHE) insgesamt von 33 auf 65 %.

Dass solch wünschenswerte Entwicklungen nicht überall stattfinden, zeigen die Daten weiterer Partner des Instituts für Internet-Sicherheit, in diesem Fall einer großen deutschen Firma und eines mittelständischen Internetproviders. Bei

iX-TRACT

- Zum Verschlüsseln von Internet-Kommunikation stehen mehrere aus heutiger Sicht ausreichend sichere Verfahren zur Verfügung.
- Messungen der tatsächlich eingesetzten Verschlüsselungsverfahren zeigen sowohl im Web als auch bei E-Mail erschreckende Defizite.
- Sowohl Client- als auch Server-Software müssen auf dem aktuellen Stand sein, und der Systemverwalter muss unsichere Konfigurationen unterbinden.

der Firma ist deutlich zu erkennen, dass die Verschlüsselung RC4/MD5 mit 88 % vor AES/SHA mit lediglich 10 % dominiert. Ähnlich sieht es beim Provider mit einem Anteil von 71 % RC4/MD5 und 23 % AES/SHA aus. Allerdings weist hier der Datenverkehr die Verschlüsselung Triple-DES/SHA mit einem nennenswerten Anteil von 5 % auf.

Die Statistik der Firma verdeutlicht ein Blick auf die Browser-Verteilung. Zu erkennen ist die durchschnittliche Nutzung des Internet Explorer von Microsoft in der Version 6 mit 44 %, in der Version 7 mit 29 % und des Mozilla Firefox mit 20 %. Zwar bietet der Internet Explorer erst ab Version 7 eine Verschlüsselung mit bis zu 256 Bit, doch erklärt dies nicht die derart starke RC4/MD5-Nutzung. Daher liegt die Vermutung nahe, dass auf den Webservern immer noch zahlreiche veraltete Softwarekomponenten laufen, von denen viele durch die strikten Verschlüsselungs-Export-Beschränkungen der USA gehemmt sein dürften. Der Datenverkehr weist sogar gelegentlich (< 0,01 %) leere Sitzungsschlüssel auf, also eine Klartextübermittlung der Informationen, was für sensible Daten fatal sein kann.

E-Mails unsicher wie Postkarten

Bei einer Partner-Universität in Brasilien findet sich ein wesentlich breiteres Spektrum an genutzten Kombinationen der Verschlüsselungsverfahren, aber die Verteilungen zeigen mit einem RC4/MD5-Anteil von 79 % und einem AES/SHA-Anteil von 12 % ein ähnliches Bild, was sich mit der gemessenen Nutzung des Internet Explorer 6 mit 50 % zumindest teilweise erklären lässt.

Gängige Krypto-Verfahren

Symmetrische Verschlüsselung		
Verfahren	Anzahl Bits	Sicherheit
DES	56	sehr unsicher
RC4	128	unsicher
AES	128	sicher
Triple-DES	168	sicher
Camellia	256	sehr sicher
AES	256	sehr sicher
Hash-Funktionen		
Verfahren	Anzahl Bits	Sicherheit
MD5	128	unsicher
RIPEMD	160, 256, 320	sicher
SHA	160, 224, 256, 384, 512	sicher

Mindestens so sicherheitskritisch wie das Websurfen ist die E-Mail-Kommunikation. Immerhin gehen beim Abrufen der E-Mails mit POP3(S) oder IMAP(S) Autorisierungsdaten wie Username und Passwort über die Leitung, ebenso beim Versenden von Nachrichten (SMTP(S)) über den Provider – zumindest wenn der eine Anmeldung verlangt, um kein offenes Mail-Relay zu betreiben. Aber auch die E-Mails selbst können sensible Daten übers unsichere Internet von einem Mailserver zum nächsten transportieren.

Die Analyse des Mailverkehrs (SMTP(S)) im Fachbereich Informatik der FH Gelsenkirchen zeigt, dass weniger als ein Prozent der E-Mails per verschlüsselter Session (nicht zu verwechseln mit einer Verschlüsselung der E-Mail-Inhalte auf Anwendungsebene) über die Leitung gehen. Zwar handelt es sich beim unverschlüsselten Mailaufkommen größtenteils um Spam, doch rechnet man den Spam-Anteil heraus, bleiben immerhin noch über 97 % der im Klartext übertragenen Nachrichten übrig.

Beim Abrufen von E-Mails sieht es ähnlich unsicher aus. Zwar ist ein schwacher Trend zu mehr Verschlüsselung zu erkennen, aber insgesamt fällt die Analyse auch hier ernüchternd aus. Im August 2006 waren nur 18 % verschlüsselt. Im Juni 2008 mit 32 % verschlüsselten Zugriffen sind die Verhältnisse immer noch insgesamt unsicher. Ergänzend war zu beobachten, dass der Einsatz des moderneren Verfahrens IMAP(S) gegenüber POP3(S) deutlich zugenommen hat, und zwar von 28 % im August 2006 auf 76 % im Juni 2008. Hier zeigt sich also deutlich, dass die Ursache für unverschlüsselten E-Mail-Abruf nicht allein in veralteten Verfahren liegt, sondern insbesondere auch darin, dass selbst neue Systeme unsicher konfiguriert laufen.

Immerhin nimmt die Qualität der genutzten Verschlüsselungsverfahren allmählich zu. 2006 dominierte noch das unsichere Verfahren RC4/MD5 mit 52 %, und das sichere AES/SHA erreichte lediglich einen Anteil von 41 %. Im Jahr 2008 hat sich das Verhältnis umgekehrt und der Anteil von AES/SHA liegt bei 55 %. Allerdings liegt RC4/MD5 mit 45 % immer noch sehr hoch und man kann davon ausgehen, dass Anwender etwa die Hälfte ihrer E-Mails nicht ausreichend geschützt versenden.

Sowohl Anwender von Browsern und E-Mail-Programmen als auch Administratoren von Serversystemen können einiges dafür tun, diese Missstände in puncto Verschlüsselung zu beheben. Ein wichtiger Schritt ist es, das Sicherheitsbewusstsein sowohl der Benutzer als auch der Betreiber zu erhöhen, damit sie nicht nur aktuelle Verfahren einsetzen, sondern diese auch mithilfe von Verkehrsanalysen so sicher wie möglich konfigurieren. Dies gilt vor allem für sicherheitskritische Onlineportale.

Bewusstsein führt zur Sicherheit

Auch Anwender eines Browsers oder E-Mail-Clients können sich ohne großen Aufwand aktiv schützen, indem sie aktuelle Versionen nutzen und deren Sicherheitseinstellungen verifizieren. Unsichere Verfahren wie RC4/MD5 sind zu deaktivieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet für verschiedene Browser eine Konfigurationsanleitung an [c]. Serverbetreiber belassen oftmals die unsicheren Standardeinstellungen der neu installierten Dienste, anstatt sie mit wenigen Handgriffen sicher zu konfigurieren. Sie haben keinen Einfluss auf das Benutzerverhalten, doch es liegt in ihrem Handlungsspielraum, zumindest ihre eigenen Server sicher zu betreiben.

Die sichersten TLS/SSL-Einstellungen nützen nichts, wenn Anwender auf gefälschte SSL-Zertifikate von Phishing-Servern hereinfallen. Zertifikate sollte man nur aus vertrauenswürdigen Quellen und in einer gültigen, nicht abgelaufenen Form akzeptieren. Da dies oft nicht eindeutig zu erkennen ist, gibt es seit einiger Zeit Extended-Validation-SSL-Zertifikate (EV), die besonders restriktiven Vergabekriterien hinsichtlich einer detaillierten Überprüfung der Zertifizierungsstelle genügen. Aktuelle Browser wie der Mozilla Firefox 3 (Version 2 per „Green Bar Extension“), der Internet Explorer 7 und Opera 9.5 honorieren gültige EV-SSL-Zertifikate mit einer grün markierten Adressleiste. Den gesunden Menschenverstand können und sollen solche Hilfen nicht ersetzen, denn auch das Erscheinungsbild eines Webbrowsers lässt sich manipulieren.

Fazit

Es ist sicherlich eine Frage der persönlichen Einstellung, ob man beim Laden nicht sicherheitskritischer Webseiten

Onlinequellen

[a]	Bundesnetzagentur, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung	www.bundesnetzagentur.de/media/archive/12198.pdf
[b]	National Institute of Standards and Technology	www.nist.gov
[c]	BSI für Bürger, Sicherheitscheck verschiedener Browser	www.bsi-fuer-buerger.de/browser/browsercheck.htm
[d]	Institut für Internet-Sicherheit	www.internet-sicherheit.de
[e]	Internet-Analysesystem	www.internet-sicherheit.de/IAS
[f]	Internet-Frühwarnsysteme	www.internet-sicherheit.de/IFS

eine Verschlüsselung für notwendig hält. Dass nur 5 bis 15 Prozent des HTTP-Verkehrs verschlüsselt sind, kann daher eigentlich niemanden ernsthaft beunruhigen.

Anders sieht es bei den Verschlüsselungsverfahren der nicht ohne Grund gesicherten Übertragungen aus. Messungen im Umfeld des Instituts für Internet-Sicherheit zeigen bis zu 88 Prozent unsichere Verfahren, teilweise sogar unverschlüsselt mit einem leeren Session Key, die den Anwendern Sicherheit lediglich vorgaukeln.

Auch im Bereich des E-Mail-Verkehrs ist der Anteil an genutzten Verschlüsselungen erschreckend gering. Fast zwei Drittel aller Nachrichtenübertragungen lassen sich im Klartext mitlesen. Die restlichen, verschlüsselten Verbindungen basieren nochmals etwa zur Hälfte auf unsicheren Verschlüsselungsverfahren.

Wer auf der sicheren Seite sein will, sollte Client-Programme und Serverdienste ausschließlich für sichere Verfahren einrichten und unsichere Verfahren deaktivieren. Dies erfordert meist die Aktualisierung der Softwarekomponenten auf zeitgemäße Versionen. Hier sind angesichts der Trägheit der Anwenderschaft vor allem die Softwarehersteller in der Pflicht. Sie müssen Upgrades mit sicheren Verschlüsselungen auch für ältere, noch im Umlauf befindliche Komponenten bereitstellen. (un)

DOMINIQUE PETERSEN

ist Mitarbeiter am Institut für Internet-Sicherheit der FH Gelsenkirchen und dort seit Januar 2007 Projektleiter der Internet-Frühwarnsysteme.

PROF. DR. NORBERT POHLMANN

ist geschäftsführender Direktor des Instituts für Internet-Sicherheit und Professor an der FH Gelsenkirchen im Fachbereich Informatik der Vertiefungsrichtung Internet und mobile Netze.

Literatur

[1] Bart Preneel, K. U. Leuven; Cryptographic Algorithms and Protocols for Network Security; ECRYPT, September 2008

iX-Link ix0901106