Sécurité

NAT – PAT, FW, Crypto, DoS, Virus, Spyware…

Sécurité – Buts

- Détecter les intrus (intruders, hackers, attackers…)
- Les empêcher de réaliser leurs noirs desseins

Sécurité – Pour quoi faire ?

- Lecture de données confidentielles
- Modification de données
- Ajout de fausses données
- Transactions bancaires (!) – espace disque (sites FTP)
- Le cas des routeurs: Lecture de RT, Modification de RT, Etablissement de peers…
- ADSL - câble: attention !

Sécurité – Type d'attaques contre les mots de passe

- Deviner (Madame Soleil / mot de passe sur un post-it / le nom des enfants…)
- Voler / Analyser le trafic
- Force brute (préférence pour un dictionnaire)
- Attention au nombre de possibilités (en fonction du nombre de symboles utilisés et du nombre de possibilités par symbole):

	1 sb	**2 sb**	**5 sb**	**7 sb**	**10 sb**
26	26	676	11881376	8031810176	141167095653376
36	36	1296	60466176	78364164096	3656158440062976
50	50	2500	312500000	781250000000	97656250000000000 (97 millions de milliards)

Sécurité: mot de passe 'fort'

Un mot de passe 'fort':

- A au moins 14 caractères;
- Contient des majuscules;
- Contient des minuscules;
- Contient des chiffres;
- Contient des symboles, tels que ` ! " ? $? % ^ & * ( ) _ - + = { [}] : ; @ ' ~ # | \ < , > . ? /
- Ne ressemble pas à vos mots de passe précédents;
- Ne contient pas votre nom et / ou prénom;
- N'est pas votre login;
- N'est pas le nom d'un ami(e);
- N'est pas le nom d'un membre de votre famille;
- N'est pas un mot du dictionnaire;
- N'est pas un nom 'classique'.

Exemple: Rfl5!32lROpo02?-Aa

Sécurité: Attention !

Lu dans un journal perfide, le 26/4/04:

172 navetteurs londoniens se sont vu offrir une barre de chocolat s'ils donnaient le mot de passe qui leur permet de se connecter au réseau informatique de leur société.

37% ont accepté immédiatement le deal. Et 34 autres % ont accepté après que leur interlocuteur leur a dit que leur mot de passe était soit le nom de leur animal domestique soit le prénom d'un de leurs enfants.

L'enquête était réalisée pour les organisateurs d'un salon sur la sécurité informatique. Les résultats sont concluants: pour hacker un système informatique, plus besoin de fureter sur le web à la recherche d'un logiciel perfectionné. Une barre de chocolat suffit !

Sécurité – Routeurs

- Les attaques les plus classiques sur des routeurs sont:
  - Accès non autorisé (mot de passe)
  - Reroutage
  - DoS
  - Renvoi d'une session (éventuellement modifiée)
  - Modification de configuration via SNMP
  - Sécurité physique (accès à la console)

NAT

- Network Address Translation
- Avantage:
  - permet d'utiliser une seule (ou plusieurs) adresse(s) publique(s) pour plusieurs machines
  - offre plus de sécurité
- Désavantage: casse l'idée de bout en bout !
- Peut influencer la couche application, si elle ne respecte pas le modèle ISO – OSI

Les différents types de NATing

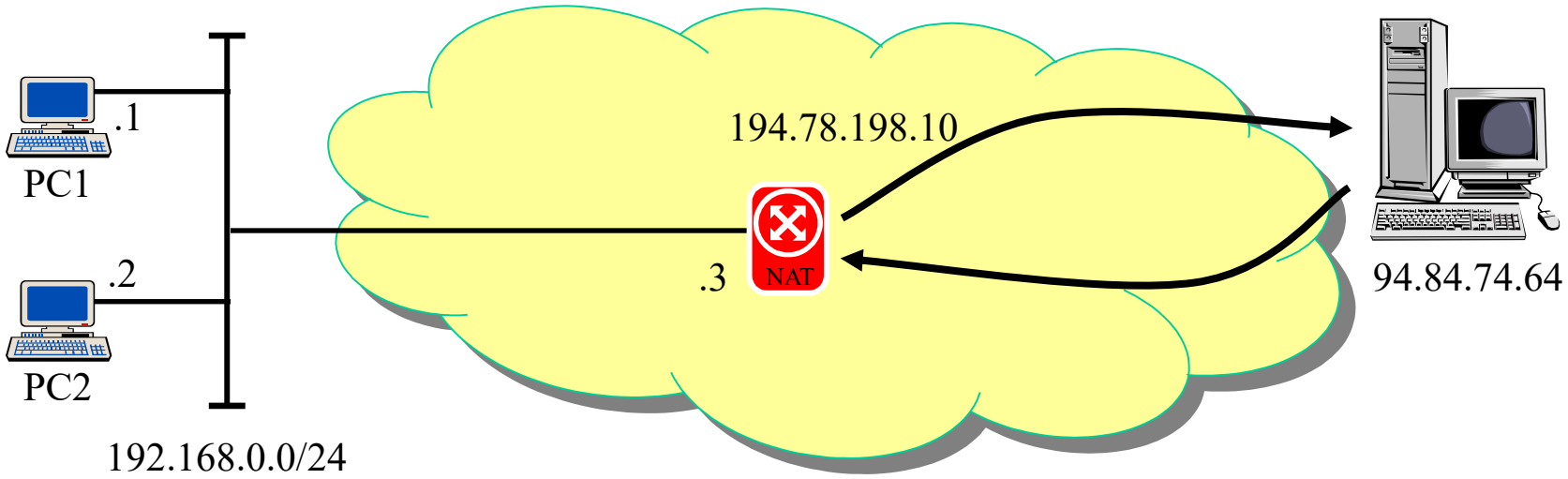
- Statique – N to N
- Dynamique – M to N
- Single – N to 1 (masquerading / overloading / PAT / NAPT)
- Sans PAT, le nombre de machines accédant à l'extérieur simultanément limité par le nombre d'adresses IP publiques disponibles

NAT – PAT – Exemple

Adresse source	Adresse destination	Porte source	Porte destination	Nouvelle adresse source	Nouvelle adresse destination	Nouvelle porte source	Nouvelle porte destination
192.168.0.1	94.84.74.64	1282	80	**194.78.198.10**	94.84.74.64	**2000**	80
192.168.0.2	94.84.74.64	1282	80	**194.78.198.10**	94.84.74.64	**2001**	80
94.84.74.64	192.168.0.1	80	1282	94.84.74.64	**194.78.198.10**	80	**2000**
94.84.74.64	192.168.0.2	80	1282	94.84.74.64	**194.78.198.10**	80	**2001**

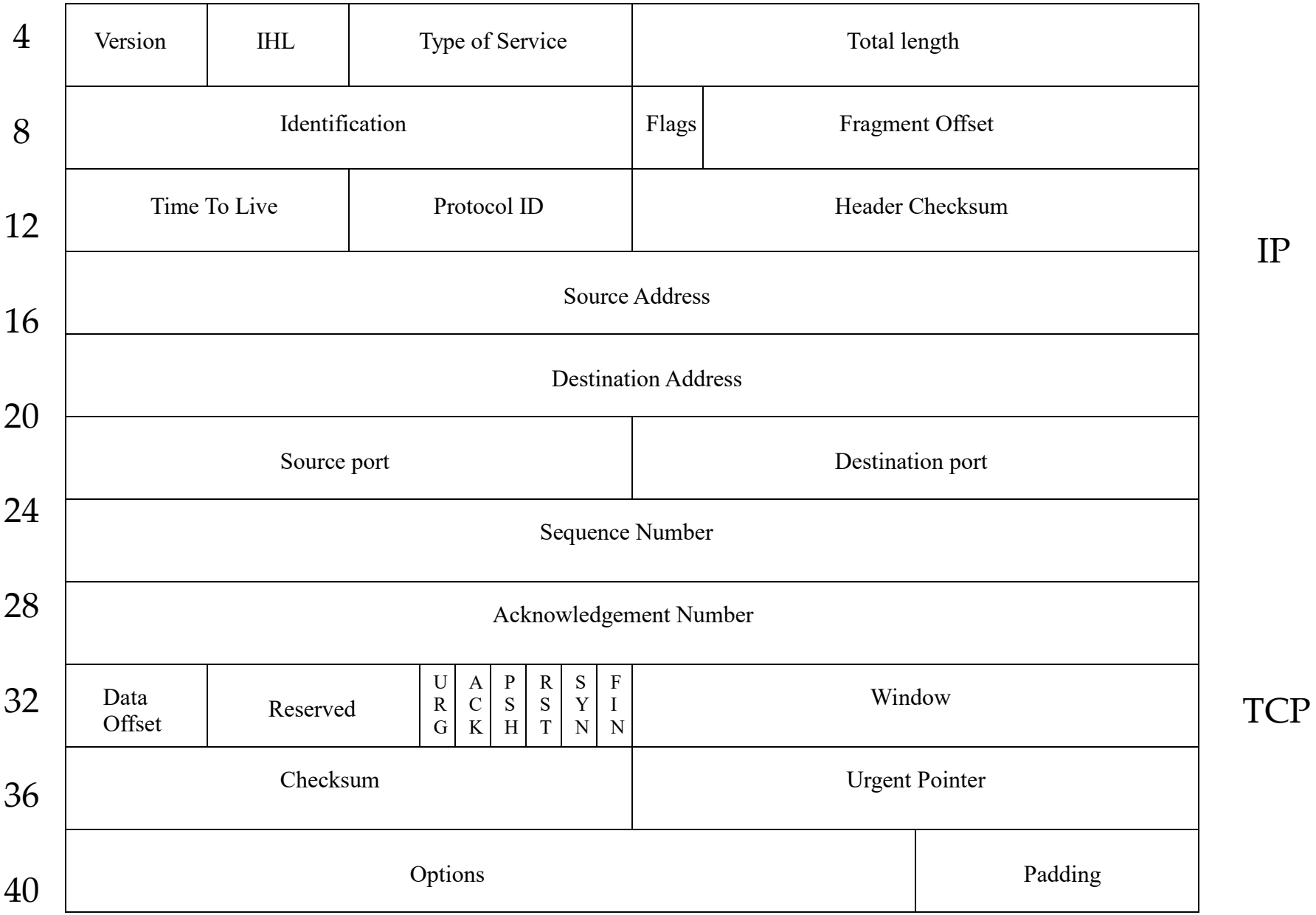
NAT

PAT



Filtres dans les routeurs

- Filtrage du trafic
- Basé sur les X (60) premiers bytes du paquet IP (par exemple)
- Permet d'assigner des priorités… ou de jeter le paquet !
- Cf Access List
  - access-list 20 permit 10.1.2.0 255.255.255.0


4
8
12
16
20
24
28
32
36
40
44
Version
IHL
Type of Service
Total length
Identification
Flags
Fragment Offset
Time To Live
Protocol ID
Header Checksum
Source Address
Destination Address
Source port
Destination port
Sequence Number
Acknowledgement Number
Data Offset
Reserved
URG
ACK
PSH
RST
SYN
FIN
Window
Checksum
Urgent Pointer
Options
Padding
IP
TCP

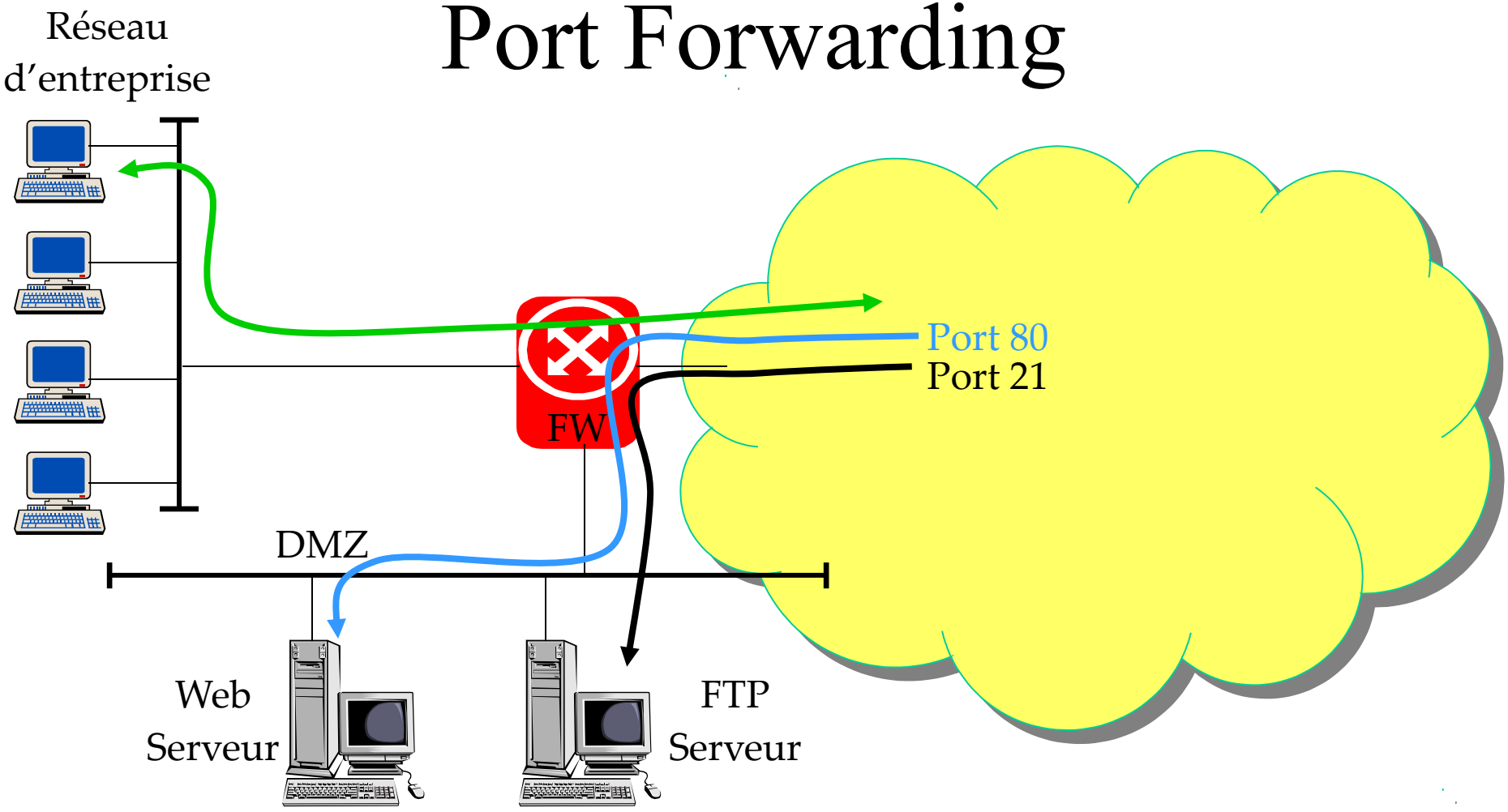
Firewall

- Différence avec des filtres d'un routeur ?
- Mise en relation de différents paquets du trafic
- Configurable, mais bloque le trafic entrant par défaut
- Possibilité de DMZ
- Possibilité de NAT
- FTP: 2 canaux (mais de plus en plus intelligents).
- Effets indésirables

Firewall – Exemple

Règle	Action	IP Source	IP Dest	Protocol	Port Source	Port Dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

Firewall – Exemple
Port Forwarding



Firewall – Statefull

- Examen des paquets et mises en relation entre le niveau 3 et 4 (et parfois 7).

Proxy

- Permet de n'accepter le trafic entrant que vers une machine particulière
- Permet à l'entreprise de contrôler les sites (ou les adresses) vers lesquels sont envoyées les requêtes
- Peut également permettre de s'anonymiser (loi Hadopi)
- Exemples:
  - Web, Mail, FTP, RTP, SIP …

Cryptographie

- Qu'est-ce que c'est: la science (basée sur des math) qui développe des techniques d'encryption et de décryption d'information
- La cryptanalyse permet (essaie) de déchifrer des messages cryptés (raisonnement analytique, outils mathématiques, recherche de patterns, patience, chance…)
- Cryptologie: cryptographie + cryptanalyse
- De base (Jules César …)
- Avancée (RSA …)

Cryptographie – Pourquoi ?

- Pour pouvoir envoyer un message à travers un canal non fiable… (un messager, un courrier, l'Internet…)

- Rien n'est prouvé ! Il suffit d'encrypter de manière suffisamment complexe pour qu'au moment où le message est lu, l'information ne soit plus valide !!!

Cryptographie – Comment ?

- Il faut encrypter un TEXTE CLAIR à l'aide d'une CLE pour le transformer en TEXTE CRYPTE

- La sécurité dépend donc de l'algorithme d'encryption ET de la clé

Cryptographie – Types

- Algorithmes symétriques
  - Introduit par Jules César
  - Une seule clé. Si l'attaquant trouve la clé…
  - DES, 3DES
  - Problème: comment communiquer la clé ??? C'est le problème de la méthode à utiliser pour distribuer les clés..
- Algorithmes asymétriques
  - Introduit par Diffie et Hellman
  - La clé (publique) est publique !
  - RSA
  - Problème: complexité

PGP

- Pretty Good Privacy (Phil Zimmermann, 1991)
- Standard de facto pour l'encryption des mails
- Etapes :
  - Création et échange des clés
  - Ecriture du mail (sous forme d'un texte)
  - Encryption du texte – production du fichier crypté
  - Envoi du texte en attachement
  - Réception du mail
  - Décryption du fichier attaché et crypté
  - Lecture
- Système hybride:
  - compression (pour éviter les patterns)
  - clé publique

Encryption – clé publique – principe mathématique

- Idée de base: avoir une paire de clé (fonction mathématique); une publique (F) et une privée (P), qui sont complémentaires.
- Soit X un message quelconque
- On veut que P(F(X)) = X
- Dans ce cas, on peut prendre un message X, l'encoder à l'aide de la fonction F du destinataire (que tout le monde connaît) et lui envoyer
- Le destinataire est le seul à connaître P et à pouvoir retrouver le message original puisque P(F(X)) = X
- Donc, plus de problème de distribution de clés !

Encryption – clé publique – signature

- En plus, on peut signer ses messages si F(P(X)) = X
- En effet, on peut prendre la clé privée de l'émetteur (Pe), et la clé publique du récepteur (Fr)
- Comme précédemment, on calcule Fr(X)
- Avant de l'envoyer, on la crypte encore une fois avec Pe. On envoie donc Pe(Fr(X))
- Le récepteur reçoit le message doublement crypté.
- Il applique la fonction Fe (clé publique de l'émetteur) à ce qu'il a reçu. Il calcule donc Fe(Pe(Fr(X))). Il trouve donc Fr(X).
- Il ne lui reste qu'à appliquer, comme précédemment, sa propre clé privée (PR). Il calcule donc Pr(Fr(X)) et il obtient… X !

Clé publique – RSA

- Rivest – Shamir – Adelman
- Idée: clé publique (cf théorie), en utilisant 2 grands nombre premiers, et en se basant sur le fait qu'un nombre n'est pas facilement factorisable, pq=m, m est la première partie de la clé publique
- On choisit un nombre e, premier avec (p-1)(q-1). On publie m et e (qui forment l'ensemble de la clé publique). C'est la deuxième partie de la clé publique.
- On publie (e mod m). C'est la clé publique.

Clé publique – RSA (suite) Référence

- Il faut maintenant calculer la clé de déchiffrement, d: d*e=1(mod(p-1)*(q-1))
- C'est la clé privée, incalculable sans connaître p et q !
- Pour encrypter le message, l'émetteur calcule C = M ^ (e mod m) (c'est la fonction F)
- Pour décrypter le message crypté, le récepteur calcule M = C ^ (d mod m) !!! (c'est la fonction P)

Encryption

- IKE
- MD5
- RSA
- DES: Data Encryption Standard (56 bits).
  De l'ordre du jour
- 3DES: Triple DES (168 bits)
  De l'ordre de milliards d'années pour les machines des années 2000 !!!

IKE

- Internet Key Exchange
- Permet de:
  - Négocier un protocole, algorithme et clés (dynamiquement)
  - Authentifier les correspondants
  - Echanger les clés de manière sécurisée
  - Gérer les clés, une fois échangées

MD5

- Message Digest 5
- Développé by Rivest (RSA)
- RFC 1321
- Signature digitale: L'algorithme part d'un message d'une longueur quelconque et produit une 'empreinte digitale' de 128 bits
- Utilisé par exemple pour confirmer qu'un fichier a été bien transmis
- Encryption d'un mot de passe dans une DB

MD5 – Reverse Engineering

- Il existe des sites qui collectionnent plusieurs milliers de mots de passe encryptés (entre 105 Mille et 43 Milliards, nov 2013)
- N'utilisez pas ces sites pour encrypter !
- Rajouter un salt dans votre algo d'encryption !

IP / Mac Spoofing

- Idée, envoyer des paquets à partir d'une machine, en utilisant l'adresse IP / Mac d'une autre machine, qui a plus de droits…
- On peut en effet vouloir permettre ou protéger les utilisateurs d'accéder ou pas à certains services (par exemple)
- Protection: VPN

Phishing

- But: soutirer des informations confidentielles à une victime consentante (voir plus loin, les ISPs) !
- Méthode: l'attaquant envoie un mail à la victime, en se faisant passer pour une organisation avec laquelle la victime est liée (banque, carde de crédit ...). Le mail renvoie la victime vers un site web, soi-disant mis à disposition de l'utilisateur par l'organisation. Là, l'utilisateur est averti qu'un problème informatique (elle a bon dos) est à l'origine d'une perte de données et que l'utilisateur doit réintroduire ces informations confidentielles (nom, num. de carte de crédit, informations médicales...)
- Protection: éducation des utilisateurs, utilisation de son cerveau, méfiance !

Phising – Exemple

Dear valued customer

We regret to inform you that your BankofAmerica account could be suspended if you don't re-update your account information. To resolve this problems please click here and re-enter your account information. If your problems could not be resolved your ac unt will be suspended for a period of 1-2 days, after this period yo r the User Agreement, Section 9, we may immediately is nd, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us. Due to the suspension of this account, please be advised you are prohibited from using BankofAmerica in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to BankofAmerica.

http://wprejnjjoriknprith.com/index.html

Regards,Safeharbor Department BankofAmerica , Inc
The BankofAmerica team
This is an automatic message. Please do not reply.

Phising - Exemple

Cher Monsieur,

Nous sommes très reconnaissants envers vous visitez notre site Web du projet. Site Web: www.keply.eu.kz

Êtes-vous intéressé à notre projet faire? Voulez-vous l'acheter?

La société peut vous fournir besoin de chaussures, sacs, pantalons,

Les prix entreprise attrayante, la variété des marchandises pour votre sélection.

s'il vous plaît profiter de votre temps libre de faire attention à ce site.

Meilleurs voeux à toi!

/2/8/c/Q

Phising bancaire

- Site non sécurisé
- Informations confidentielles demandées par téléphone
- Contact téléphonique anonyme !
- La démarche vient d'eux !
- Utilisez votre cerveau !!!

DoS attacks

- Idée: donner suffisamment de travail au device pour qu'il ne puisse plus fonctionner correctement (ICMP en rafale… Smurf attack)
- Surtout sur des mails server, web servers
- Amélioration (?): DDoS !

Exploits

- Caractéristiques ‘imprévues’ de certains programmes … voire bugs !
- Utilisés par les hackers pour réaliser des opérations que le programme peut faire, mais pas l’utilisateur…
- Généralement résolus par des fixes

Exploits – Exemple 1

- 13 Jan 04: MS Website: 'Buffer Overrun in MDAC Function Could Allow Code Execution'

Microsoft Data Access Components (MDAC) is a collection of components that provides the underlying functionality for a number of database operations, such as connecting to remote databases and returning data to a client. When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. Because of a vulnerability in a specific MDAC component, an attacker could respond to this request with a specially-crafted packet that could cause a buffer overflow.

An attacker who successfully exploited this vulnerability could gain the same level of privileges over the system as the program that initiated the broadcast request. The actions an attacker could carry out would be dependent on the permissions under which the program using MDAC ran. If the program ran with limited privileges, an attacker would be limited accordingly; however, if the program ran under the local system context, the attacker would have the same level of permissions.

Exploits – Exemple 2

- Sep. 04: MS Website: Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)

A buffer overrun vulnerability exists in the processing of JPEG image formats that could allow remote code execution on an affected system. Any program that processes JPEG images on the affected systems could be vulnerable to this attack, and any system that uses the affected programs or components could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Exploits et sécurité: les backdoors

- Il s'agit d'une porte d'entrée dans le code qui permet de faire des choses... non documentées (undocumented features)
- Version soft: 'Easter Eggs'
- Mis en lumière par Huawei et ZTE (été 2012): gros stress par rapport à de prétendues backdoors dans les équipements de switching téléphonique

Backdoors

- Espionnage industriel ? Contrôle des concurrents ? Huawei, encore.
- Existence avec certains produits MS ? MS dit que non, mais le code n'est pas dispo... Et quid des lois ?
- La NSA demande à Torvalds de mettre des backdoors dans Linux !
  'The father of Linus Torvalds has confirmed that the NSA wanted a backdoor in Linux !' Nov 2013. Source ITWorld.
- Voir discussion au Parlement Européen du 11 novembre (Youtube)

Backdoors dans Linux ?

- "When my oldest son [Linus Torvalds] was asked the same question: 'Has he been approached by the NSA about backdoors?' he said 'No', but at the same time he nodded. Then he was sort of in the legal free. He had given the right answer, [but] everybody understood that the NSA had approached him". Nils Torvalds, Parlement Europeen, 11 Novembre 2013.

Bug fixing: à jour ?

- Novembre 2014:Microsoft a résolu un bug présent dans Windows depuis 19 ans - depuis Windows 95 - et qui permettait en principe à des personnes malveillantes de prendre le contrôle d'un ordinateur à distance.
- ‘Les utilisateurs qui ont paramétré leur Windows de telle manière à recevoir automatiquement les mises à jour, ne doivent rien faire de particulier. Ils seront protégés', assure un porte-parole de Microsoft.

Espionnage

- Octobre 2013: les Etats Unis avouent espionner plusieurs dirigeants européens (Merckel, Hollande, Di Rupo...)
- Ils se justifient en disant que... tout le monde le fait !
- Voir le fichier Sip-trace-sample.cap

Cybercriminalité

Datanews, le 28/11/2014:

Technique	Coût (en €)	Gain (estimé) (en € pour 100 victimes)
Phising	120	8.000
Cheval de Troie	800	16.000
Ransomware	1.600	16.000
Cheval de Troie bancaire	2.400	58.000

Géolocalisation

- Datanews, le 2/12/2014:

  ‘...à partir du 1er janvier, l'utilisateur que vous êtes, concédera à Facebook la permission d'utiliser votre GPS, Bluetooth et wifi pour déterminer votre emplacement. Cela donnera au réseau social la possibilité de mieux cibler ses publicités, en liaison par exemple avec une ville ou un magasin proche. Il n'y a pas de choix possible sur ce plan’.

Virus

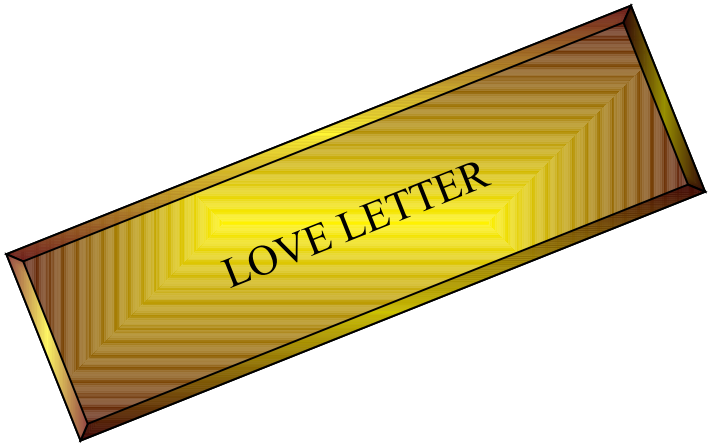
- Programmes (exécutables)!
- Pas de virus dans un mail, mais bien dans un fichier attaché (.exe, .scr, .doc, .xls, .mdb, .vbs …)
- Antivirus gratuit sur le web
- Caractéristiques: petits, auto-répliquants, pas visibles immédiatement, comportement imprévu, automodifiant …

Virus en chiffres

- « *Chaque mois, 600 nouveaux virus font leur apparition sur le Net (20 par jour en moyenne).* » Skynet, 26/3/2002.
- Norton Antivirus:
  - 62.507 virus connus le 7/12/2002.
  - 63.111 virus connus le 22/2/2003.
  - plus de 73.000 le 25/10/2007.
- Même si c'est exagéré, cela montre bien la tendance !
- 80% des virus se propagent et infectent les machines des clients via le mail.

Virus

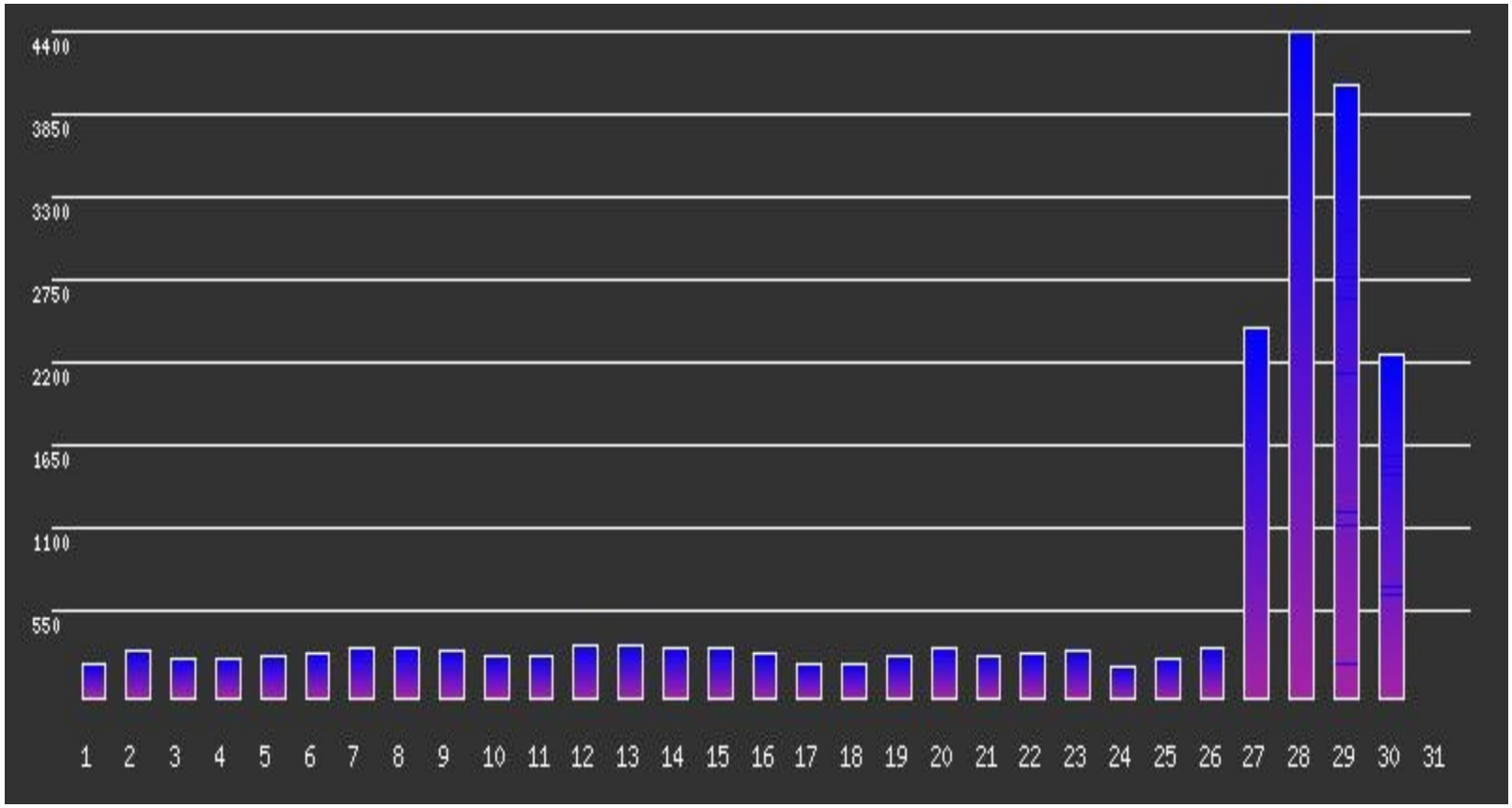
- Exemple: I LOVE YOU…
- A empoisonné des milliers (millions) de boites aux lettres
- Basé sur des faiblesses d'architecture de MS…



Virus et DDoS

- « Samedi 25 janvier 2003, 06 heures 30 du matin, une attaque lancée par un ou plusieurs groupes pirates commence à perturber l'Internet via un DDoS mis en place par un virus SQL nommé Saphhire »
- Il a été lancé à partir de plusieurs milliers de machines, exploitant une faille du SQL server de Microsoft.
- Résultat, des quantités de DNS inaccessibles, et des millions d'internautes touchés… Un quasi arrêt de l'Internet pendant quelques heures…

Virus: MyDoom aka Novarg.



Le graphique de l'Antivirus d'un gros ISP, janvier 2004

MegaUpload est fermé !!!

- Le 19 janvier 2012, le FBI décide de fermer le site de partage de fichier MegaUpload.com.
- Le groupe de hackers Anonymous décide de contre-attaquer en faisant une immense DDOS (entre autres) avec des gens volontaires téléchargeant un petit soft) visant les sites, entre autres, du FBI, du DoJ, de la RIAA (Recording Industry Association of America) et MIAA, de Sony, et de différents Majors.
- Anonymous parle, sur YouTube, de la première guerre cybernétique. A vos consciences, citoyens...
- Résultat: plusieurs sites hackés, piratés, inaccessibles durant des jours. Le site de Sony diffuse TOUT son contenu gratuitement pendant des jours !

Spywares

- Pas vraiment des virus, mais en possèdent certaines caractéristiques.
- Collectent des données sur votre machine et les envoie à un serveur
- Nécessitent généralement un ‘Antispyware’... (le meilleur étant... Pas IE !)

Les ISPs

- Le géant américain Google scanne le contenu des courriels sur son service de messagerie, « pour protéger les consommateurs des spams, des virus », mais aussi « pour cibler les publicités en se basant sur le contenu des mails », reconnaît un de ses juristes, Peter Fleischer. Les informations collectées permettent en effet des publicités « sur-mesure ». Le Soir, 22 Janvier 2008 !

Spamming en chiffres

- Le Soir du 4/10/2010: “Selon le dossier d’accusation, Oleg Nikolaïenko contrôlait un réseau de 500.000 ordinateurs infectés via lesquels il pouvait envoyer chaque jour 10 milliards de pourriels dans le monde entier. Il était en échange rémunéré par des services proposant de vendre des fausses montres de luxe ou des médicaments contrefaisant par exemple le Viagra.”
- Marché porteur ! Voir Virus et chevaux de Troie...
- Si on estime que 1 pour dix mille des spams est porteur, en envoyant 10 milliards de mails par jour, le Mr Nikolaienko reçoit chaque jour 10^{10} / 10^4 = 1 million de clients par jour !!!

Hoaxes

- Ou Scams ou canulars...
- Fausse information, déguisée sous l'aspect d'une vraie, généralement basée sur la bonne volonté et l'envie de bien faire du gogo...
- Problématique pour les mails serveurs

BYOD

- Nouvelle problèmatique: comment sécuriser le réseau et l'infrastructure en laissant n'importe quel device s'y connecter ?

Les réseaux sociaux

- Quand on fait une publication sur les réseaux sociaux, il peut y avoir des conséquences... inattendues:
  - Taxes (une bonne journée de boulot alors qu'on ne travaille pas)
  - Congés (Chouette parcours sur les pistes alors qu'on est en congé de maladie)
  - Effet pervers de la médisance (allant jusqu'à la mort :-()

Film !

- 13 minutes
- Anglais
- Ericsson
- Mentalité américaine
- Pas toujours complètement exact…

- … mais amusant !

Film