Strengthening Weak Identities Through Inter-Domain Trust Transfer

Giridhari Venkatadri, Oana Goga, Changtao Zhong, Bimal Viswanath, Nishanth Sastry, Krishna Gummadi
Trustworthiness of online identities
Trustworthiness of online identities

Trustworthiness of an identity: The likelihood that the identity will respect the terms of service (ToS) of its domain in the future
Online identity-infrastructures

Trusted certificate

strong identity-infrastructure

weak identity-infrastructure

oana.goga@mpi-sws.org
Online identity-infrastructures

**Accountability**
- Trusted certificate: Yes
- Weak identity-infrastructure: No

**Anonymity**
- Trusted certificate: No
- Weak identity-infrastructure: Yes

**Adoption**
- Trusted certificate: No
- Weak identity-infrastructure: Yes

**Resistance to fake identity attacks**
- Trusted certificate: Yes
- Weak identity-infrastructure: No
Online identity-infrastructures

- Accountability: ✔️
- Anonymity: ✗
- Adoption: ✗
- Resistance to fake identity attacks: ✔️

Strong identity-infrastructure:
- Trusted certificate
- oana.goga@mpi-sws.org

Weak identity-infrastructure:
- Trusted certificate
- oana.goga@mpi-sws.org

Up to 40% of newly created identities on Twitter are malicious!!
Online identity-infrastructures

Challenge: How to reason about the trustworthiness of weak identities?

Accountability
Anonymity
Adoption
Resistance to fake identity attacks

Up to 40% of newly created identities on Twitter are malicious!!
Trustworthiness of weak identities

Current techniques: Based on the past activity of each identity within the domain

Limitation: Domains need to observe the behavior of weak identities over time (time lag)

• Malicious users can still exploit new identities to misbehave
• Honest users must wait to acquire access to resources (e.g., Reddit posting quotas)
**Key idea**

Strengthen weak identities through inter-domain trust-transfer

Trusted certificate
Key idea

Strengthen weak identities through inter-domain trust-transfer

- Use the weak identities of users on other domains as external trust certificates
Why would this work?

1. Many hone users maintain weak identities on multiple domains
2. Users already interconnect their identities (e.g., social login)
3. Malicious attackers would incur additional costs
4. More established domains could provide good trust references for newer domains
This talk

1. Potential for inter-domain trust transfer
2. Inter-domain trust transfer framework
3. Leverage inter-domain trust transfer for identity curation
This talk

1. Potential for inter-domain trust transfer
2. Inter-domain trust transfer framework
3. Leverage inter-domain trust transfer for identity curation
Potential for inter-domain trust transfer

Can activity signals from Facebook and Twitter help Pinterest reason about trustworthiness better?

Dataset
- 1.7M random identities on Pinterest, and their matching identities on Facebook and Twitter
- Activity signals computed based on public data on Twitter and Facebook (e.g., account age, # followers, suspension)
- Diverse set of untrustworthy identities on Pinterest
Source domain and trustworthiness

(activity signal)

(Fraction of blocked pins)

(Fraction of identities)

(untrustworthiness on Pinterest)
Correlation between distrustworthiness on Pinterest and the choice of the source domain (untrustworthiness on Pinterest)
Suspension signal and trustworthiness

(activity signal)

Fraction of identities suspended vs. Fraction of blocked pins

Facebook
Twitter

(untrustworthiness on Pinterest)
Suspension signal and trustworthiness

Untrustworthy Pinterest identities are more likely to be suspended on Twitter (but not on Facebook!)

(untrustworthiness on Pinterest)
This talk

1. Potential for inter-domain trust transfer
2. Inter-domain trust transfer framework
3. Leverage inter-domain trust transfer for identity curation
This talk

1. Potential for inter-domain trust transfer
2. Inter-domain trust transfer framework
3. Leverage inter-domain trust transfer for identity curation
Inter-domain trust transfer framework

Source domains

S1

S2

Sn

Target domain
Inter-domain trust transfer framework

What are the challenges?
1. How to link the matching identities of a user?
1. How to link the matching identities of a user?

Source domains

Target domain

Sn

S1

S2
1. How to link the matching identities of a user?

Solution: single sign-on protocols
1. How to link the matching identities of a user?

This can be done in an anonymous way as well!

Solution: single sign-on protocols
2. What information to export?
2. What information to export?
2. What information to export?

Ideal information:
- Useful for the target domain
- Do not ruin the privacy of users
2. What information to export?

Ideal information:
- Useful for the target domain
- Do not ruin the privacy of users

Solution:
- Each source domain can choose the information it wants to transfer
- The source domain can ask the permission of the user (e.g., OAuth)
- Break correlation with possible sensitive information (e.g., L-diversity, t-closeness)
3. How to interpret and combine the information?

Inf(100) 100 followers

Inf(1000) 1000 likes
3. How to interpret and combine the information?

Solution: Target domain needs to do a calibration step (e.g. using a classifier and all available activity signals)
This talk

1. Potential for inter-domain trust transfer
2. Inter-domain trust transfer framework
3. Leverage inter-domain trust transfer for identity curation
This talk

1. Potential for inter-domain trust transfer
2. Inter-domain trust transfer framework
3. Leverage inter-domain trust transfer for identity curation
Identity curation

Curated set of identities: a set of identities with high probability to be trustworthy

Why curate?
I. Early access to elevated privileges
II. Sybil-resilient content recommendation

Question:
Can activity signals from Facebook/Twitter help Pinterest:
• Curate more identities?
• Curate identities early-on?
Pinterest can curate more identities.
Pinterest can curate more identities
Pinterest can curate more identities

Trust transfer allows to curate more than twice as many identities!!
Pinterest can curate identities early-on
Pinterest can curate identities early-on
Pinterest can curate identities early-on

Trust transfer allows to curate identities up to 15 months in advance!!
Conclusions

• Lack of external trust certificates for weak identities could be mitigated by user’s weak identities on other domains
  • Users can keep their identities anonymous!
• Inter-domain trust transfer framework
  • Low deployment overheads
  • Without significant loss of privacy
• Evaluation on real-world domains is very promising!
  • Even simple activity signals go a long way