Online Social Network Platforms: Toward a Model-Backed Security Evaluation

Erwan Le Malécot, Mio Suzuki, Masashi Eto,
Daisuke Inoue, Koji Nakao

National Institute of Information and Communications Technology

2012

Introduction

- Online Social Network (OSN) platforms: essentially platforms that build upon the digital expression of social relationships to put their users in relation with each other and enable them to share resources accordingly.
- Presently enjoying an ever growing popularity (e.g. Facebook, etc.), but at the same time, are also increasingly pointed at for security/privacy issues stemming from their usage.
- Growing body of literature discussing those issues, but most of the corresponding research efforts actually turn out to be extremely focused on the particulars.
- Believe that adopting a more formal/general approach could provide further insight into the problem. . .

Introduction (Cont'd)

- Incentive: achieve a better understanding of the inherent risks associated with OSN platforms → identification of likely attack patterns + preemptive design of generic countermeasures.
- To this end, proposal of a conceptual model of the functioning of OSN platforms → tying of user actions to their effect on the internal data abstraction maintained by such platforms.
- Originality: integration of the notion of resources as first-class entities in the model → better suitability for security-oriented assessment (cf. most of the malicious activity targeting OSN platforms somehow revolving around "shared" resources).
- Inception. . .

Preliminary Observations

- A multitude of thriving OSN platforms: some generic, some much more targeted (e.g. collective enjoyment of specific hobbies, establishment of business relationships, etc.).
- Look diverse but most actually share the same core formula: centralized architecture + Web-based interface for access (+ tight integration with the rest of the World Wide Web).
- Also rather uniform modus operandi: registration, credentials selection, profile creation, mingling + sharing...
- Approach: try to derive a generic representation from the displayed similitudes.

Abstraction

- Extracted core set of functionalities → registered users are enabled: ① to create a protected digital representation of themselves on the platform, ② to define connections with other registered users based on social affinities, ③ to publish resources and to make them available to other users, and ④ to browse the resulting pool of content by connectivity.
- Can then view OSN platforms as the combination of 2 basic parts: the social graph formed by their registered users linked through the relationships they specify among themselves + the pool of resources published by those users (which can also be seen as a graph in the Web context).
- Most previous (modeling) works dealing mainly/solely with the social graph component. . .

Motivation

Justification

- Came to realize that most contemporary attack scenarios centered around user generated resources, with attackers either trying to get illegitimate access to that content, or to "corrupt" it (cf. spam → scam pattern, etc.).
- Key to deal with such attacks: comprehending how those resources fit into the big picture...

Related Works

- A few proposals aiming at the modeling of OSN platforms, however from our review: incomplete or far too detailed (for our purpose) → quest for the "right" level of abstration...

Definition

Overview

- Model made of 2 complementary parts: an abstract depiction of the data structure exposed by OSN platforms + a rendition of their users and of the set of actions available to them.

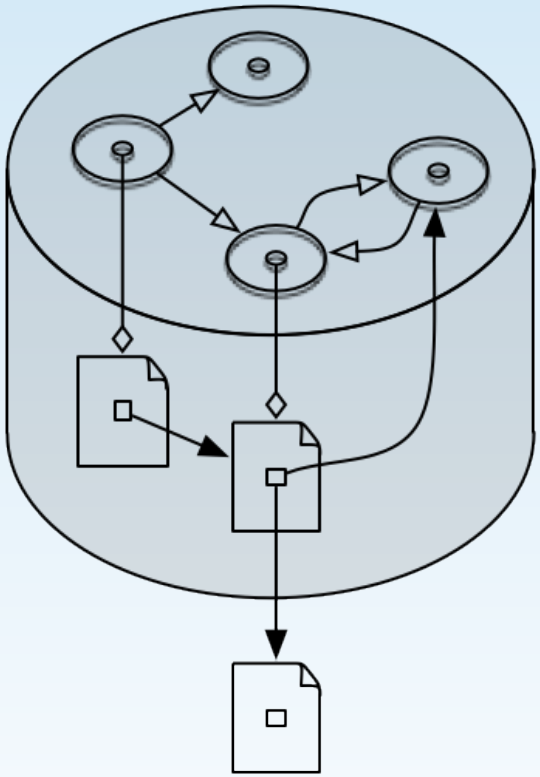
Structure

- Each OSN platform portrayed as a vertex-labeled directed graph (cf. its *operational graph*) whose vertices stand either for identities registered by users on the platform (i.e. *Id nodes*), or resources published by them (i.e. *Rs nodes*).
- Arcs of the graph associated with different meanings depending on the labels of their ending nodes. . .

Definition (Cont'd)

Arc Semantics

- **(Id** *a*, **Id** *b***)** arc ⇔ *a* *is trusted by* *b* (cf. *a* was accepted as a "friend" by *b*).
- **(Id** *a*, **Rs** *x***)** arc ⇔ *a* *owns* *x* (cf. *x* was published by *b* on the platform).
- **(Rs** *x*, **Rs** *y***)** arc ⇔ *x* *refers to* *y* (cf. *x* embeds a mention to, or part of *y*).
- **(Rs** *x*, **Id** *a***)** arc ⇔ *x* *refers to* *a* (cf. tagging of *a* on *x*).



Glue

Remarks

- Social graph of an OSN platform materialized by the induced subgraph formed by the Id nodes of its operational graph.
- Topological features of such defined graphs (cf. as derived from actual OSN platforms)?

Consumers

- Entities that interact with the previously defined structure → to be modeled as *active graph crawlers*.
- "Active": appointed ability to modify the constitution of the op. graph they are interacting with.

Operations

Management

- **`accessAs(Id` *i*`)`**: specifies the root Id node *i* from which the consumer is to start crawling the op. graph + identity under which subsequent operations are to be realized.
- **`register(Id` *i*`)`**: append Id node *i* to the op. graph.
- **`unregister(Id` *i*`)`**: remove Id node *i* from the op. graph, iff *i* is the consumer's current root node.
- **`publish(Rs` *r*`)`**: append Rs node *r* to the op. graph, *r* to be linked by an (Id, Rs) arc to the consumer's current root node.
- **`unpublish(Rs` *r*`)`**: remove Rs node *r* from the op. graph, iff *r* linked by an (Id, Rs) arc to the consumer's current root node.

Operations (Cont'd)

Connecting

- **`link(Nd` n_1`, Nd` n_2`)`**: create an arc from node n_1 to node n_2, subject to the following conditions depending on the nature of the arc...
  - **`(Id, Id)`**: iff n_2 is the consumer's current root node.
  - **`(Id, Rs)`**: unavailable (cf. **`publish`**).
  - **`(Rs, Rs)`**: iff n_1 is "owned" by the consumer's current identity.
  - **`(Rs, Id)`**: iff n_1 is "owned" by the consumer's current identity.

  Additional condition: node linked from/to is to be "known" to the consumer (cf. "crawling" definition/description).
- **`unlink(Nd` n_1`, Nd` n_2`)`**: delete an existing arc from node n_1 to node n_2, subject to the same conditions as **`link`**.

Operations (Cont'd)

Crawling

- **`followArc(Arc` *a*`)`**: crawl arc *a* and learn about the node at its end (cf. node now considered as known to the consumer).
- **`getArcs(Nd` *n*`)`**: retrieve the set of outgoing arcs from known node *n*.

Usage

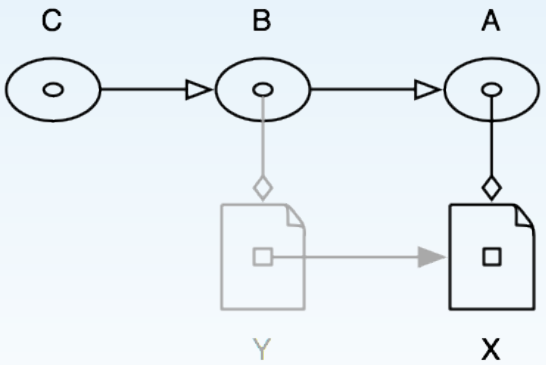
- Consumer activity: succession of graph discovery phases (cf. via crawling operations from their root Id nodes), and graph manipulation phases → by design, such modifying operations only made available on the discovered subgraph.
- Bootstrapping?

Extensibility

- Notion of “public” resources which are made freely accessible regardless of connectivity → definition of an auxiliary identity (cf. the “collective” identity) which is made to trust all other identities, and can in turn be trusted by willing consumers.
- Comments: difference with “classic” resources essentially the fact that a comment is automatically referred back to by the resource it refers to → adding of the following **`tie`** operation (to be used in conjunction with **`publish`**).
  - **`tie(Rs`** r_1**`, Rs`** r_2**`)`**: create an arc from owned Rs node r_1 to known Rs node r_2, a second arc from r_2 to r_1 being then reciprocally created.
- Finally, warrant creation of links to external resources (i.e. not part of the considered OSN platform) from internal ones.

Access Control?

- Expectation that only the entity that “registered” an identity is to be allowed to subsequently “assume” that identity on the OSN platform → need for authentication mechanisms, e.g. binding the use of **`accessAs`** to a prior use of **`register`**.
- Other occurrence: ability of a consumer to restrict access to the resources that he publishes to a set of specific identities.



- Common policy: possibility to restrict such access to his set of “friends”, but not so trivial to implement/get right in practice → future work. . .

Approach(es)

- Envision 2 main ways of exploiting our model in relation with the security of OSN platforms: ① a bottom-up approach focusing on the uncovering of potential attack patterns from the review of the list of operations available to attackers, and ② a top-down approach focusing on the investigation of observed concrete attacks through their decomposition into a sequence of elementary operations.
- Main goal: gain some insight into how to devise mitigation mechanisms against such identified/analyzed attacks.
- Design of behavior-based evaluation mechanisms toward the identification of the consumers exhibiting malicious intent (cf. modeling of those consumers).

Attack Scenarios

- Attack model: assume that malicious individuals can make use of any of the operations that we previously defined as available to consumers to achieve their goals.
- Supplemented by identity theft + the registration of multiple identities for their own use (cf. sybil attacks on the system).
- Privacy breach: the attacker managing to get his hand on a piece of information considered as confidential by operational standards → managing to learn about, and follow an arc to a coveted resource.
- Security breach: the attacker managing to compromise the running environment of a targeted user → managing to lure that consumer into following an arc to a previously arranged "booby-trapped" resource.

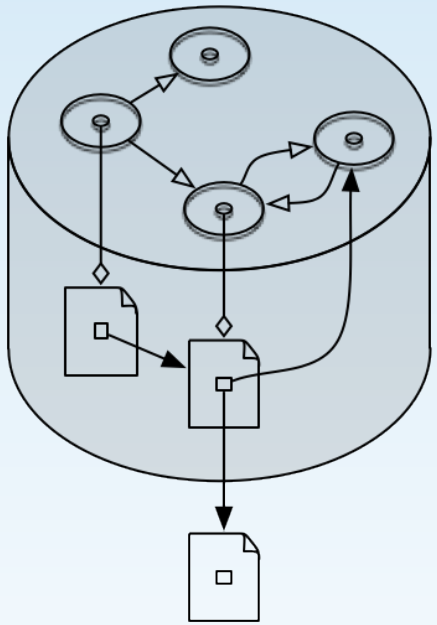
Attack Scenarios (Cont'd)

- Therefore, notion of privacy: intrinsically linked to the ability of the attacker to crawl the operational graph, and how large a portion of it → the attacker attempting to artificially extend his "reach" (e.g. compromise of well-connected identities, use of social engineering techniques to induce trust, etc.)
- Notion of security: the attacker's strategy would rather be to increase the proportion of the operational graph under his control (cf. proportion of booby-trapped nodes) + to increase their connectivity so as to boost their chances from being reached by unwary consumers...

Ramifications

“Dangerousness” of an Attacker

- In terms of privacy: correlated with the characteristics of the forest of (crawlable) directed trees springing from the root Id nodes under his control (cf. arcs directed away from the roots).
- In terms of security: correlated with the characteristics of the forest of trees rooted on the Rs nodes under his control, arcs of the trees being this time directed toward their roots.



Leads

- We expect the study of those forests (cf. as extracted from actual platforms, or artificially built through simulation) to give out some hints on the latent capabilities of attackers based on the set of “raw materials” put at their disposal (e.g. availability of the **`tie`** operation on the targeted OSN platform, or not).
- Then, once a Rs/Id node is identified as nefarious, the study of the surrounding portion of operational graph could help uncover additional identities that might have been colluding to make that node more “visible” on the platform. . .
- Practicality of seek and destroy attack scenarios (cf. **`unlink`**, **`unpublish`**, **`unregister`**)?

Conclusion

Summary

- Formulation of an abstract model of the workings of an OSN platform, aiming at providing a ground for a more systematic evaluation of their security → stripped-down representation of the data abstraction maintained by OSN platforms + set of operations provided to their users for interaction.

Future Work

- Evaluation based on concrete datasets extracted from a number of actual OSN platforms (+ simulation. . .).
- Model of some use in other research areas?

Any questions/comments?