

Social privacy score through vulnerability contagion process

Aghiles DJOUDI, Guy PUJOLLE

Sorbonne University

March 24, 2019

Plan

1. Introduction

2. Contribution

3. Conclusion

Context

Introduction

| | World (2018) | World (2022) | France (2018) |
|---------------------------------|--------------|--------------|---------------|
| Users | 3.8 billion | 4.2 billion | 25.9 million |
| Email accounts | 4.4 billion | 5.6 billion | 68 million |
| Email accounts per user | 1.7 | 1.9 | 2.1 |
| Emails received each day | 281 billion | 333 billion | 1.4 billion |
| The email market | 9.8 Mrds \$ | 20.4 Mrds \$ | ? |

Table 1: Email statistics [1].

- Email:
 - More than 50% of the world population use email
 - Usage: 75% personal, 25% professional
- Facebook:
 - 2.2 billion active users (29% worldwide)
 - 10 billion messages are sent every day
 - 8.051 billion \$

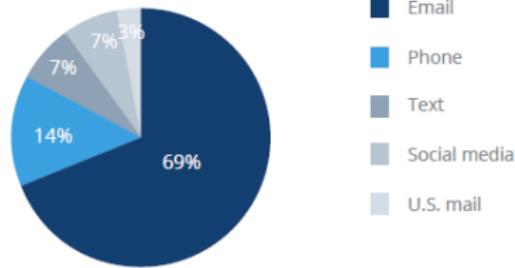


Figure 1: Communication tools [1].

Context

Introduction

| | World (2018) | World (2022) | France (2018) |
|---------------------------------|--------------|--------------|---------------|
| Users | 3.8 billion | 4.2 billion | 25.9 million |
| Email accounts | 4.4 billion | 5.6 billion | 68 million |
| Email accounts per user | 1.7 | 1.9 | 2.1 |
| Emails received each day | 281 billion | 333 billion | 1.4 billion |
| The email market | 9.8 Mrds \$ | 20.4 Mrds \$ | ? |

Table 1: Email statistics [1].

- ▶ Email:
 - ▶ More than 50% of the world population use email
 - ▶ Usage: 75% personal, 25% professional
- ▶ Facebook:
 - ▶ 2.2 billion active users (29% worldwide)
 - ▶ 10 billion messages are sent every day
 - ▶ 8.051 billion \$

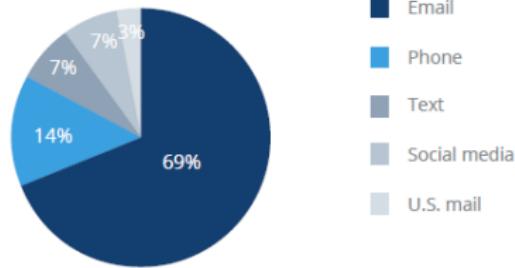


Figure 1: Communication tools [1].

Problematic

Introduction

- Privacy issues:

1. External vulnerabilities

- Network technologies: 4G, 5G, Wifi, Ethernet.
- Security protocols: HTTPS, SMTPS, IPsec

2. Internal vulnerabilities

- Service providers
 - * General Terms and Conditions of Use (GTC)
- 3rd parties
 - * Privacy settings
 - * Permission management
- Users
 - * Configuration of user accounts
 - * Users list management



Figure 2: Privacy, Am I concerned ?.

Problematic

Introduction

- Privacy issues:

1. External vulnerabilities

- Network technologies: 4G, 5G, Wifi, Ethernet.
- Security protocols: HTTPS, SMTPS, IPsec

2. Internal vulnerabilities

- Service providers
 - * General Terms and Conditions of Use (GTC)
- 3rd parties
 - * Privacy settings
 - * Permission management
- Users
 - * Configuration of user accounts
 - * Users list management



Figure 2: Privacy, Am I concerned ?.

Motivation

Introduction

- ▶ Give users a way to measure their vulnerabilities
- ▶ Help users to better configure their email accounts.
- ▶ Alert users of a new vulnerability.
- ▶ Make users aware about the level of threat diffusion.



Figure 3: Privacy index [2].

Challenges

Introduction

- ▶ Recommend customized security measures
 - New password every time period
 - Secure the exchange with vulnerable accounts
 - Adapt permissions to changes
- ▶ Vulnerability measurement of the social environment
 - Measure the level of vulnerability of interactions
 - Measure the level of influence between users.
- ▶ Calculate the vulnerability of the message path
 - Identification of MTA servers
 - Assign a trust score to each server
 - Calculate the average confidence of the path.

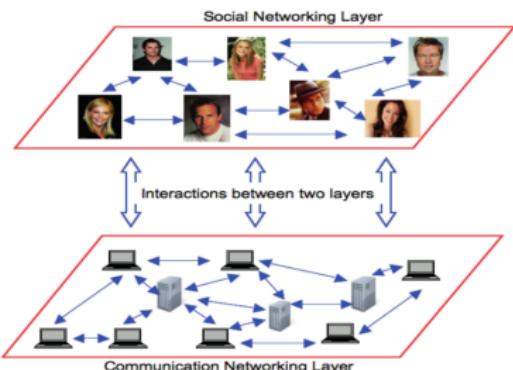
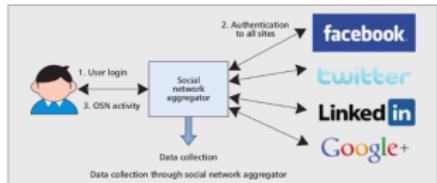


Figure 4: Social interaction.

Challenges

Introduction

- ➡ Recommend customized security measures
 - New password every time period
 - Secure the exchange with vulnerable accounts
 - Adapt permissions to changes
- ➡ Vulnerability measurement of the social environment
 - Measure the level of vulnerability of interactions
 - Measure the level of influence between users
- ➡ Calculate the vulnerability of the message path
 - Identification of MTA servers
 - Assign a trust score to each server
 - Calculate the average confidence of the path.

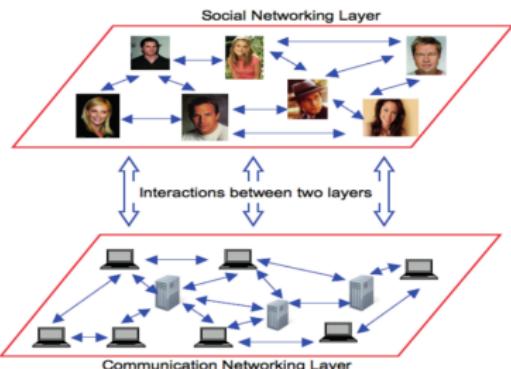
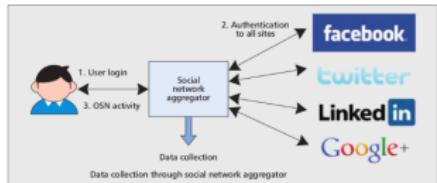


Figure 4: Social interaction.

Contributions

Introduction

- ➡ Social vulnerability estimation.
 - Individual vulnerability -> Social vulnerability.
 - Vulnerability diffusion process.
 - Relationship between trust and vulnerability.
 - Data: Enron & Caliopen emails.



Figure 5: The vulnerability of one user is the vulnerability of all users.

Plan

1. Introduction

2. Contribution

3. Conclusion

Plan

- 1. Introduction
 - 2. Contribution
 - 3. Conclusion
- 1. Related work
 - 2. Diffusion process
 - 3. Experimentation
 - 4. Results exploitation

Plan

1. Introduction

2. Contribution

3. Conclusion

- 1. Related work
- 2. Diffusion process
- 3. Experimentation
- 4. Results exploitation

Related work

Comparison

| Works | Contribution | Goal |
|--------------------|---------------------------------|---|
| [3] Protect U | Classification of interlocutors | Friends lists management |
| [4] Privacy Wizard | Friends Classification | Permission Configuration |
| [5] SocialMarket | Common Interests | Assessment of Trust Relationships |
| [6] PARE | Information Leakage | Evaluation of Information Dissemination |
| [7] LENS | Spam Protection | Trusted Emitters Evaluation |
| [8] SocialEmail | Classify msg by paths | Evaluate message reliability |
| [9] Privacy Index | Visibility, sensitivity | Msg exposure assessment |

Table 2: Contributions from existing work.

Plan

- 1. Introduction
 - 2. Contribution
 - 3. Conclusion
- 1. Related work
 - 2. Diffusion process
 - 3. Experimentation
 - 4. Results exploitation

Step 1: Individual vulnerability measurement

Method

| Parameter | Value |
|--------------------|-----------------------------|
| Network connection | Private, Public |
| Technology | Ethernet, 5G, 4G, Wifi |
| Operating system | Windows, Unix, Mac |
| Web browser | Firefox, Chrome, Opera, ... |
| Password strength | low, medium, strength |
| Sessions opened | counter |
| TLS version | v1.0, v1.1, v1.2, v1.3 |

Table 3: Individual Vulnerability parameter

$$Y = \sum_i^n \frac{w * V}{n} \quad (1)$$

- **Y:** Individual vulnerability
- **w:** Weight of each vulnerability
- **V:** Scores mentioned above

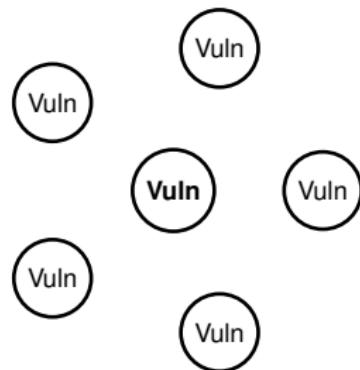


Figure 6: Individual vulnerability level.

Step 2: Users reputation estimation

Method

| Parameter | Value |
|----------------------------|------------------------------|
| Frequency of msg exchanged | continuous |
| Discussion time | continuous |
| % of messages exchanged | cipher, signed or clear |
| Message type exchanged | Text, images, videos, script |

Table 4: Trust grant features

$$\alpha = P(\text{reputation}) = P(X \geq 1) = 1 - (1 - P(\text{trust}))^n \quad (2)$$

Where,

- **X**: trust grant, random variable, $X \sim B(n,p)$
- **n**: deg(node)
- **P(X=1)**: The probability of being assigned one trust grant by an interlocutor

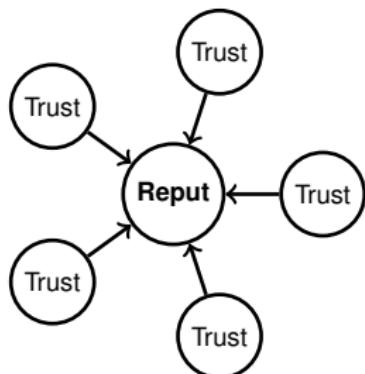


Figure 7: Reputation level.

Step 3: Social vulnerability measurement

Freidkin's theory of social influence

- Input (Features):

- $Y^{(1)}$ = Vector of the individual vulnerabilities of N users (eq 1)
- α = The level of reputation (influence) of each user (eq 2)
- M = Adjacency matrix $N \times N$

- Model:

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

- Output:

- $Y^{(t)}$ = Vector of the social vulnerabilities of the N users

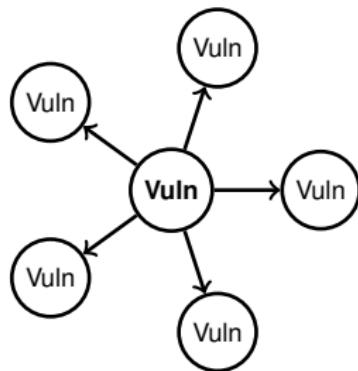


Figure 8: Social vulnerability.

Step 3: Social vulnerability measurement

Freidkin's theory of social influence

Formal properties of the model:

- When a user's influence is high, the model is reduced to:
 - average vulnerabilities of his friends weighted by their trust levels.

$$Y^{(t)} = 1 * M Y^{(t-1)} + (1 - 1) Y^{(t-1)} \quad (3)$$

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

- In the absence of influence, the model is reduced to:
 - his own vulnerability weighted by the level of mistrust of his friends

$$Y^{(t)} = 0 * M Y^{(t-1)} + (1 - 0) Y^{(t-1)} \quad (3)$$

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

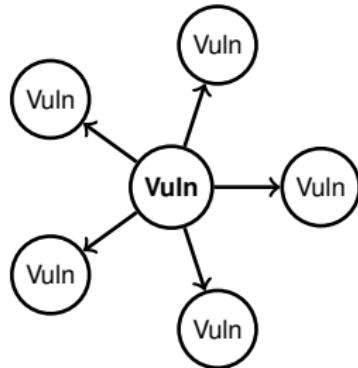


Figure 9: Social vulnerability.

Plan

- 1. Introduction
 - 2. Contribution
 - 3. Conclusion
- 1. Related work
 - 2. Diffusion process
 - 3. Experimentation**
 - 4. Results exploitation

Email datasets

Experimentation

| Parameter | Value |
|---------------------|----------|
| Users | 958 |
| Messages | 6966 |
| Diameter | 958 |
| # of msg on average | 2.413361 |
| Msg density | 0.00252 |
| Modularity | 0.654600 |
| Average distance | 3.042114 |

Table 5: Enron dataset properties.



Figure 10: Enron logo.

| Parameter | Value |
|---------------------|----------|
| Users | 5885 |
| Messages | 26547 |
| Diameter | 2096 |
| # of msg on average | 9.02192 |
| Msg density | 0.001533 |
| Modularity | 0.86526 |
| Average distance | 3.914097 |

Table 6: Caliopen dataset properties.



Figure 11: Caliopen logo.

Plan

- 1. Introduction
- 2. Contribution
- 3. Conclusion
 - 1. Related work
 - 2. Diffusion process
 - 3. Experimentation
 - 4. Results exploitation

Results exploitation

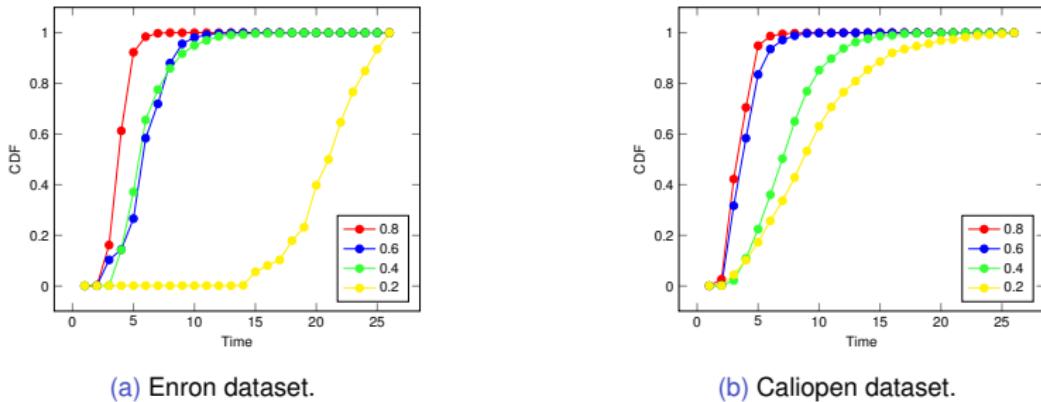
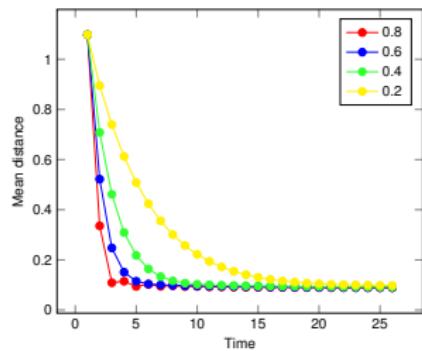


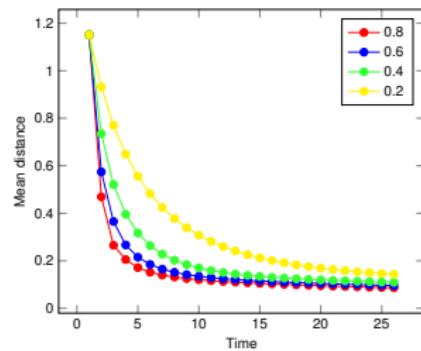
Figure 12: Cumulative distribution function of infected users.

- Figures shows the CDF of the vulnerability diffusion process.
- The vulnerability diffusion process increases as the reputation level of vulnerable users increases.
- Users with high reputation values contribute significantly to the diffusion
 - They spread their vulnerabilities quickly and widely through the network.

Results exploitation



(a) Enron dataset.



(b) Caliopen dataset.

Figure 13: Convergence of the diffusion process.

- The process converge when the mean distance between social vulnerability scores is the minimum.
- Assigning trust to vulnerable users allows them to achieve a high level of reputation.
- Consequently, they infect all other vulnerability values.

Results

Comparison

Initial values:

- generated randomly (normal distribution)
- represent individual vulnerabilities.
- dark color = highly infected

Final values:

- obtained after convergence.
- represent social vulnerabilities.

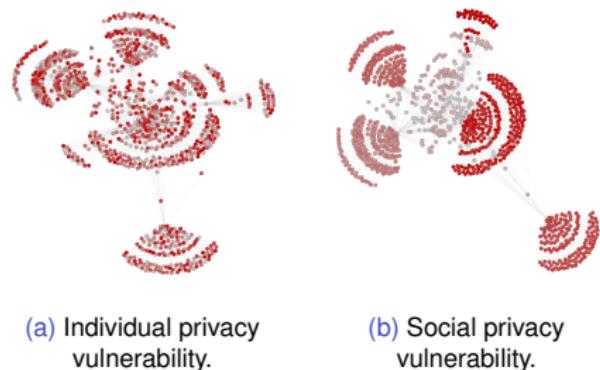


Figure 14: Individual & Social privacy vulnerabilities.

| User ID | Individual Vul | Social Vul |
|---------|----------------|------------|
| 34 | 0.84 | 0.67 |
| 67 | 0.12 | 0.87 |
| 206 | 0.76 | 0.33 |
| 588 | 0.23 | 0.78 |

Table 7: Individual and social privacy vulnerabilities.

Plan

1. Introduction

2. Contribution

3. Conclusion

Conclusion

- ➡ The purpose of this work is to simulate a diffusion process of individual vulnerabilities.
 - ➡ The vulnerability of one user is the vulnerability of all users.
 - ➡ At the end of the diffusion (convergence), all users gets their social vulnerability scores.
- ➡ Future work
 - ➡ To propose mechanisms to improve the reputation of non-vulnerable users.
 - * Suggest well known interlocutors with acceptable vulnerability scores.
 - ➡ To propose mechanisms to improve the vulnerability of reputed users.
 - * Recommend configurations and software.

Conclusion

- ➡ The purpose of this work is to simulate a diffusion process of individual vulnerabilities.
 - The vulnerability of one user is the vulnerability of all users.
 - At the end of the diffusion (convergence), all users gets their social vulnerability scores.
- ➡ Future work
 - To propose mechanisms to improve the reputation of non-vulnerable users.
 - * Suggest well known interlocutors with acceptable vulnerability scores.
 - To propose mechanisms to improve the vulnerability of reputed users.
 - * Recommend configurations and software.

Thank you !

References

- [1] [Nombre d'e-mails envoyés par jour dans le monde 2017-2022 | Prvision](#), [Online; accessed 1. Mar. 2019], Mar. 2019.
- [2] E. M. Maximilien, T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu, " Privacy-as-a-Service: Models, Algorithms, and Results on the Facebook Platform," in *Proceedings of Web*, 00054, vol. 2, 2009.
- [3] A. E. Gandouz, " PROTECT_U: Un Systeme Communautaire Pour La Protection Des Usagers de Facebook", p. 77, 2012, 00001.
- [4] L. Fang and K. LeFevre, " Privacy Wizards for Social Networking Sites", 00397, ACM Press, 2010, p. 351.
- [5] D. Frey, A. Jégou, and A.-M. Kermarrec, " Social Market: Combining Explicit and Implicit Social Networks," in *Stabilization, Safety, and Security of Distributed Systems*, ser. Lecture Notes in Computer Science, 00019, Springer, Berlin, Heidelberg, Oct. 10, 2011, pp. 193–207.
- [6] Yongbo Zeng, Yan Sun, Liudong Xing, and V. Vokkarane, " A Study of Online Social Network Privacy Via the TAPE Framework," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1270–1284, Oct. 2015, 00003.
- [7] S. Hameed, X. Fu, P. Hui, and N. Sastry, " 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.
- [8] T. Tran, J. Rowe, and S. F. Wu, " Social Email: A Framework and Application for More Socially-Aware Communications," in *Social Informatics*, L. Bolc, M. Makowski, and A. Wierzbicki, Eds., vol. 6430, 00000, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 203–215.
- [9] R. K. Nepali and Y. Wang, " SONET: A SOcial NETwork Model for Privacy Monitoring and Ranking", 00021, IEEE, Jul. 2013, pp. 162–166.