La Sécurité des Systèmes d'Information : la cryptographie démystifiée

Conférence du 08/06/09, à la maison des Arts et Métiers

Cette conférence a été organisée conjointement par l'EM Lyon Alumni Club NTIC, l'AIN7 et le groupe Informatique et Télécom Arts et Métiers Paristech.

Ordre du jour

A l'ère du tout numérique et du tout internet, nos informations sont-elles bien sécurisées ? Les techniques mises en œuvre pour le secteur militaire, l'industrie ou le grand public sont-elles si différentes ? Les solutions de chiffrement, parfois complexes et lourdes, sont-elles toujours adaptées aux besoins opérationnels ?

Jean-Pierre Lamoitier, néophyte mais arithméticien amateur, et Philippe Painchault, responsable des solutions de Sécurité SI chez Thalès, avaient pour objectif de nous initier à la science des messages secrets. Olivier Bidot nous a ensuite présenté les spécificités liées à l'aéronautique militaire. Enfin Jacques Pantin a élargi les horizons du champ d'application à la signature électronique sur le web et les procédures mises en œuvre pour conférer une valeur légale à un document transmis par Internet.

Le débat a été animé par Maryse Lemmet, précédemment responsable SSI à EDF.

Remerciements

Aux conférenciers :

- Olivier Bidot, Ingénieur SSI à la DGA – domaine aéronautique
- Jean-Pierre Lamoitier, Ingénieur Arts et Métiers et mathématicien
- Philippe Painchault, responsable des solutions SSI chez Thalès
- Jacques Pantin, PDG de Dictao

Aux organisateurs :

- Maryse Lemmet et Eric Nizard pour l'AIN7
- Pierre Dumolard pour l'EM Lyon Alumni Club NTIC
- Valentine Ferréol pour le groupe Informatique et Télécom Arts et Métiers Paristech

Introduction

Le SI est maintenant au cœur des entreprises, à la fois support et moteur de notre industrie, de notre commerce, de notre administration, bref au cœur de notre façon de vivre. Dans la vie de tous les jours, la dématérialisation, les échanges, le tout numérique font que chacun est de plus en plus dépendant des outils mis à sa disposition : suivi et transactions bancaires, déclaration d'impôts, achats en ligne, ..etc

S'il en était besoin, des événements récents sont là pour nous le prouver. Que le SI défaille et c'est toute une machine, une chaine de production, une entreprise, un secteur d'activité qui s'arrête ! Dans ce contexte, il est naturel de prendre les mesures pour sécuriser le SI au juste niveau : c'est ce qu'on entend résoudre par la sécurité du SI.

Ce sujet de la SSI, très vaste, nous vous proposons ce soir une 1ère approche centrée sur la brique de base que représente le chiffrement.

Vous le savez, la SSI s'intéresse aux critères de DICT des informations (disponibilité, intégrité, confidentialité et traçabilité). Le chiffrement est vieux comme le monde, c'est un jeu d'enfant très commun, il a précédé l'ère du numérique. Mais c'est avec le numérique qu'il est devenu de plus en plus sophistiqué et surtout qu'il est devenu omniprésent.

NDLR : La cryptologie englobe la cryptologie (l'écriture secrète) et la cryptanalyse (l'analyse de cette dernière).

Bases mathématiques – J-P. Lamoitier

Jean-Pierre nous a présenté avec beaucoup de passion les bases mathématiques, fondements de la cryptologie (science du chiffrement).

La cryptographie est en effet basée sur des principes mathématiques permettant la résolution de problèmes à partir des nombres entiers. L'objectif est bien de transformer un message 'clair' en un message chiffré dont l'algorithme et le chiffrement sont tels que les moyens à mettre en œuvre pour retrouver le message clair soient hors de portée d'un « attaquant ».

En fait on cherche des nombres qui sont soit premiers soit presque premiers donc difficiles à factoriser. Les techniques de factorisation permettent quant à elles de « casser le code secret »

Ont été présentés les principes et les propriétés des nombres premiers tels que l'identité de Bezout (ou Bachet de Méziriac), la méthode de la descente infinie le petit théorème de Fermat.

L'arithmétique classique s'intéresse aux entiers naturels (la suite des nombres premiers est illimitée !), plus particulièrement aux nombres figurés, aux nombres parfaits au grand théorème de Fermat et aux équations diophantiennes.

Equations diophantiennes : pour résoudre une équation du type : $ax + by = c.$
D'après l'identité de Bezout : si a et b sont premiers entre eux, il existe u et v tels que $au + bv = 1$

L'arithmétique modulaire contrairement à l'arithmétique classique ne travaille plus sur des nombres mais sur des classes d'équivalence.

Jean-Pierre nous a ensuite présenté les principales fonctions arithmétiques et les logarithmes discrets.

Les techniques anciennes (utilisées du temps de Jules César) sont basées sur la transposition de caractères ou sur la transposition de petits blocs.

Les techniques modernes utilisent soit une clé secrète (dite symétrique) soit une clé publique (dite asymétrique) ; la clé secrète est remise à un porteur dépositaire alors que la clé publique est conservée par l'émetteur.

Logarithmes discrets : *k* est le logarithme discret de *a* en base *g* si $gk = a$ modulo *p.*
Ce logarithme est qualifié de discret car il ne prend que des valeurs entières et en utilisant des chiffres élevés (a et g avec plusieurs dizaines de chiffres) les équations sont très difficiles à résoudre.
Les pseudo-premiers quant à eux sont le produit de 2 GRANDS nombres premiers.

Principe de RSA : soient *p* et *q* deux nombres premiers. Nous calculons $n = pq$. Si l'entier *e* est premier avec le nombre $(p - 1)(q - 1)$, alors il existe un entier $d > 0$ tel que : $ed \equiv 1 \bmod (p - 1)(q - 1)$ et tel que pour tout nombre entier a premier avec n, nous aurons $aed \equiv a \bmod n$.

Jusqu'en 2006, la taille de clé préconisée par la DCSSI était de 512 bit ou plus (154 chiffres décimaux). Aujourd'hui la taille préconisée est d'au moins 768 bit (si possible 1024 bit).

Il existe maintenant des processeurs effectuant très rapidement des opérations en arithmétique modulaire y compris sur des entiers longs. Il est d'ailleurs maintenant question d'intégrer ces processeurs dans des cartes à puces…

Typologies des solutions et des usages – P.Painchault

La cryptologie est une science très ancienne qui s'est développée dès l'antiquité en Chine, en Egypte et en Inde. Il faut ensuite attendre la Renaissance pour voir apparaître les chiffres polyalphabétiques (principe simple de substitution) et la méthode de transposition par blocs. C'est au XVIIe siècle que la France se dote d'un service d'Etat dédié à la cryptographie et prend ainsi l'avantage contre les Anglais.

Cette science, négligée par Napoléon, sort du domaine strictement militaire au début du XIXe siècle pour être utilisée par les civils (exemple d'ouvrages de G.Sand). La cryptographie a joué un rôle décisif durant la 2ème Guerre Mondiale, avec en particulier le Télégramme de Zimmermann qui fut décrypté et le code Navajo qui ne le fut pas !

La cryptographie moderne a pris son essor avec les évolutions de l'Informatique. En effet, le traitement et la mise en œuvre d'algorithmes complexes tels que RSA et les logarithmes discrets, sont devenus possibles avec les avancées Informatiques.

Les domaines d'application vont de la confidentialité, à l'authentification et l'intégrité des messages. La sécurisation et l'intégrité correspondent à des besoins distincts et pouvant être contradictoires : le chiffrement peut avoir pour conséquence d'altérer le message initial.

Une des préoccupations de base de la cryptographie est la gestion des clés : la génération (nécessité de suites aléatoires, de nombres particuliers) et distribution de celles-ci (certifications, échanges de clés, protocoles d'échanges). Les usages se sont généralisés avec les avancées des technologies numériques (transactions bancaires, protection de données informatiques, services mobiles…).

On distingue la cryptographie à clé symétrique à clé secrète, de la cryptographie asymétrique à clé publique permettant le chiffrement ou privée permettant le déchiffrement. Pour la cryptographie symétrique, le message est découpé en blocs qui sont ensuite chiffrés soit en utilisant la même clé (méthode ECB) soit en utilisant la méthode CBC (chaînée). Avec un bon algorithme et des tailles de clés suffisantes, la seule attaque possible est de parcourir l'intégralité de l'espace des clés.

La cryptographie asymétrique est utilisée pour le chiffrement mais également pour assurer l'authenticité d'un message. Elle est basée sur la factorisation des nombres via le principe de RSA (depuis 1978) ou via les logarithmes discrets. L'algorithme RSA nécessite de grandes puissances de calcul, la gestion de bibliothèques de calculs de nombres premiers. Toutefois, en utilisant les logarithmes discrets, avec par exemple des courbes elliptiques, la taille des clés peut être considérablement réduite.

Souvent le chiffrement est une combinaison des 2 approches : symétrique et asymétrique. La diffusion des clés se fait par chiffrement asymétrique et la transmission des données se fait avec un chiffrement symétrique.

La cryptographie est en évolution permanente tant sur le plan de la recherche (il n'existe actuellement pas de preuve de sécurité des techniques de chiffrement utilisées) que sur la définition de standards ou de nouvelles techniques telles que la cryptologie quantique.

Application aux aéronefs de la DGA – O .Bidot

Olivier nous a dressé un tour d'horizon des différentes missions de la DGA, 1er investisseur de l'Etat, la part d'investissement par typologie d'activité et les domaines d'application concernés : préparer le futur, équiper les forces armées et promouvoir les exportations.

L'enjeu de la cryptographie se situe à la fois sur le plan national et international (exemple des missions interalliées dans le cadre de l'OTAN). Dans un cas comme dans l'autre la volonté française est d'être indépendante et autonome, afin de préserver notre liberté de décision et d'action pour typiquement la protection les données de renseignement.

En moyenne chaque aéronef contient 4 types d'équipements cryptographiques. Le traitement de l'obsolescence des équipements et des algorithmes représente une activité qualifiée de critique et sur laquelle il est nécessaire de prévoir des investissements à long terme.

Olivier nous a ensuite présenté les principaux types d'aéronefs de l'armée de Terre, de l'armée de l'Air et de la Marine ainsi que les spécificités liées à leur utilisation : les hélicoptères et drones, les avions de combats, dont certains pouvant être équipés d'armes nucléaires, les avions de transport dont l'avion Présidentiel, les avions spéciaux (ATL2) tels que ceux utilisés actuellement pour rechercher l'épave et les corps disparus au cours du vol AF 747.

L'objectif est de développer des équipements de confiance, intégrés dans des systèmes d'information opérationnels ou systèmes d'armes qui puissent être homologués, selon les référentiels réglementaires Français ou OTAN. Les spécifications portent sur la Confidentialité, l'Intégrité, la Disponibilité et la Preuve d'Origine. Un agrément DCSSI est recherché pour les produits de sécurité. Une homologation sous-tend l'acceptation du risque résiduel mis en évidence puis devant être accepté par une autorité qualifiée.

Les exigences en termes de Sécurité des Systèmes embarqués sont encore plus élevées pour les drones et satellites, du fait que ces équipements doivent être autonomes. L'événement type redouté que l'on étudie alors est une prise de contrôle, hostile, à distance.

Nous avons ensuite détaillé plus particulièrement les équipements de chiffrement de phonie et data mis en œuvre à bord des aéronefs et les principes de fonctionnement du GPS militaire et enfin l'IFF sécurisé.

Pour la phonie, deux types différents de cryptage sont mis en œuvre : l'évasion de fréquence, selon des algorithmes TRANSEC pour la transmission du message, et COMSEC pour le chiffrement du message transmis .
Chaque satellite de la constellation NAVSTAR utilisé pour le « Global Positionning System » émet simultanément 2 signaux de fréquence distincts utilisant 2 codes l'un public l'autre réservé aux activités militaires. Pour cet usage le but du chiffrement est de ne pas être brouillé par une quelconque station de leurrage et de n'utiliser que les signaux venus des satellites NAVSTAR.

La distribution des clés se fait via des injecteurs. Les clés sont maintenant chiffrées dans l'injecteur par des algorithmes gouvernementaux. On parle alors de clés « noires ». Pour toute mission utilisant des systèmes sécurisés des étapes de préparation / restitution sont indispensables..

Pour préparer l'avenir, la DGA travaille notamment sur les projets de modernisation du GPS (SAASM), le développement de Galileo. En outre, un programme de modernisation des radiocommunications a été lancé en 2008 visant à définir d'un standard de forme d'onde multiple pour une radio logicielle sécurisée et interopérable aux performances accrues.

Ces projets mettent en évidence un besoin de convergence entre certaines techniques SSI et la Sûreté de fonctionnement.

Pour terminer nous avons visionné une interview de J.Stern qui a reçu en mai 2009 le prix « Science et Défense » attribué par la DGA.

Application aux usages grand public Internet, web – J.Pantin

Les techniques de cryptographies modernes (clé asymétriques) sont apparues il y a environ 30 ans mais n'ont connu qu'un réel essor à la fin des années 90. Se sont alors développés de systèmes dédiés à la gestion des clés : Infrastructures de Gestion des Clés (ou PKI, en anglais…). Leurs coûts et leurs complexités ont considérablement diminué.

Parallèlement et sur la même période, le cadre réglementaire a beaucoup évolué. Le grand public, les industriels et le secteur juridique acceptent maintenant la signature électronique et se sont approprié les outils informatiques associés.

Mais la fraude numérique est également exponentielle. La Banque de France oblige maintenant les organismes bancaires à faire évoluer leurs systèmes informatiques. L'utilisation de One Time Pad (mot de passe unique valable pour une seule transaction) se généralise.

Il faut distinguer 3 niveaux de sécurité : la sécurité périmétrique (ex : pare-feu), l'authentification d'une personne physique (identifiant / mot de passe) et l'authentification d'une personne morale (exemple d'une transaction entre 2 entreprises).

Les actes notariés doivent intégrer les aspects d'Intégrité, d'Authentification et de Preuve d'Origine. Les clés utilisées sont actuellement de 2048 bits et sont estimées valides jusqu'en 2017. Il est donc nécessaire et recommandé de changer périodiquement les algorithmes des ces documents numériques pour s'affranchir de cette limite dans le temps.

Questions / réponses

Qui coordonne et atteste que les clés et certificats sont valides ? Des structures progressivement hiérarchisées se sont mises en place, par secteur d'activité (ex : banque, aéronautique…). Dans le secteur militaire, il existe des certifications croisées entre IGC des différents pays ainsi que des accords d'interopérabilité.

Le temps nécessaire à la mise au point de nouvelle clés augmente mais le temps nécessaire à les casser ne cesse de diminuer.

Quelles possibilités et quelles perspectives pour la cryptographie quantique ? pour l'instant il s'agit d'une technique futuriste car la mise au point d'équipements informatiques capables de traiter de telles techniques de chiffrement est très complexe.

Quelle reconnaissance pour les techniques de chiffrement ? Il existe 3 niveaux : 1 étoile (ex de la télédéclaration d'impôts), 2 étoiles (ex : déclaration TVA donc bi-partite) et 3 étoiles (utilisées par les notaires).
Le Référentiel Général de Sécurité consolide les critères et spécifications associées.