Démarche générale

Sécurité: atteindre un *objectif* malgré la présence d'un *adversaire*

Il faut Définir

1. Une **règle** (*Seule Alice doit pouvoir lire le message de Bob*)
2. Un **modèle d'attaquant** (*peut écouter le réseau, mais pas se connecter en root sur le serveur*)
3. **Objectif =** impossible pour un attaquant suivant le **modèle**, de violer la **règle**

Démarche générale

Sécurité: atteindre un *objectif* malgré la présence d'un *adversaire*

Il faut Définir

1. Une **règle** (*Seule Alice doit pouvoir lire le message de Bob*)
2. Un **modèle d'attaquant** (*peut écouter le réseau, mais pas se connecter en root sur le serveur*)
3. **Objectif =** impossible pour un attaquant suivant le **modèle**, de violer la **règle**

⇝ Difficultés:

- besoin de garantir une assertion négative et générale: "Aucun attaquant ..."
- Les modèles d'attaquant réalistes sont nombreux
- la sécurité est celle du maillon le plus faible

Démarche générale

Sécurité: atteindre un *objectif* malgré la présence d'un *adversaire*

Il faut Définir

1. Une **règle** (*Seule Alice doit pouvoir lire le message de Bob*)
2. Un **modèle d'attaquant** (*peut écouter le réseau, mais pas se connecter en root sur le serveur*)
3. **Objectif =** impossible pour un attaquant suivant le **modèle**, de violer la **règle**

⇝ Difficultés:

- besoin de garantir une assertion négative et générale: "Aucun attaquant ..."
- Les modèles d'attaquant réalistes sont nombreux
- la sécurité est celle du maillon le plus faible

Pas de sécurité parfaite:

- chaque solution est valable sur certaines zones de paramètres
- compromis entre risques tolérés, moyens investis et valeurs de l'information à protéger

Objectifs de la sécurité

- Disponibilité: le service doit rester fonctionnel
- Intégrité (integrity): garantir que les données ne sont pas altérées
- Confidentialité (privacy): diffusion d'une donnée limitée aux personnes autorisées

Objectifs de la sécurité

- Disponibilité: le service doit rester fonctionnel
- Intégrité (integrity): garantir que les données ne sont pas altérées
- Confidentialité (privacy): diffusion d'une donnée limitée aux personnes autorisées

et également:

- Preuve: garantir des propriétés sur l'état du système d'information:
  - Authentification: faire preuve de son identité
  - Non-répudiation: impossible de se dédire

Différence en Sûreté et Sécurité

Sûreté

- protection contre les dysfonctionnements et défaillances involontaires
- Exemple: panne d'un disque, saturation d'une billeterie en ligne, etc
- quantifiable statistiquement (fiabilité d'un disque)

Sécurité

- Protection contre les actions malveillante volontaires
- Exemple: vol de données, blocage d'un service, etc
- non quantifiable statistiquement, mais évaluation des niveaux de risques et impacts.

Différence en Sûreté et Sécurité

Sûreté

Ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises.

Sécurité

Ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés.

⇝ des périmètres distincts, mais délimitation parfois floue

Terminologie

Vulnérabilité: faiblesse dans un système lié à sa conception, son installation, sa configuration pouvant entraîner des dommages.

Menace: cause potentielle d'un incident pouvant entraîner des dommages sur un bien. (code malveillant, utilisateur malintentionné, etc)

Attaque: concrétisation d'une menace par l'exploitation d'une vulnérabilité. Action malveillante entraînant des dommages à un bien.

Terminologie

Vulnérabilité: faiblesse dans un système lié à sa conception, son installation, sa configuration pouvant entraîner des dommages.

Menace: cause potentielle d'un incident pouvant entraîner des dommages sur un bien. (code malveillant, utilisateur malintentionné, etc)

Attaque: concrétisation d'une menace par l'exploitation d'une vulnérabilité. Action malveillante entraînant des dommages à un bien.

Objectif d'un expert en sécurité d'un système d'information:

Idéalement: garantir l'absence de vulnérabilité

En pratique: inatteignable

- ⇝ maîtriser les vulnérabilités
- ⇝ veille sur les menaces
- ⇝ détecter les attaques
- ⇝ gestion des incidents / des crises

Terminologie (suite)

Exploitation: acte d'exploiter une vulnérabilité

Exploit: logiciel faisant l'exploitation

Zero day: attaque exploitant une vulnérabilité avant qu'elle ne soit révélée et donc qu'un correctif n'ait pu être proposé.

Black Hat: l'attaquant mal intentionné

White Hat: l'attaquant bien intentionné

Quels adversaires?

Qui?

- Script kiddie
- Elite hacker
- Organisation, communauté
- Acteurs privés structurés
- État

Motivations

- Gain Financier
- Réputation
- Idéologique (déstabilisation)
- Géopolitique (espionnage)

Voir le Rapport Menace et Incidents 2023 du CERT-FR:
`https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-002/`

Un très large spectre de vulnérabilités possibles

- Fondements théoriques de la crypto (e.g. SIDH en compétition NIST)
- Obsolescence des paramètres de sécurité (DES, LogJam)
- Faille dans la conception d'un protocole
- Faille dans une implantation
- Faille dans la configuration d'un système, absence de mises à jour
- Faiblesse d'un mot de passe
- Faille humaine (phishing)

Quelques champs de la sécurité informatique

Sécurité systèmes, réseaux, internet

contrôle d'accès, firewall, phishing, compartimentation, DNS sécurisé, etc

Sécurité logicielle

vulnérabilité des exécutables et applications (buffers overflows, string formats, etc).
$\rightsquigarrow$ audit, vérification formelle

Sécurité matérielle

fuite d'information d'un circuit, canaux cachés, attaques au laser, etc.
$\rightsquigarrow$ masquage, temps constant

Cryptographie

outil (primitives et protocoles) pour garantir la confidentialité, l'authentification, l'intégrité, etc

Architectures de sécurité

infrastructures de confiance, blockchain, etc

Aspects juridiques et sociétaux

vie privée, réglementation, cyberdéfense et sécurité nationale, investigation numérique, audit, gestion de crise, etc

Outline

Quelques exemples d'attaques

Scam (non technique mais rentable)

- Fraude 4-1-9: un héritage sans héritier au Niger vous attends
  ⇝ vieux comme le monde : *Lettres de Jérusalem* (révolution FR)
- Une de vos connaissances dit avoir besoin d'argent en vacance
  ⇝ simple impersonnation à partir d'un couple d'email

Chantage à la webcam (bluff technique)

- Un attaquant prétend par mail avoir piraté votre ordinateur, et pris des informations compromettantes. Demande de rançon pour non-divulgation
  ⇝ Rien n'est vrai (à condition d'avoir un mot de passe sûr)

Hameçonnage (Phishing)

- **Objectif:** inciter la victime à visiter un site controlé par l'attaquant
  - sous-tirer des infos (login/pwd, numéro de CB, etc)
  - voire infecter le système de la victime

Hameçonnage (Phishing)

- **Objectif:** inciter la victime à visiter un site controlé par l'attaquant
  - sous-tirer des infos (login/pwd, numéro de CB, etc)
  - voire infecter le système de la victime
- **Exemples:**
  - Facture impayée
  - *"Cliquez ici pour confirmer la livraison de votre colis"*
  - *"Changement de mot de passe obligatoire, saisissez votre ancien mdp"*

Hameçonnage (Phishing)

- **Objectif:** inciter la victime à visiter un site controlé par l'attaquant
  - sous-tirer des infos (login/pwd, numéro de CB, etc)
  - voire infecter le système de la victime
- **Exemples:**
  - Facture impayée
  - *"Cliquez ici pour confirmer la livraison de votre colis"*
  - *"Changement de mot de passe obligatoire, saisissez votre ancien mdp"*

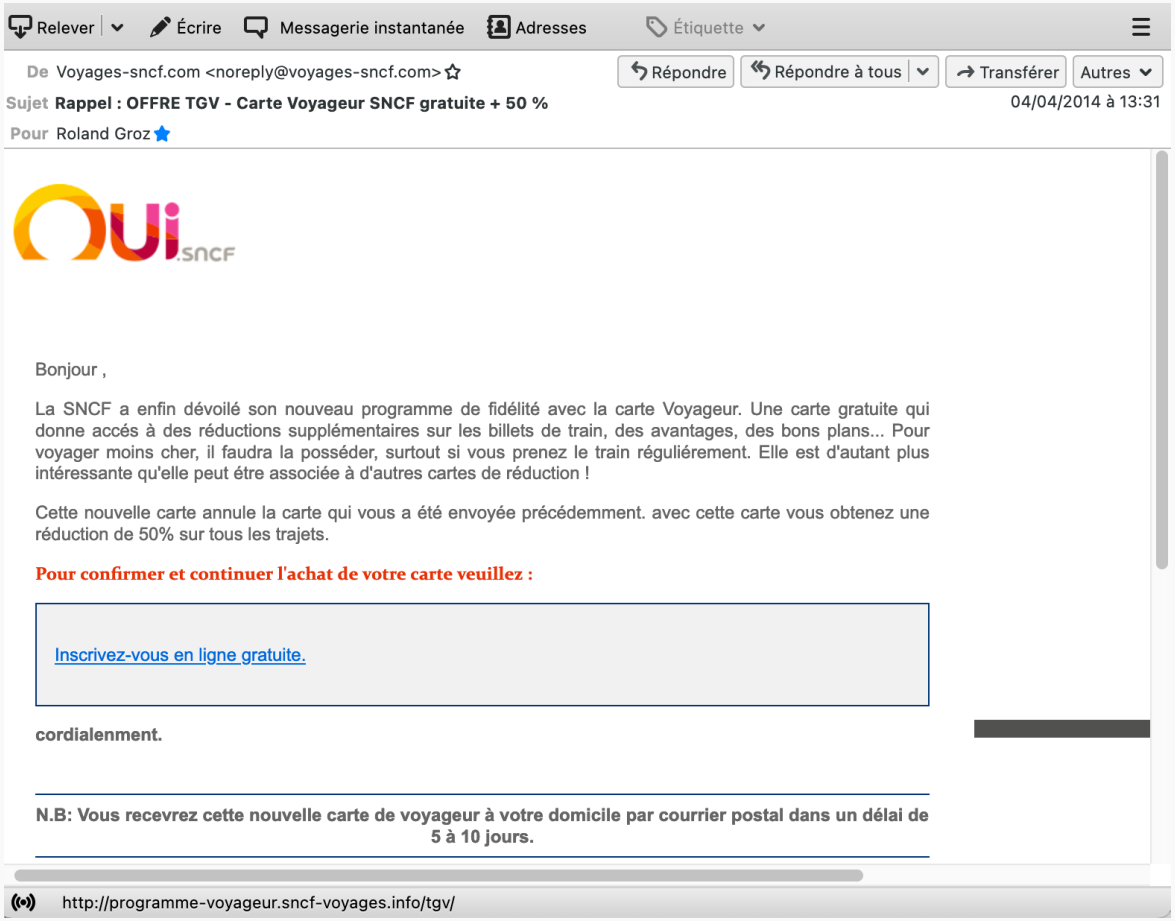
Techniques de dissimulation

- `lcl.fr` peut cacher, en html un `<a href="pirate.ly"> lcl.fr </a>`
  ⇝ toujours contrôler l'adresse effective du lien (mouse-over ou inspection src)
- cybersquatting:
  - homoglyph: `lcl.fr` vs `1cl.fr`
  - TLD swap: `vinci.group` vs `vinci.com`
  - typo-squatting: `datebook.com`, ...

Un hameçonnage bien fait

Programme fidélité de la SNCF

- lancé au moment où la SNCF en faisait la promo
- mail crédible
- renvoyant sur `sncf-voyages.info`
- site enregistré qq jours avant,
- auprès d'un registrar australien
- avec adresse en Californie



Un hameçonnage bien fait

```
$ whois sncf-voyages.info
Domain Name:SNCF-VOYAGES.INFO
Domain ID: D52194680-LRMS
Creation Date: 2014-03-30T16:03:45Z
Updated Date: 2014-03-30T16:03:47Z
Registry Expiry Date: 2015-03-30T16:03:45Z
Sponsoring Registrar:Melbourne IT, Ltd (R141-LRMS)
Sponsoring Registrar IANA ID: 13
WHOIS Server:
Referral URL:
Domain Status: clientTransferProhibited
Domain Status: serverTransferProhibited
Registrant ID:A139572874465680
Registrant Name:Rodriguez Carlos
Registrant Organization:Private Registration US
Registrant Street: PO Box 61359
Registrant City:Sunnyvale
Registrant State/Province:CA
Registrant Postal Code:94088
Registrant Country:US
```

Attaques croisées

- La victime se connecte sur un site légitime
- L'attaquant a posté un message de façon légitime sur ce site (commentaire, image, etc)
  - ce message contient du code (souvent JavaScript),
  - invisible par la victime
  - qui sera exécuté par son navigateur sans qu'elle ne s'en rende compte

Attaques croisées

- La victime se connecte sur un site légitime
- L'attaquant a posté un message de façon légitime sur ce site (commentaire, image, etc)
  - ce message contient du code (souvent JavaScript),
  - invisible par la victime
  - qui sera exécuté par son navigateur sans qu'elle ne s'en rende compte
- Actions:
  - vol de cookies (donc de sessions),
  - redirection vers d'autres sites (phishing), etc
  - action sur le site : post de messages, suppression de données,etc

Attaques croisées

- La victime se connecte sur un site légitime
- L'attaquant a posté un message de façon légitime sur ce site (commentaire, image, etc)
  - ce message contient du code (souvent JavaScript),
  - invisible par la victime
  - qui sera exécuté par son navigateur sans qu'elle ne s'en rende compte
- Actions:
  - vol de cookies (donc de sessions),
  - redirection vers d'autres sites (phishing), etc
  - action sur le site : post de messages, suppression de données,etc

Détecter un site vulnérable:

⇝ poster `<script>alert('coucou')</script>` dans une boîte de diagloque

⇝ si cela ouvre une boite de dialogue, le site est vulnérable

Cross Site Scripting (XSS)

XSS réfléchi

Quand les données fournies par le client dans l'url de requète se retrouvent dans la page produite en réponse.

1. L'Attaquant convainc la victime de cliquer sur un lien (cf phishing, ingénierie sociale)
2. Le lien contient un code malicieux qui se retrouve intégré à la page produite
3. Le navigateur de la victime exécute ce code malicieux

Cross Site Scripting (XSS)

XSS réfléchi

Quand les données fournies par le client dans l'url de requète se retrouvent dans la page produite en réponse.

1. L'Attaquant convainc la victime de cliquer sur un lien (cf phishing, ingénierie sociale)
2. Le lien contient un code malicieux qui se retrouve intégré à la page produite
3. Le navigateur de la victime exécute ce code malicieux

XSS stocké

Quand le code malicieux réside sur le site vulnérable

1. L'Attaquant poste un commentaire sur un forum ou un image
2. Un code malicieux y est inclu, mais non visible
3. La Victime consulte le site
4. Son navigateur exécute le code malicieux en silence

⇝ surface d'attaque plus grande

XSS un exemple

- une image innocente: `tux.png`
- mais le code html sur la page est :

```
<IMG src="tux.png" on mouseover="javascript:  .....">
```

- L'attaquant a pu générer ce code simplement en nommant son fichier image:

```
tux.png "on mouseover="javascript:  .....
```

Contre-mesures

- *Sanitization* des textes saisis dans les boîtes de dialogue
  - filtrer les <,>
  - préfixer les variables
  - ...
- Mais de nombreuses façons de tromper les sanitiseurs

Contre-mesures

- *Sanitization* des textes saisis dans les boîtes de dialogue
  - filtrer les <,>
  - préfixer les variables
  - ...
- Mais de nombreuses façons de tromper les sanitiseurs
- Post-traiter le code html produit avant envoi au client

Contre-mesures

- *Sanitization* des textes saisis dans les boîtes de dialogue
  - filtrer les <,>
  - préfixer les variables
  - ...
- Mais de nombreuses façons de tromper les sanitiseurs
- Post-traiter le code html produit avant envoi au client
- Globalement, repose sur la rigueur des développeurs du site
- Énorme volume de sites, et de boîtes de dialogue dans chaque site
  $\rightsquigarrow$ la majorité des sites Web ont des vulnérabilités XSS

Outline