Introduction à la sécurité
Concevoir des systèmes sûrs

Marie-Laure Potet
Roland Groz

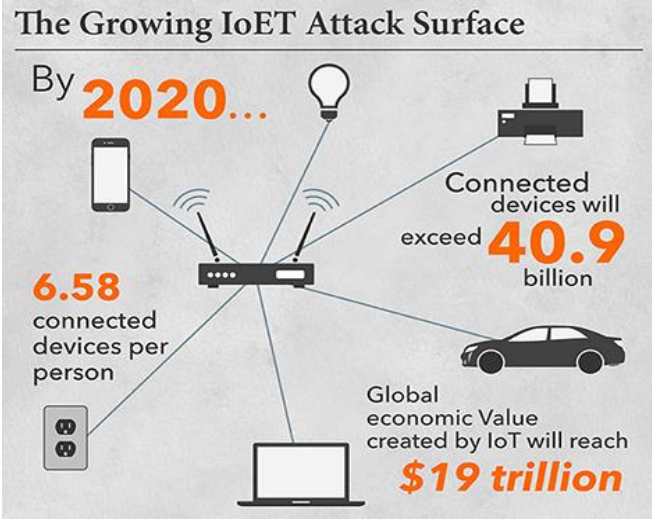
Pourquoi on est doublement concerné à l'Ensimag ?

- Utilisateur de l'internet et citoyen
  - Les risques

- Fabriquant de solutions numériques
  - Les garanties

Les enjeux

- Protection de la vie privée (données personnelles, identité, …)
- Protection des données professionnelles et des données sensibles (propriété intellectuelle)
- Protection des infrastructures informatiques (interne et externe)
- Protection des infrastructures industrielles et des objets connectés (OIV, OSE)



Des exemples : scénarios d’attaque et vulnérabilités

http://iotworm.eyalro.net/

- Attaque sur les ampoules connectées : un drone faisant clignoter tout un bâtiment (DOS)
- Zigbee : low-cost, proximité

Les étapes

- Etape 1 : découvrir et exploiter un bug dans l'implémentation du protocole
- Etape 2 : une attaque permettant de trouver la clé AES permettant d'encrypter et authentifier un nouveau firmware.
- Etape 3 : construire une « mise à jour » du logiciel (over the air) qui exploite la faille
- Résultat : un déni de service
- Correction : correction du bug, meilleure protection des clés

Recommandations

https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-selection_crypto-1.0.pdf

- Utiliser la cryptographie à l'état de l'art
- Ne pas réimplanter des algorithmes de crypto (bibliothèques éprouvées)

2.2.5 Utiliser des bibliothèques éprouvées

L'implémentation logicielle de mécanismes cryptographiques est une tâche délicate qui ne peut pas être effectuée correctement par des non-spécialistes. Il est en effet non seulement nécessaire de s'assurer que les opérations réalisées sont correctes en toutes circonstances, y compris pour ce qui concerne le traitement des erreurs, mais également de prendre en compte les fuites d'information qui peuvent survenir via des canaux inattendus [5]. C'est pourquoi il est impératif de n'employer que des bibliothèques éprouvées bénéficiant d'un suivi de leur sécurité pour tout appel à des mécanismes cryptographiques. C'est également vrai pour la génération de clés symétriques ou asymétriques. La génération de clés asymétriques fait en particulier appel à des méthodes mathématiques non triviales, ce qui est une raison supplémentaire de ne pas la réimplémenter soi-même.

$$C = P^e \bmod N$$
$$P = C^d \bmod N$$

C: Cipher Text

P: Plain Text

e: Public Key

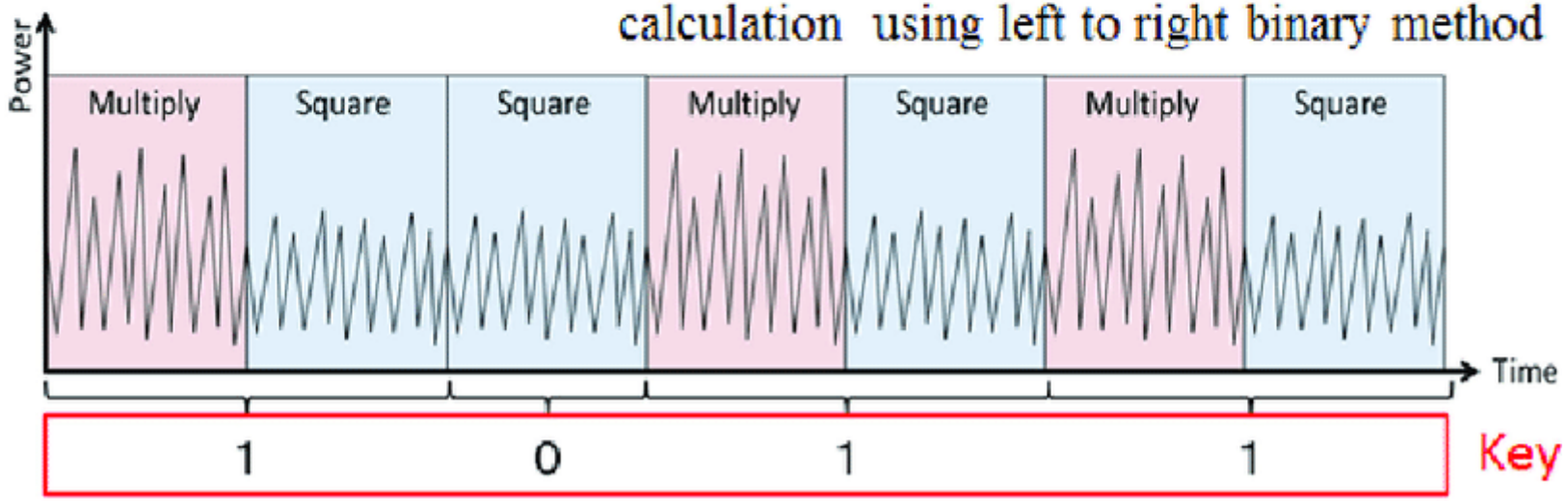
d: Private Key

N: modulo

(a) RSA crypto algorithm

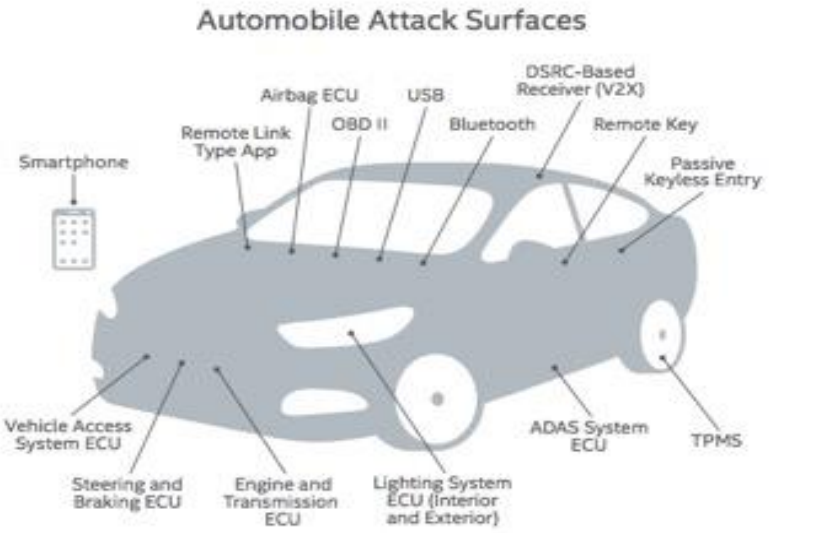
input : X, N, $d = (d_{k-1}, d_{k-2}, \ldots\ldots, d_0)$
output: $Z = X^d \bmod N$
$Z \leftarrow 1$;
For $i = k - 1$ down to 0 do
  $Z \leftarrow Z \times Z \bmod N$; //Square
    if ($d_i = 1$) then
    $Z \leftarrow Z \times X \bmod N$; //Multiply
  end
end
return Z;

(b) Modular exponentiation (X^d mod N) calculation using left to right binary method



(c) Power dissipation model during modular exponentiation

La voiture connectée



Fifteen of the most hackable and exposed attack surfaces, including several electronic control units, on a next-generation car.

220 millions de voitures connectées en 2020, 12% directement connectées à Internet, plus de 12 points d'entrée pour les attaques

Voiture connectée

Jeep Cherokee (2013, 2015) : prise du contrôle du véhicule

Charlie Miller et Chris Valasek maintenant chercheurs en sécurité chez Uber

- Système de divertissement offre des services permettant d'exécuter du code arbitraire

- Envoi de commandes sur le bus CAN sans authentification

http://www.01net.com/actualites/voiture-connectee-voici-les-hacks-les-plus-fous-des-dernieres-annees-1043464.html

Construire des systèmes sécurisés / se protéger

un vaste programme …

De la spécification à l'implémentation

- Penser la sécurité en amont : que veut-on protéger ? Contre qui veut-on se protéger ?

- Proposer des solutions de sécurité et les valider vis-à-vis des besoins (chiffrement, contrôle d'accès, …)

- Analyser les implémentations (SW/HW)

Ici : application à la vérification de protocoles cryptographiques : authentification, paiement, vote, …

Un exemple de tous les jours

- Paiement sur internet :
  - Que veut-on protéger ?
  - Contre quoi ?
  - Quelles assurances a-t-on ?
  - Quelles sont les responsabilités de chacun ?

Exemple

- La confidentialité des données bancaires
- L'intégrité du montant et de la commande
- L'authenticité du site bancaire et du porteur de carte
- La non-répudiation du marchand
- La protection des données (la banque n'a pas à savoir ce qui est acheté, le marchand n'a pas à connaitre les informations bancaires)
- …

Des protocoles sécurisés
3D-Secure V1

- Le 1er octobre 2008 s'est opéré en France un transfert de responsabilité, communément désigné par l'expression "liability shift". Lors d'un paiement à distance, en particulier sur Internet, **il est dorénavant de la responsabilité des banques d'authentifier les transactions et de ne plus seulement les valider**. Auparavant, lorsqu'un paiement par carte bancaire était répudié par son porteur, sa banque pour le rembourser venait récupérer le montant de la transaction sur le compte de l'e-commerçant. Or depuis 2001, avec la technologie 3DSecure, les banques sont capables de vérifier au moment du paiement que l'acheteur est bien le détenteur de la carte bancaire utilisée.

- https://deontofi.com/fraude-aux-cartes-de-credit-avec-code-sms-les-banques-doivent-rembourser/

3D-Secure – V1

⇒Verified by Visa, MasterCard secure code, J-Secure …

- Utilisation de TLS pour la protection des échanges
  - Confidentitalité/intégrité
- Identification du détenteur de la carte
  - Information carte
- Authentification en ligne
  - sms

=> Transfert de responsabilité en cas de fraude (acheteur)

TLS

- Permet :
  - Chiffrement asymétrique (RSA, Diffie-Hellman) : master key
  - Chiffrement symétrique (DES, 3DES, RC4, ..) : clés de session
  - Signature cryptographique des messages (MD5, SHA …)

Les propriétés

- La confidentialité des données bancaires : OK
- L'intégrité du montant et de la commande : OK
- L'authenticité du site bancaire et du porteur de la carte : OK
- La non-répudiation du marchand : OK
- La protection des données (la banque n'a pas à savoir ce qui est acheté, le marchand n'a pas à connaitre les informations bancaires) : KO
- …

3D-Secure V2

Double authentification à partir de janvier 2020 (directive européenne DSP2-authentification forte)

– https://www.usine-digitale.fr/article/la-fin-programmee-de-l-otp-sms.N814310

Remise en cause de l'OTP dans le domaine du paiement électronique

Le 3 mai 2017, l'opérateur de communications électroniques O2-Telefonica Germany a confirmé que certains de ses clients, au cours des derniers mois, avaient vu leurs comptes bancaires vidés en raison de l'utilisation par des hackers d'une faille de sécurité du protocole SS7 qui a corrompu les procédures d'authentification par SMS. Rappelons que les potentielles failles de sécurité du protocole SS7 ont été rendues publiques en 2014.

3D-Secure V2

Obligatoire depuis mai 21 avec une tolérance en 22.

Concrètement, au moment de payer son achat sur internet, le client doit fournir deux des trois éléments d'identification suivants :

- **un mot de passe ou code numérique** (dît élément de connaissance)
- **son portable ou sa ligne téléphonique** (dît élément de possession)
- **son empreinte digitale ou faciale ou le son de sa voix** (dît élément d'inhérence)

Le plus souvent, les banques demandent à leurs clients de télécharger leur application mobile qui intègre le service d'authentification forte (nommé SécuriPass, Certicode Plus, Clé Digitale, etc... selon les établissements) sur leur smartphone, ce qui permet de combiner un élément de possession (le téléphone) avec un élément de connaissance (un code) ou d'inhérence (son empreinte digitale). Au moment de payer un achat, le client reçoit une notification qui le dirige vers l'application installée sur le téléphone. Il doit alors saisir son mot de passe ou son empreinte biométrique pour valider le paiement.

Les propriétés

- La confidentialité des données bancaires : OK
- L'intégrité du montant et de la commande : OK
- L'authenticité du site bancaire et du porteur de la carte : OK
- La non-répudiation du marchand : OK
- La protection des données (la banque n'a pas à savoir ce qui est acheté, le marchand n'a pas à connaitre les informations bancaires) : KO
- …

Ce qu'on va voir

- Protocoles de sécurité : authentification, handshake, paiement, vote, enchères …
  - Modéliser des protocoles
  - Définir des propriétés de sécurité
  - Définir les capacités de l'aataquant
  - Prouver la robustesse de la spécification

Un TP : vérifier/corriger des protocoles

Un TD : concevoir un protocole de vote