# « Social Engineering » et systèmes d'information

**CLUSIF**

**14 juin 2007**

**Stéphane Jourdois**

# Agenda

## Première partie : Première approche

- Définition
- Pourquoi choisir cette méthode ?
- Pas vraiment d'exemples réels

## Deuxième partie : Manuel de l'attaquant

- Connaissances préalables
- Cibles
- Caractéristiques humaines
- Leviers d'attaque
- Media
- Exemple : le « phishing »

## Troisième partie : Moyens de lutte

- Confinement et classification
- Sensibilisation et directives
- Détection et remontée d'incidents

# Première approche

**« Social Engineering » et systèmes d’information**

# Définition

## Social Engineering

- **« Faire réaliser à une personne une action dont elle n'aurait pas pris l'initiative seule ».**

- **Traduit en français par :**
  - *Subversion psychologique*,
  - *Ingénierie sociale* (attention à l'équivalent RH),
  - *Psychologie sociale*.

- **Note : naissance antérieure à l'informatique.**

# Pourquoi choisir cette méthode ?

## Les caractéristiques pour l'attaquant

– **Méthode peu chère financièrement mais parfois coûteuse en temps passé.**

– **Science humaine, donc résultats non garantis et non prévisibles de façon précise.**

– **Périmètre très vaste (cf. la psychologie sociale).**

– **Faible niveau de détection.**

– **Permet un compromis entre la vitesse et la discrétion.**

# Pourquoi choisir cette méthode ?

## Les objectifs

– **Tous les objectifs du piratage « classique » :**
  - Gagner de l'argent,
  - Sabotage,
  - Etc.

– **Les objectifs ne sont pas nécessairement liés au SI.**

– **Processus itératif : découper un objectif final en plusieurs étapes réalisables, dont certaines en utilisant le SE :**
  - Obtenir un accès au SI,
  - Elever ses privilèges,
  - Compromettre l'intégrité d'une information du SI.

# Manuel de l’attaquant

## « Social Engineering » et systèmes d’information

# Connaissances préalables

## Psychologie

- **Humaine en général**

- **Sociale en particulier, dont :**
  - Manipulation,
  - Pouvoir (ou pression).

## Technique

- **Piratage classique, forcément complémentaire d'une attaque par Social Engineering,**

- **Fonctionnement en détail des systèmes d'information.**

# Connaissances préalables

## Contexte

– **Sur la cible :**
  - Vie privée,
  - Vie sociale (fonction, ancienneté, etc.) ;

– **Sur la société :**
  - Fonctionnement,
  - Système d'information,
  - Sous-traitants,
  - Etc.

# Cibles

## Globalement

**L'humain par définition…**

**« Tout utilisateur dispose d'une information », et « toute information est bonne à prendre ».**

## 1 - Support informatique

- **Rôle : aider.**
- **Authentification souvent défectueuse.**
- **Contraintes de temps.**
- **Cible pour les attaques de l'intérieur.**

# Cibles

## 2 - Utilisateurs de services en ligne

- Peu sensibilisés.
- Mauvaise connaissance des habitudes des sociétés.
- Tendance des sociétés à communiquer par mail (noie et crédibilise le phishing).
- Cible privilégiée des attaques non ciblées.

## 3 - Utilisateurs réguliers du SI

- Connaissent l'organisation de la société, les procédures, et ceux qui la composent.
- Cible pour l'assemblage d'un annuaire bien renseigné.

# Cibles

## 4 - Nouveaux utilisateurs et utilisateurs occasionnels

- Mauvaise connaissance du SI et de la société.
- Sensibilisation naissante.
- Cible plus facile mais parfois moins utile.

## 5 – Administrateurs

- Meilleure sensibilisation à la confidentialité des informations, en particulier des authentifiants.
- Meilleure connaissance du système d'information.
- Meilleure détection des requêtes sortant de l'ordinaire.
- Tendance à la remontée d'informations.
- Cible difficile et exigeante, mais des attaques spécifiques existent, et les bénéfices sont plus élevés.

# Caractéristiques humaines

## Traits humains

- **Accorder sa confiance**
- **Aider**
- **Eviter les problèmes**

# Leviers d'attaque

## Amitié et coopération (1/2)

- **Empathie**
  - Comprendre les sentiments d'autrui sans les ressentir soi-même.
  - Recentrer et reformuler les dires de l'interlocuteur.
- **Sympathie**
  - Feindre le réflexe de sympathie et attirer la sympathie.
  - Se montrer aimable, serviable et coopératif.
  - Donner plus d'informations que demandées.
  - Entretiens réguliers.
- **Injustice**
  - Tendance à vouloir réparer les injustices morales.
  - Impose une bonne connaissance de la société cible.
  - Monter un scénario d'injustice crédible, qui peut être éviter avec le concours de la cible.

# Leviers d'attaque

## Amitié et coopération (2/2)

- **Détresse**
  - « Faute avouée est à demi pardonnée ».
  - Contraintes de temps et de moyens.
  - Utilisation des points précédents.

- **Exposition des sociétés**
  - Avoir des employés humains ?

- **Points marquants**
  - Préalable : connaissance personnelle éventuelle du sujet
  - Méthode discrète (en plusieurs essais).
  - Difficile à éviter en société.
  - Difficile à détecter, parce que les victimes ne trahissent pas un « ami », et ne se vantent pas d'avoir transgressé une règle.

# Leviers d'attaque

## Usurpation d'identité et intimidation (1/2)

- **Pouvoir et soumission**
  - Usurper l'identité d'une personne possédant du pouvoir, de l'influence, directement ou indirectement.
  - Usurper l'identité de l'assistant d'une personne connue et haut placée.
  - Beauvois et Joule, dans « Petit traité de manipulation à l'usage des honnêtes gens », éditions Presses Universitaires de Grenoble, 1987 :
    - Soumission sans pression
    - Soumission forcée
    - Pied dans la porte
    - Amorçage

# Leviers d'attaque

## Usurpation d'identité et intimidation (2/2)

- **Diffusion des responsabilités**
  - « Les autres l'ont déjà fait ».
  - « J'en prend la responsabilité ».

- **Exposition des sociétés**
  - Les rachats augmentent l'exposition.
  - Multiplication des acteurs dans la filière sécurité, flou sur les responsabilités.
  - Contextes culturels différents au sein du même groupe.
- **Points marquants**
  - Préalable : annuaire bien renseigné, organigramme.
  - Méthode un peu plus risquée et détectable que la précédente.
  - Plus rapide (un seul essai).

# Leviers d'attaque

## Sabotage et « Reverse Social Engineering »

- ***Modus operandi***
  - Saboter un élément du SI, et se faire connaître comme l'interlocuteur adéquat dans ce cas.
  - Initiative de la cible.
  - Gain de prestige auprès de la cible lorsque la panne est réparée.
  - Pour réparer, ou pour enquêter, une information que possède la cible est nécessaire…

- **Exposition des sociétés**
  - Les dénis de services, souvent négligés lors des audits de sécurité, deviennent utiles à l'attaquant.

- **Points marquants**
  - Très peu discret.
  - Parfaitement efficace.
  - Longue préparation et moyens plus conséquents.

# Leviers d'attaque

## Techniques associées

– **« Trash recovering » (récupération des poubelles)**
  - Très efficace une fois passée la première appréhension.
  - Les sociétés modernes produisent des poubelles propres, et contenant beaucoup d'informations sensibles (disques durs, papiers classifiés mal détruits, organigrammes et annuaires, effets personnels, etc.).

– **« Shoulder surfing » (navigation par-dessus l'épaule)**
  - Regarder par-dessus l'épaule de la cible pendant qu'il tape.

# Media

**La vitesse du media conditionne la réussite de l'attaque : la cible réfléchit à froid.**

**Les nouveaux média fournissent de nouvelles méthodes d'attaque, donc nouvelles vulnérabilités.**

## 1 – Téléphone

- **Le plus utilisé,**
- **Le plus rapide, et**
- **Le plus discret, mais**
- **… Le plus connu (cf. démarchage téléphonique).**
- **Ne pas laisser le temps de réfléchir ➔ garder l'initiative.**

# Media

## 2 - Internet (courrier électronique ou autres protocoles)

- Rapide,
- Discret,
- De plus en plus connu pour les attaques non ciblées.
- Cf. phishing plus loin

## 3 – Fax

- Intermédiaire entre média électronique et papier.
- Rapide et peu détecté.
- Support de choix assez peu utilisé.

## 4 - Courrier papier

- Lent mais peu détecté

# Exemple : le « phishing »

## Phishing

– **« Attaque de Social Engineering, limitée à l'usurpation d'identité non ciblée, et en général par mail ».**

– **Contraction de :**
  - « fishing », pécher, et de
  - « phreaking », piratage de lignes téléphoniques.

– **Traduit en français par :**
  - *Hameçonnage*, surtout au Québec.
  - *Filoutage*, J.O. du 12 février 2006, Commission générale de terminologie et de néologie de France.

# Moyens de lutte

**« Social Engineering » et systèmes d’information**

# Sensibilisation et directives

## Sensibilisation

- **Méthode la plus logique et la plus importante.**
- **Coûteuse en temps et en ressources, périme rapidement.**
- **La sensibilisation transverse est parfois complexe dans les groupes.**
- **Exemple : lettre hebdomadaire qui donne un exemple de scénario et rappelle que la vigilance est de mise.**
  - Limite : crédibilité des exemples de sensibilisation. La menace est sous-estimée quand on parle aux gens de Social Engineering.
- **Exemple : Audit puis communication aux utilisateurs.**

# Sensibilisation et directives

## Directives de sécurité

- **Doivent prendre en compte la menace de Social Engineering, en particulier celles qui traitent de la classification des informations.**
- **Exemple : procédure de call-back (rappel téléphonique).**
- **Exemple : Contrôle d'accès physique (accueil et escorte).**
  - Chaque exception représente une vulnérabilité.
- **Déplacement de la responsabilité de l'utilisateur vers l'émetteur de la directive**
- **Impact plus limité dans les pays latins que dans les pays anglo-saxons et germaniques.**
- **« Etre inventif pendant la rédaction des directives et la sensibilisation ».**
- **Attention aux règles trop strictes qui incitent au contournement.**

# Confinement et classification

## Retirer l'information à l'utilisateur

- Authentification physique : OTP, tokens x509, biométrie, etc.

## Classifier l'information

- Augmentation de la résistance des utilisateurs à délivrer une information dont ils savent qu'elle est classifiée.
- Limite : morcellement des informations.

# Détection et remontée d'incidents

- **Une attaque est plus ou moins discrète, donc détectable.**
- **Etablissement d'un Responsable local de la sécurité, qui centralise les incidents de sécurité, et est seul habilité à donner aux utilisateurs un avis formel et authentifié sur une action sortant de l'ordinaire.**
- **La contre-attaque est rendue possible par la remontée d'incidents**
- **Détails devant éveiller les soupçons : l'interlocuteur**
  - hésite,
  - refuse de donner des noms, ou utilise des noms approximatifs,
  - est pressé, ou si sa batterie de portable est en fin de vie,
  - menace, ou utilise des arguments personnels,
  - ne connaît manifestement pas toutes les règles de fonctionnement de l'entreprise,
  - commet de petites erreurs,
  - demande des informations sensibles,
  - Refuse d'être rappelé.

# Conclusion

**« Social Engineering » et systèmes d’information**

# Conclusion

**Kevin Mitnick :**

**« You could spend a fortune purchasing technology and services… and your network infrastructure could still remain vulnerable to old-fashioned manipulation ».**

**Voir les attaques dans les films au cinéma.**

**Le Social Engineering reposant sur des caractères humains, l'avenir de cette technique est assuré.**

# Contact

**Stéphane Jourdois**

**Tél. : +33 1 41 58 56 47**

**Mail : sjourdois@arseo.com**



**14 juin 2007**

**ARSeO**

**8 rue de Valmy**

**93100 Montreuil**

**France**

**www.arseo.com**