Sécurité des données et des services dans l'internet

Autor(en): **Schütz, Frédéric / Billard, David**

Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **91 (2000)**

Heft 7

PDF erstellt am: **08.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-855535

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Sécurité des données et des services dans l'Internet

La sécurité dans l'Internet recouvre deux aspects majeurs: la protection des données aussi bien que des services contre les attaques. Cet article décrit les attaques les plus fréquentes et montre que, paradoxalement, les systèmes dits «ouverts» sont nettement plus sûrs que les systèmes «propriétaires» dont le fonctionnement est gardé secret.

L'actualité concernant les nouvelles technologies de l'information et de la communication (NTIC) se fait souvent l'écho de problèmes de sécurité dans l'Internet. On parle alors de «hackers» qui «piratent» un site, ou même «d'espions» écoutant les communications les plus secrètes des grands groupes industriels. Si les informations techniques données sont souvent trop succinctes pour permettre de distinguer la part réelle de danger compromettant les systèmes, il n'en demeure pas moins que des attaques existent, constituent une menace grave et que des techniques de sécurité doivent être déployées, afin de les contrer.

Cet article propose de recenser les principales attaques auxquelles un concepteur de systèmes d'information peut s'attendre et contre lesquelles il doit se prémunir. Le document est structuré en trois parties: les attaques contre les données, celles contre les services, et des considérations générales sur les garanties que l'on devrait pouvoir attendre d'un système en matière de sécurité informatique.

Attaques contre les données

Les attaques contre les données sont celles auxquelles tout le monde s'attend lorsque l'on parle de sécurité. Typiquement, chacun va se préoccuper de la façon dont son numéro de carte de crédit va circuler dans l'Internet, avant même de considérer si le produit ou le service qu'il a commandé sera bien délivré. Cela peut aussi être constaté dans les milieux hospitaliers, où les données sensibles concernant un patient seront au centre des préoccupations.

Adresse des auteurs
Frédéric Schütz et Dr *David Billard*
Centre Universitaire d'Informatique (CUI)
Université de Genève
Rue du Général Dufour 24, 1211 Genève 4
Frederic.Schutz@cui.unige.ch

Dans les chapitres suivants nous détaillerons les attaques les plus fréquentes lors de la communication d'information:

- l'écoute de messages
- l'interception de messages
- la falsification de messages
- la création de faux messages

Nous verrons aussi que protéger la communication d'information ne suffit pas si les systèmes finaux (par exemple les serveurs Web) ne protègent pas aussi le stockage de leurs données.

L'écoute de messages

Dans cette attaque, une tierce personne prend connaissance d'un message qui ne la concerne pas, en espionnant les communications. Malheureusement, dans l'état actuel de la technique, personne ne peut empêcher un message d'être lu.

La parade à ces attaques est d'utiliser des algorithmes de cryptographie, c'est-à-dire de dissimuler le message en le chiffrant d'une manière dont seuls l'expéditeur et le destinataire connaissent le secret. Une des plus anciennes méthodes de ce genre est le fameux code de Jules César, dans lequel chaque lettre est remplacée par la lettre suivante dans l'ordre lexicographique («bonjour» serait codé «cpokpvs»). Les méthodes actuelles, basées sur des problèmes mathématiques compliqués, sont bien entendu beaucoup plus sophistiquées.

L'interception de messages

Dans cette attaque, une tierce personne intercepte un message qui ne sera donc pas remis à son (ou ses) destinataire. Toujours dans l'état actuel de la technique, personne ne peut empêcher un message d'être intercepté. Cependant, l'important est que:

- l'expéditeur et le destinataire soient informés qu'un message a été «perdu»
- le contenu du message ne soit pas divulgué

Pour le premier point, un système à base d'accusé de réception peut être mis en place (le destinataire d'un message envoie un autre message d'acquittement à l'expéditeur) et permettra, en cas de non-réception au bout d'un temps fini (quelques minutes), d'indiquer à l'expéditeur qu'un de ses messages a pu être intercepté ou perdu.

Pour le second point, naturellement, il est nécessaire de protéger l'information comme dans le cas de l'écoute de message.

La falsification de messages

Dans cette attaque, une tierce personne intercepte un message, en modifie le contenu, puis le transmet au destinataire premier. Toujours dans l'état actuel de la technique, personne ne peut empêcher un message d'être intercepté, modifié puis remis dans le circuit. Cependant, l'important est que:

- le contenu du message ne soit pas modifiable sans que le destinataire ne s'en aperçoive
- le contenu du message ne soit pas divulgué
- le destinataire s'aperçoive que l'émetteur réel du message n'est pas celui auquel on peut s'attendre

Pour le premier point, l'intégrité du message doit être préservée. Cela présuppose le deuxième point, ainsi que la non-modification (ajout ou suppression de contenu) du message original.

Pour garantir cette intégrité, l'expéditeur peut appliquer au message une formule mathématique, connue seulement de l'expéditeur et du destinataire, dont le résultat est une fonction du message original. Le résultat est envoyé au destinataire en même temps que le message. Le destinataire applique lui aussi la même formule mathématique au message reçu. Si le résultat est le même que le résultat envoyé par l'expéditeur, cela implique que l'intégrité du message a été préservée lors de la transmission.

Pour le troisième point, l'expéditeur peut ajouter une signature électronique au message, signature connue uniquement de l'expéditeur et du destinataire. Cette signature sera construite par une technique similaire à celle du premier point.

La création de faux messages

Dans cette attaque, une tierce personne fabrique de toutes pièces un message, puis le transmet en se faisant passer pour l'expéditeur premier. Ici encore, dans l'état actuel de la technique, personne ne peut empêcher un faux message d'être envoyé. Cependant, l'important est que le destinataire s'aperçoive que l'expéditeur n'est pas celui qu'il prétend être.

Dans ce cas, on peut toujours avoir recours à une signature électronique, comme dans le cas précédent.

La protection des données sur les serveurs

Avec l'essor du commerce électronique, les internautes sont de plus en plus sollicités pour laisser leurs données personnelles (adresse, âge, numéro de cartes de crédit) à l'occasion de visites ou d'achats sur des sites Web. Les sites Web offrent une communication sécurisée (donc la confidentialité de l'information lors de son transit par l'Internet est garantie) au moyen d'algorithmes de chiffrement complexes et résolvent ainsi les problèmes vus plus haut.

Cependant, il peut arriver que le stockage de ces données, qui ont transité de façon confidentielle sur le réseau, ne soit pas sécurisé, lui. C'est ainsi que le *Canard Enchaîné* du 10 mars 1999 a relaté comment un journaliste pigiste passionné d'informatique est tombé complètement par hasard sur la liste de tous les clients d'une boutique de livraison de fleurs. Il y découvrait les noms et adresses des clients ainsi que ceux chez qui les livraisons devaient être effectuées, les numéros de cartes bancaires, et beaucoup plus grave (à notre goût) les mots d'amour que les clients pouvaient adresser avec les fleurs.

Attaques contre les services

D'autres attaques existent, dirigées non pas contre des données, mais contre des services: au lieu d'essayer d'accéder à des informations, dans le but de les lire ou de les modifier, elles visent à empêcher les utilisateurs légitimes d'y accéder, d'où leur nom d'attaques «déni de service» (denial of service). Plusieurs démonstrations à grande échelle ont fait l'actualité au début de cette année et ont montré les problèmes qui peuvent en découler (fig. 1).

Pour comprendre comment une telle attaque peut se produire, examinons ce qui se passe quand deux ordinateurs A et B veulent communiquer entre eux sur Internet, par exemple dans le cas où l'utilisateur de l'ordinateur client A désire consulter une page Web située sur l'ordinateur serveur B. Avant tout échange de données, les deux machines doivent s'assurer que leur correspondant est prêt a recevoir des données. Pour cela, A commence par envoyer un message de «bonjour» (nommé SYN), et attend la réponse. Quand le serveur reçoit ce message, il répond «bonjour, bien reçu» (SYN ACK) et attend à son tour une réponse. Le client répond à son tour «bien reçu» (ACK), et peut commencer à envoyer des données, étant certain que son interlocuteur est bien attentif (fig. 2).

Que se passe-t-il si le client n'envoie jamais son signal ACK? Le serveur va patienter un certain temps (une minute par exemple), et s'il n'a rien reçu au bout de ce délai, il en concluera que la connexion a échoué, l'effacera de sa mémoire et se remettra en attente d'une nouvelle demande de connexion. Pendant son attente d'une confirmation ACK, le serveur est évidemment capable de traiter simultanément plusieurs autres tentatives de connexion, mais ses capacités n'étant pas infinies, leur nombre est limité. Si cette limite est atteinte, plus aucune connexion n'est possible.

Imaginons maintenant qu'un pirate initialise un très grand nombre de connexions, mais ne réponde jamais aux sollicitations du serveur. Ce dernier va épuiser entièrement ses ressources pour répondre à ces fausses demandes et ne sera plus capable d'accepter les connexions des utilisateurs légitimes. La machine, victime d'une attaque appelée «SYN flooding» (inondation de SYN), se retrouvera complètement paralysée.

Il est extrêmement difficile de se protéger de telles situations puisque chaque tentative de connexion, prise individuellement, ne peut être distinguée d'une demande réelle. C'est uniquement en analysant un grand nombre de connexions que la victime aura une chance de déterminer la source de l'attaque et pourra la repousser en refusant d'office toutes les demandes de la même provenance.

Malheureusement, il est relativement facile de compliquer ces techniques d'attaque pour les rendre quasiment impossibles à prévenir. Une des versions les plus menaçantes est le «déni de service distribué»: le pirate commence par s'introduire dans plusieurs ordinateurs connectés à Internet, en cherchant ceux qui présentent des failles de sécurité. Il lance ensuite une attaque coordonnée sur la même cible à partir de chacun d'eux. Attaqué par un grand nombre de sources en même temps, la victime ne peut rien faire sinon déconnecter son serveur. L'effet est semblable à celui qui se produit quand un grand nombre de personnes, sans aucune intention malveillante, décide de se

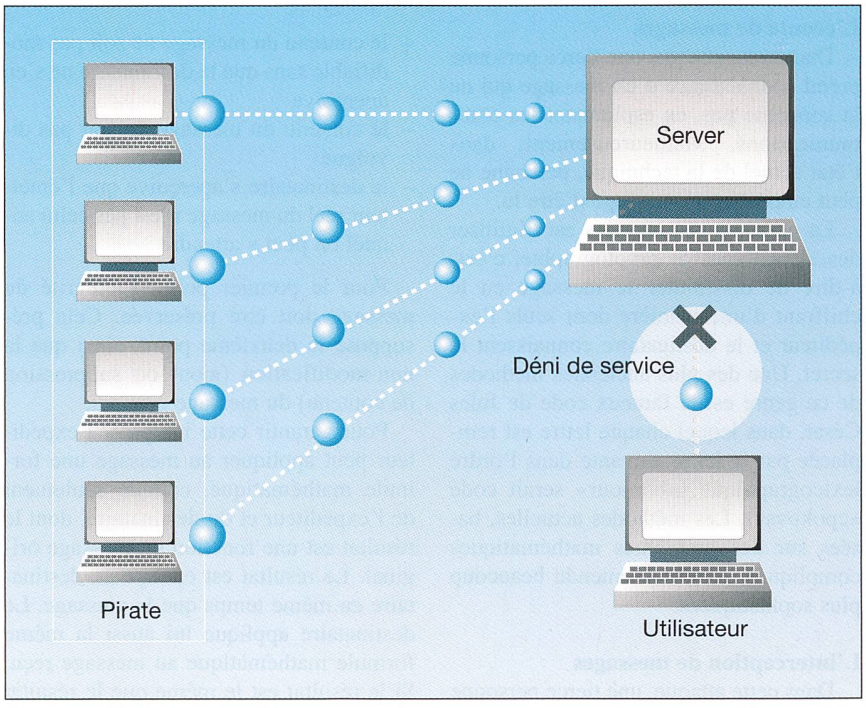

Fig. 1 Attaque de «déni de service»

Le pirate initialise un très grand nombre de connexions sans répondre aux sollicitations du serveur. Epuisé par ces demandes, le serveur n'est plus capable à répondre aux utilisateurs légitimes.

connecter en même temps au même serveur, provoquant sa surcharge et l'empêchant de répondre aux requêtes.

Ces menaces sont quasiment aussi anciennes que les protocoles de communications qui composent Internet. Qu'est-ce qui fait la nouveauté des démonstrations de ce début d'année? Il y a encore quelques mois, de telles attaques demandaient d'importantes compétences. Ce n'est plus le cas aujourd'hui: il a suffit de quelques programmeurs qualifiés mais peu scrupuleux pour distribuer des programmes d'attaques automatisées, et quelques clics de souris suffisent à des pirates en herbe même non-expérimentés pour créer de gros dégâts.

Même si le danger de telles attaques peut être relativisé par le fait qu'elles ne provoquent pas de réel dégât autre qu'une impossibilité d'accès temporaire et ne menacent aucune donnée confidentielle, elles peuvent s'avérer extrêmement problématiques vu l'importance qu'a pris l'Internet dans notre vie actuelle. Il est également possible que des attaques de déni de service servent à détourner l'attention des responsables de la sécurité pendant qu'une autre attaque, plus insidieuse, est lancée. Malheureusement, aucune bonne protection contre ces attaques n'est visible à court ou à moyen terme.

Quelles garanties peut-on avoir en matière de sécurité informatique?

L'utilisateur d'un système informatique est en général facilement capable de juger de la qualité du système, en regardant si celui-ci est efficace, simple à utiliser, et s'il produit exactement le résultat attendu. La situation est complètement différente dans le domaine de la sécurité, où deux systèmes peuvent être utilisés pendant des mois sans que l'on ne remarque une différence, alors que l'un des deux fournit une excellente protection et l'autre est totalement inefficace.

Comment peut-on donc faire la différence entre un bon et un mauvais système de sécurité? Une idée couramment répandue est que le fonctionnement d'un dispositif de sécurité doit être gardé secret sous prétexte qu'un agresseur qui ne connaît pas le système ne saurait pas comment l'attaquer. Même si cela paraît plausible, rien n'est plus faux! Dans un tel système, les faiblesses découvertes après coup sont souvent tenues secrètes et les utilisateurs légitimes ignorent qu'ils utilisent un système peu sûr. Par contre, des pirates ne seront pas arrêtés par la barrière du secret et parviendront à un moment ou à un autre à découvrir ces faiblesses et à les exploiter.

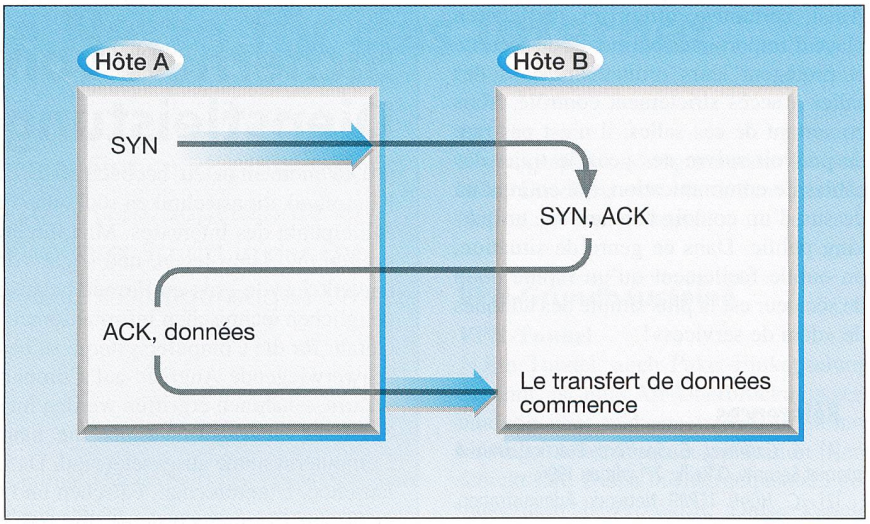

Fig. 2 Déroulement de communication, suivant le protocole TCP

Plusieurs exemples ont montré récemment que le choix du secret ne garantit aucunement la sécurité. Par exemple, le système de chiffrement des téléphones mobiles GSM, celui qui contrôle la lecture des disques DVD ainsi que le système de sécurité des cartes bancaires françaises, tous trois tenus secrets et prétendus sûrs, ont révélé d'importantes faiblesses dès qu'ils ont été rendus publics. Si dans le premier cas c'est grâce à une fuite interne que le système a été décrit, c'est uniquement suite au travail d'informaticiens externes sans intention frauduleuse que les deux autres systèmes ont été dévoilés. Une fois les données techniques de la sécurité connues, la seule réaction des constructeurs a été d'ordre judiciaire, afin de restreindre le plus possible la diffusion de l'information, ce qui ne peut pas rendre le système plus fiable.

De l'autre côté, le fait que la description d'un système de sécurité soit ouvert (public) signifiera qu'il a été conçu dès le début pour rester sûr même si son fonctionnement est connu. De plus, cette ouverture permettra de faire examiner le système en détail par un très grand nombre de personnes indépendantes, manière efficace d'obtenir de bonnes garanties de sécurité.

Dans cette optique, de nombreux programmes sont actuellement diffusés selon le modèle «open source», qui consiste à diffuser publiquement le code source. Cette manière de faire permet à chacun de l'examiner pour y trouver d'éventuels problèmes de sécurité (et de les corriger le cas échéant). Même si cela ne garantit pas une sécurité parfaite (qui n'existe pas), la correction des problèmes est beaucoup plus rapide et surtout, elle ne dépend pas des intérêts commerciaux du vendeur.

Entre un système dont la seule garantie de sécurité est la parole du vendeur, mais que personne ne peut réellement inspecter, et un autre que des centaines de personnes ont examiné, de plus en plus d'administrateurs systèmes optent pour la seconde solution. C'est une des raisons qui expliquent le succès actuel des systèmes d'exploitation tels que GNU/Linux ou OpenBSD, dont le code source est disponible et qui sont considérés comme étant beaucoup plus sûrs que des systèmes commerciaux tels que Microsoft Windows (95/98/NT/2000).

Conclusions

Comme on l'a vu, la sécurité informatique est un problème global qui doit être assuré de bout en bout, c'est-à-dire inclure dans son étude aussi bien la communication des données que leur stockage. Ainsi, l'utilisation du meilleur algorithme de cryptographie connu n'apportera aucune sécurité si l'utilisateur du système choisit «toto» comme mot de passe pour accéder aux données, ou s'il choisit un mot de passe tellement compliqué qu'il sera obligé de l'écrire sur un «post-it» collé sous son clavier. De même, l'utilisation d'un pare-feu (firewall) pour filtrer les accès provenant de l'extérieur de l'entreprise est souvent vu comme une panacée, tout en oubliant que 80% des problèmes de sécurité (que leur origine soit accidentelle ou malveillante) ont leur origine à l'intérieur de l'entreprise, où le firewall n'a aucun effet.

Dans beaucoup de cas, la sécurité physique (contrôle des accès aux machines, etc.) est souvent négligée ou incomplète.

Ainsi, certaines entreprises mettent en place d'importantes politiques de sécurité et protègent leurs ordinateurs dans des salles à accès strictement contrôlé. Mais en sortant de ces salles, il n'est pas rare de pouvoir suivre des yeux le trajet des câbles de communication, qui courent au dessus d'un couloir donnant sur un parking public. Dans ce genre de situation, on oublie facilement qu'un rapide coup de sécateur est la plus simple des attaques de «déni de services»!

Références

[1] *S. Garfinkel, G. Spafford:* Practical Unix & Internet Security. O'Reilly, 2nd edition 1996.

[2] *C. Hunt:* TCP/IP Network Administration. O'Reilly, 1997.

[3] *E. Léopold, S. Lhoste:* La sécurité informatique, que sais-je? PUF, n° 3460, 1999.

[4] *B. Schneier:* Crypto-gram. Lettre électronique d'information mensuelle sur la cryptographie et la sécurité. http://www.counterpane.com/crypto-gram.html.

[5] *Jacques Stern:* La science du secret. Editions Odile Jacob, 1998.

Sicherheit von Daten und Dienstleistungen im Internet

Die momentan zu beobachtende Entwicklung der neuen Informations- und Kommunikationstechniken rückt das Problem der Sicherheit des Internets in den Mittelpunkt des Interesses. Man fürchtet sich vor Hackern, die Internetseiten angreifen und lahm legen, und sogar vor «Spionen», die den geheimen Nachrichtenverkehr von grossen Firmen belauschen. Wenn auch die in solchen Fällen zugänglichen technischen Informationen häufig zu spärlich sind, um die tatsächliche Gefahr für die Computersysteme zu beurteilen, so besteht doch kein Zweifel, dass schwerwiegende Angriffe auf Computersysteme stattfinden und dass daher Abwehrmassnahmen ergriffen werden müssen.

Dieser Beitrag beschreibt die häufigsten Angriffsszenarien, denen heutige Computersysteme ausgesetzt sind. Dazu zählen Angriffe auf die Daten selbst (Belauschen, Unterbrechen, Fälschen und Verfälschen der Kommunikation) und Angriffe auf Computersysteme, die das Erbringen einer Dienstleistung verhindern sollen.

Der Artikel zeigt, dass die Kommunikationssicherheit nur dann richtig beurteilt wird, wenn alle Aspekte eines Computersystems berücksichtigt werden. Paradoxerweise zeichnen sich offene Systeme (Open Source) durch eine grössere Sicherheit aus als proprietäre Systeme, deren Funktionsweise von den Herstellern geheim gehalten werden.

Wie stark ist das Immunsystem Ihrer Informationstechnologie?

Auch auf dem Gebiet der IT handeln wir nach den Massstäben unseres Konzeptes TSM® Total Security Management.

Ihr Nutzen:
→ **Sie besitzen die Gewissheit, dass Ihre Daten und Informationen sicher sind**
→ **Ihr Sicherheitsstandard schafft Vertrauen**

- Integrale Sicherheit
- Sicherheitspolitik
- Sicherheitskonzepte
- Audits und Risikoanalysen
- Verfahren/Methoden zur Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität
- Internet-Sicherheit und -Recht
- Technische und juristische Expertisen

SEV ASE **Kontaktpersonen:**

Oliver Bärtsch
Tel. 01 956 13 80
Fax 01 956 13 08
oliver.baertsch@sev.ch

Roland Iseli
Tel. 01 956 13 31
Fax 01 956 14 01
roland.iseli@sev.ch

Dr. Werner Borer
Tel. 01 956 13 32
Fax 01 956 14 01
werner.borer@sev.ch