Évaluation de la confidentialité par un processus de diffusion de vulnérabilité

Aghiles DJOUDI

Sorbonne Université

June 7, 2019

Outline

Context

Introduction

	Monde (2018)	Monde (2022)	France (2018)
Nombre dutilisateurs	3,8 milliards	4,2 milliards	25,9 millions
Nombre de comptes émail	4,4 milliards	5,6 milliards	68 millions
Nombre dadresses émail par utilisateurs	1,7	1,9	2,1
Nombre de mails reçus chaque jour	281 milliards	333 milliards	1,4 milliard
Le marché de lémail	9,8 Mrds de $	20,4 Mrds	?

Table 1: Les chiffres 2018 de lémail [**BibEntry2014Sep**].

Context

Introduction

	Monde (2018)	Monde (2022)	France (2018)
Nombre dutilisateurs	3,8 milliards	4,2 milliards	25,9 millions
Nombre de comptes émail	4,4 milliards	5,6 milliards	68 millions
Nombre dadresses émail par utilisateurs	1,7	1,9	2,1
Nombre de mails reçus chaque jour	281 milliards	333 milliards	1,4 milliard
Le marché de lémail	9,8 Mrds de $	20,4 Mrds	?

Table 1: Les chiffres 2018 de lémail [**BibEntry2014Sep**].

Motivation

Introduction

- Donner un moyen aux utilisateurs de mesurer leur vulnérabilités
- Aider les utilisateurs à mieux configurer leur messagerie.
- Alerter les utilisateurs d'une nouvelle vulnérabilité.
- Sensibiliser les utilisateurs du niveau de diffusion des menaces.

Figure 1: Indice de confidentialité [1].

Défis

Introduction

- Recommander des mesures de sécurité personnalisés
  - Nouveau mot de passe chaque période de temps
  - Sécuriser l'échange avec des comptes vulnérables
  - Adapter les permissions aux changements
- Calculer la vulnérabilité de l'environnement social
  - Calculer le niveau de vulnérabilité des interactions
  - Calculer le niveau d'influence entre les utilisateurs.
- Calculer la vulnérabilité du chemin des messages
  - Identification des serveurs MTA
  - Attribuer une note de confiance à chaque serveur
  - Calculer la confiance moyenne du chemin.

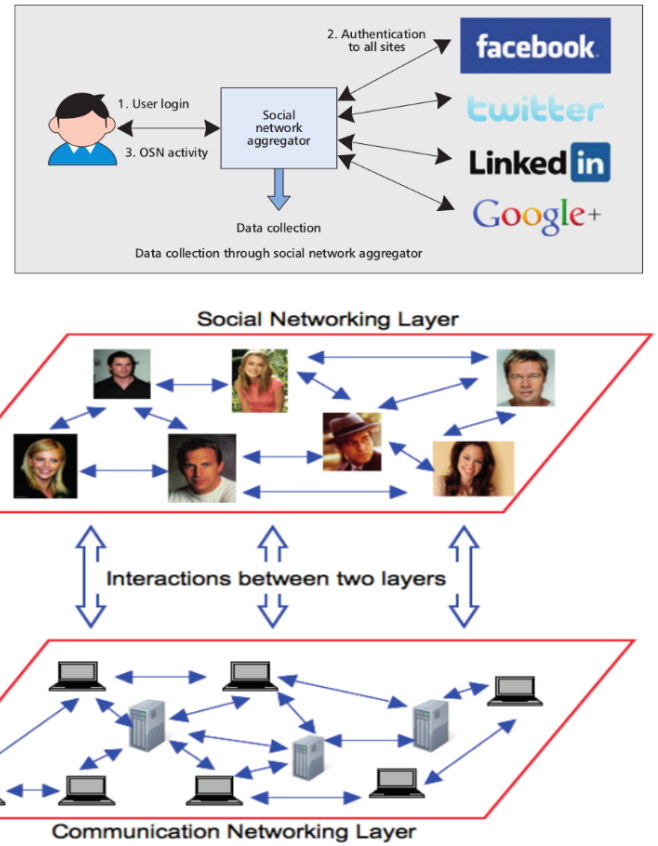
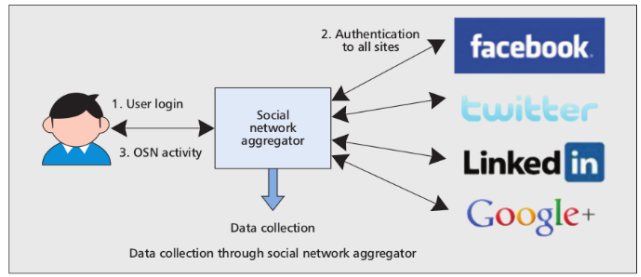


Figure 2: Interaction sociale.

Défis

Introduction

- Recommander des mesures de sécurité personnalisés
  - Nouveau mot de passe chaque période de temps
  - Sécuriser l'échange avec des comptes vulnérables
  - Adapter les permissions aux changements
- Calculer la vulnérabilité de l'environnement social
  - Calculer le niveau de vulnérabilité des interactions
  - Calculer le niveau d'influence entre les utilisateurs
- Calculer la vulnérabilité du chemin des messages
  - Identification des serveurs MTA
  - Attribuer une note de confiance à chaque serveur
  - Calculer la confiance moyenne du chemin.



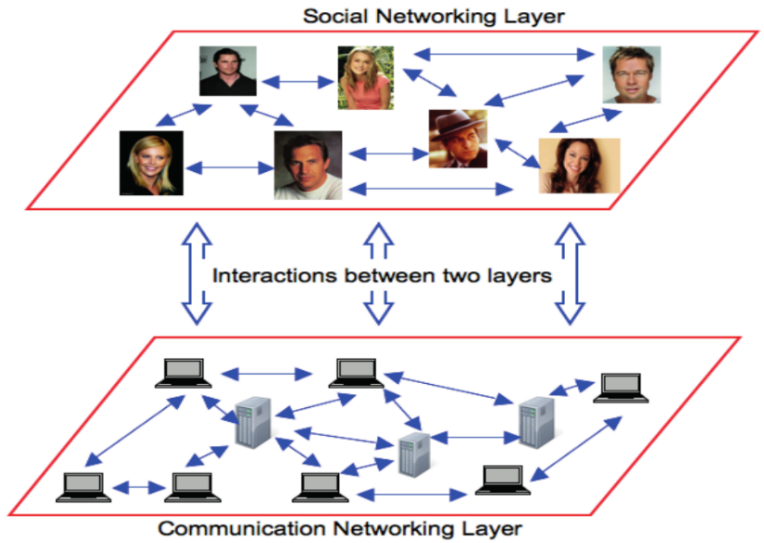


Figure 2: Interaction sociale.

Contributions

Introduction

- Estimation de l'indice de confidentialité social.
  - Vulnérabilité individuelle -> Vulnérabilité sociale.
  - Processus de diffusion de vulnérabilité.
  - Relation entre confiance et vulnérabilité.
  - Données: Émails de Enron & Caliopen.

Figure 3: La vulnérabilité d'un utilisateur est la vulnérabilité de tous.

Outline

Outline

Outline

Travaux connexes

Comparaison

Travaux	Contribution	Performance
[2] Protect U	Classification des interlocuteurs	Configuration des listes d'amis
[3] Privacy Wizard	Classification des interlocuteurs	Configuration des permissions
[4] SocialMarket	Intérêt communs	Évaluation des relation de confiance
[5] TAPE	Fuite d'information	Évaluation de la diffusion de l'info
[6] LENS	Protection anti-spam	Évaluation des émetteurs de confiance
[7] SocialEmail	Classer les chemins des msg	Évaluation de la fiabilité du message
[8] Privacy Index	Visibilité, sensibilité	Évaluation de l'exposition des msg

Table 2: Contributions des travaux existants.

Outline

Etape 1: Calcule de la vulnérabilité individuelle

Méthode

- Entrée:
  - Vulnérabilité de la machine utilisée:
    - Connexion réseaux (privé (1) ou publique (2))
    - Type d'architecture: Ethernet, 5G, 4G, Wifi (1:4)
    - Système d'exploitation (Windows, Unix) (1:2)
    - Navigateur web (1:10)
  - Vulnérabilité du compte utilisé
    - Mdp utilisé, mode de récupération des mdp (1:5)
    - Nombre de sessions ouvertes en même temps.(1:nbr)
    - Mode de chiffrement, signature, version TLS
- Sortie:

$$Pi = \sum_{i}^{n} \frac{w * V}{n} \quad (1)$$

  - Pi: Vulnérabilité individuelle
  - w: Poids de chaque vulnérabilité
  - V: Les vulnérabilités cités au dessus

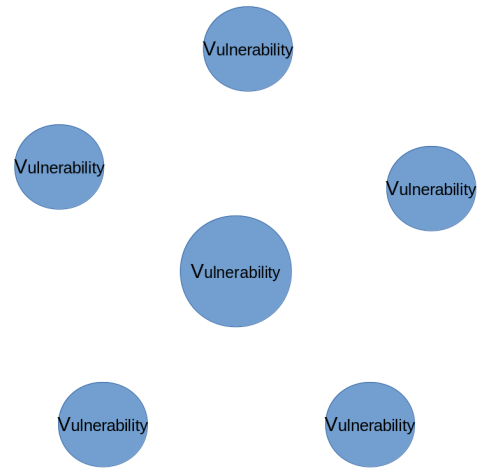


Figure 4: Vulnérabilité individuelle.

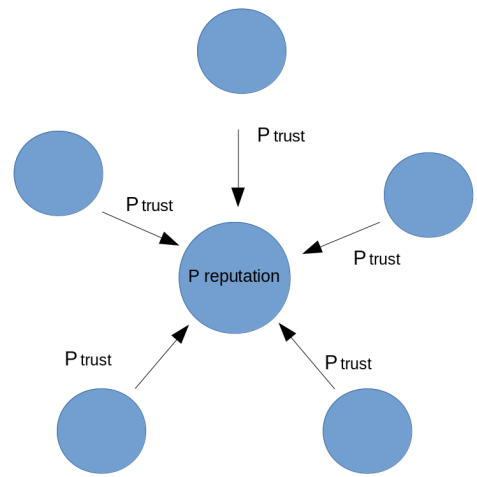
Etape 2: Calcule de la réputation des utilisateurs

Méthode

- Entrée:
  - Fréquence d'utilisation de la messagerie.
  - Horaire, durée des échanges (1:5)
  - % des échanges chiffrés, signés, claires (1:3)
  - Importance des interlocuteurs: Liste favoris (2), noir(1)
  - Type de données: Texte, images, vidéos, script (1:4)
- Méthode:
  - Loi binomiale
- Output:

$$P(reputation) = P(X \geq 1) = 1 - (1 - P(trust))^n \qquad (2)$$

  - Where,
    - X: Niveau de confiance, X ~B(n,p)
    - n: deg(noeud)
    - P(X=1): La probabilité de se faire attribué une confiance par un interlocuteur



P reputation = 1 - (1 - P trust)^n

Figure 5: Niveau de réputation.

Etape 3: Calcule de la vulnérabilité sociale

Théorie de l'influence sociale de Freidkin

- Entrée:
  - $Y^{(1)}$ = Vecteur des vulnérabilités individuelles de N utilisateurs (eq 1)
  - α= Le niveau de réputation (d'influence) de chaque utilisateur (eq 2)
  - M = Matrice d'adjacence N x N
- Modèle:

$$Y^{(t)} = \alpha M Y^{(t-1)} + (1-\alpha) Y^{(t-1)} \tag{3}$$

- Sortie:
  - $Y^{(t)}$ = Vecteur des vulnérabilités sociales des N utilisateurs

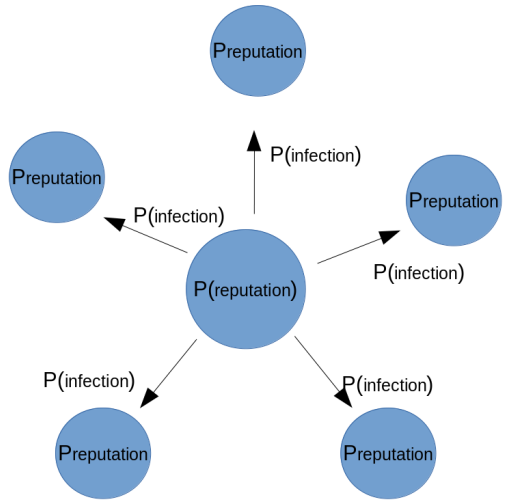


Figure 6: Vulnérabilité Sociale.

Etape 3: Calcule de la vulnérabilité sociale

Théorie de l'influence sociale de Freidkin

Propriétés formelles du modèle:

- Lorsque l'influence d'un utilisateur est élevé, le modèle se réduit aux:
  - vulnérabilités moyennes de ses amis pondérées par leur niveaux de confiances.

$$Y^{(t)} = 1 * MY^{(t-1)} + (1-1)\,Y^{(t-1)} \tag{3}$$

$$Y^{(t)} = MY^{(t-1)}$$

- En absence d'influence, le modèle se réduit à:
  - sa propre vulnérabilité pondérée par le niveau de méfiance de ses amis

$$Y^{(t)} = 0 * MY^{(t-1)} + (1-0)\,Y^{(t-1)} \tag{3}$$

$$Y^{(t)} = Y^{(t-1)}$$

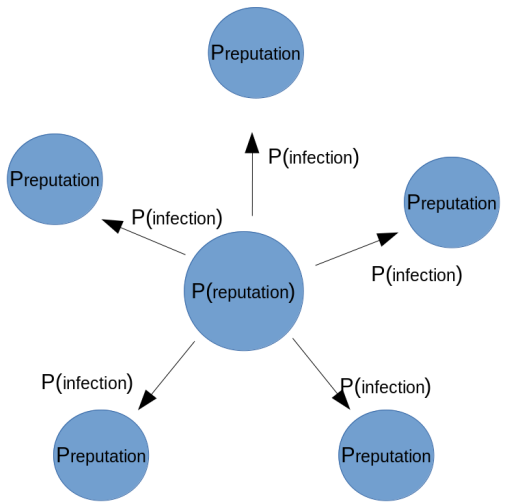


Figure 7: Vulnérabilité sociale.

Outline

Expérimentation

Expérimentation

Paramètre	Valeur
Utilisateurs	958
Messages	6966
Diamètre	958
# de msg en moyenne	2.413361
Densité des msg	0.00252
Modularité	0.654600
Distance moyenne	3.042114

Table 3: Propriétés des données Enron.

Figure 8: Enron logo.

Paramètre	Valeur
Utilisateurs	5885
Messages	26547
Diamètre	2096
# de msg en moyenne	9.02192
Densité des msg	0.001533
Modularité	0.86526
Distance moyenne	3.914097

Table 4: Propriétés des données Caliopen.

Figure 9: Caliopen logo.

Outline

Conclusion

- Le but de ce travail est de simuler un processus de contamination des vulnérabilités individuelles.
  - La vulnérabilité d'un utilisateur est la vulnérabilité de tous.
  - A la fin de la diffusion, tous les utilisateurs auront un indice de vulnérabilité social.
- Travaux futures
  - Proposer des mécanismes pour améliorer la réputation des utilisateurs non-vulnérables.
    - Suggérer des interlocuteurs bien réputés avec des indices de vulnérabilité acceptables.
  - Proposer des mécanismes pour améliorer la vulnérabilité des utilisateurs réputés.
    - Recommander des configurations et des logiciels.

Conclusion

- Le but de ce travail est de simuler un processus de contamination des vulnérabilités individuelles.
  - La vulnérabilité d'un utilisateur est la vulnérabilité de tous.
  - A la fin de la diffusion, tous les utilisateurs auront un indice de vulnérabilité social.
- Travaux futures
  - Proposer des mécanismes pour améliorer la réputation des utilisateurs non-vulnérables.
    - Suggérer des interlocuteurs bien réputés avec des indices de vulnérabilité acceptables.
  - Proposer des mécanismes pour améliorer la vulnérabilité des utilisateurs réputés.
    - Recommander des configurations et des logiciels.

Thank you !

References

[1] E. Michael Maximilien et al. “ Privacy-as-a-Service: Models, Algorithms, and Results on the Facebook Platform ”. In: *Proceedings of Web*. Vol. 2. 00054. 2009 (p. 5).

[2] Ala Eddine Gandouz. “ PROTECT_U: Un Systeme Communautaire Pour La Protection Des Usagers de Facebook ”. In: (2012). 00001, p. 77 (p. 12).

[3] Lujun Fang and Kristen LeFevre. “ Privacy Wizards for Social Networking Sites ”. In: 00397. ACM Press, 2010, p. 351 (p. 12).

[4] Davide Frey, Arnaud Jégou, and Anne-Marie Kermarrec. “ Social Market: Combining Explicit and Implicit Social Networks ”. In: *Stabilization, Safety, and Security of Distributed Systems*. Symposium on Self-Stabilizing Systems. Lecture Notes in Computer Science. 00019. Springer, Berlin, Heidelberg, Oct. 10, 2011, pp. 193–207 (p. 12).

[5] Yongbo Zeng et al. “ A Study of Online Social Network Privacy Via the TAPE Framework ”. In: *IEEE Journal of Selected Topics in Signal Processing* 9.7 (Oct. 2015). 00003, pp. 1270–1284 (p. 12).

[6] Sufian Hameed et al. “ LENS: Leveraging Social Networking and Trust to Prevent Spam Transmission ”. In: *Network Protocols (ICNP), 2011 19th IEEE International Conference On*. 00019. IEEE, 2011, pp. 13–18 (p. 12).

[7] Thomas Tran, Jeff Rowe, and S. Felix Wu. “ Social Email: A Framework and Application for More Socially-Aware Communications ”. In: *Social Informatics*. Ed. by Leonard Bolc, Marek Makowski, and Adam Wierzbicki. Vol. 6430. 00000. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 203–215 (p. 12).

[8] Raj Kumar Nepali and Yong Wang. “ SONET: A SOcial NETwork Model for Privacy Monitoring and Ranking ”. In: 00021. IEEE, July 2013, pp. 162–166 (p. 12).