Attack Spectrum and Countermeasures

Introduction

- Diversity of OSN platforms opens doors for a variety of attacks
- Attacks are done in 3 areas:
- Privacy of the users - refers to the ability of an individual to control and selectively disclose information about him
- Integrity of their profiles - to prevent any unauthorized modification or tampering of user-generated content and profile information
- Availability of the user-provided contents - aims at assuring the operability of the social network services in the face of attacks and faults

Attacks vs Security Objectives

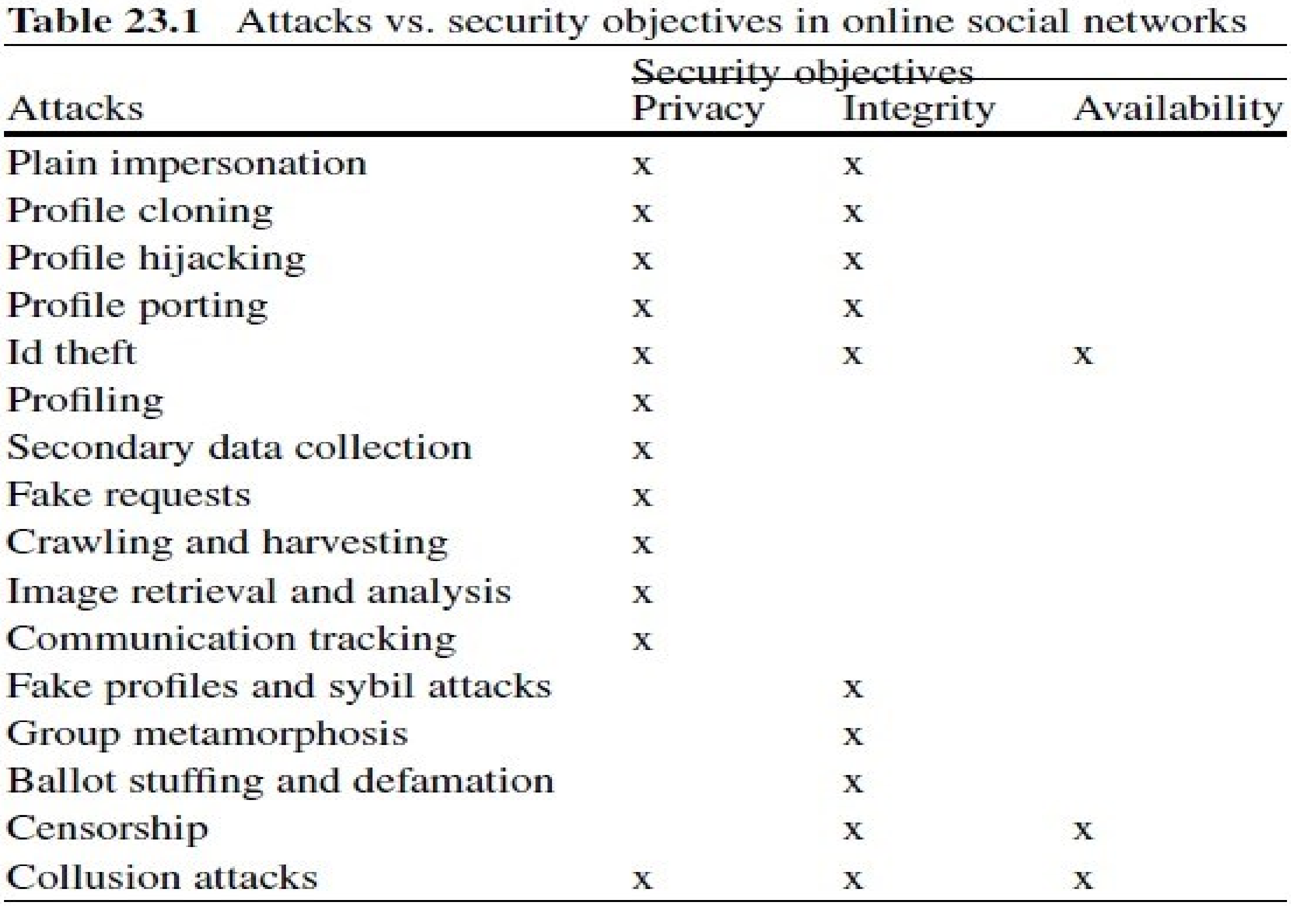

Table 23.1 Attacks vs. security objectives in online social networks

	Security objectives		
Attacks	Privacy	Integrity	Availability
Plain impersonation	x	x	
Profile cloning	x	x	
Profile hijacking	x	x	
Profile porting	x	x	
Id theft	x	x	x
Profiling	x		
Secondary data collection	x		
Fake requests	x		
Crawling and harvesting	x		
Image retrieval and analysis	x		
Communication tracking	x		
Fake profiles and sybil attacks		x	
Group metamorphosis		x	
Ballot stuffing and defamation		x	
Censorship		x	x
Collusion attacks	x	x	x

1. Plain Impersonation

- Adversary can participate in OSN applications on behalf of impersonated user
- Success of attack depends on the authentication mechanisms deployed during registration process
- Prominent secondary effect - misuse of trust that users inherently have in messages Ex. 419 Scam
- **Countermeasures:**
- Thwarted through stronger authentication techniques
- Require some real-world identification prior to user switching on her account

2. Profile Cloning

- Create new profile using the same (or similar)content as existing one
- As users hide email address, difficult for OSN Providers to distinguish between the original profiles and their clones
- Taking this advantage, adversary creates confusion through impersonation – gain access to private info’ of registered users
- profile cloning can be automated – tools like iCloner
- **Countermeasures:**
- Detect similarities between profiles - Cloned profiles usually have later registration date

3. Profile Hijacking

- Obtain control over some existing profile within an OSN platform
- Technically viewed successful if the adversary can obtain passwords of other users
- majority users choose weak passwords can be recovered via an automated dictionary attack
- adversary obtain passwords via social-engineering attacks such as phishing – users use same password for many sites
- Can distribute messages to direct users to fake login websites
- OSN providers themselves have full control over registered profiles

Contd...

- **Countermeasures:**

- Restricting number of login attempts or using human interaction CAPTCHAs

- If some profile appears more attractive to be hijacked, password access to profile can be changed

4. Profile Porting

- Another type of impersonation
- Profile exists in one OSN platform is cloned into another OSN platform
- Unknown to user as she will not have profile in all platform to visit
- OSN platforms cannot distinguish amongst ported profiles
- **Countermeasures:**
- Need profile similarity detection tools work across different platforms
- To deploy such tools require cooperation amongst the providers
- Problem - OSN providers are cautious in granting access to their profile database to competitors.

5. ID Theft

- Should be able to convince anyone about the ownership of some particular OSN profile
- Adversary misuse the reputation or expertise of the real profile owner
- Owner unaware of the attack
- A successful ID theft attack takes control over the target profile
- Requires same effort as profile hijacking attack
- Adversary suffice to claim the ownership of a profile and perform communication via other channels

Contd...

- **Countermeasures:**

- Thwarting ID theft attacks by technical means impossible

- Only solution to rely on other means of real-world identification (national identity cards, driver’s licenses, etc.)

6. Profiling

- OSNs provide users to express themselves via application such as forums, guest books, discussions, polls, multimedia data, etc.
- Adversary observes collect publicly information about OSN activities in automated way
- **Countermeasures:**
- Fine-grained access control and anonymizing techniques
- Allow access to the profiles based on individual basis not on roles
- Users decide whether their activities (e.g. discussion comments) should be kept unlinkable to their profile

7. Secondary Data Collection

- Attacker aims to collect information about profile of owner via secondary sources

- Internet search engine and Internet service are used to collect and aggregates all information

- Obtain more information than available from profile

- misuse it against the user both in the virtual environment of OSN platform and in real life

- Public and private profiles on different platforms simplifies attacker task

- **Countermeasures:**
- Measures not possible for OSN providers

- users limit information kept in profile to avoid linkability with secondary sources

8. Fake Requests

- An adversary with own OSN profile sends *fake requests to other users* to expand his own network

- Dissemination of fake requests can be automated

- Since most OSN users tend to accept fake requests, it simplifies adversary task

- Access profiles on direct or nth grade connections

- **Countermeasures:**

- OSN cannot restrict requests (improve connections is aim of SN), it is left to user responsibility

9. Crawling and Harvesting

- *Crawling collects and aggregates publicly available information* across multiple OSN profiles and applications in an automated way

- Attack does not target any particular user

- First step in crawling , expand his network through fake requests to collect public info as much possible

- Collected info is misused for different purposes - selling data to marketing agencies, offline analysis targeting attacks on OSN users

Contd...

- **Countermeasures:**
- Through CAPTCHA's, but can be bypassed by tools
- Harvesting - adversary simultaneously crawls across different OSN platforms
- Results in larger datasets on private information about the OSN users

10. Image Retrieval Analysis

- An automated attack aiming to collect multimedia data (incl. images, videos, etc.) available with the OSN platform
- Next analysed via automated pattern recognition tools to find links to the OSN profiles of displayed users
- Can reveal more private information about users than they are willing to give
- Analysis of digital content further strengthened by considering secondary sources (search over the Internet)
- **Countermeasures:**
- A more restrictive access control policies for the digital content.

11. Communication Tracking

- *A profiling attack aiming to reveal information* about communications of the same user

- Attacker may collect more information about the user than available in the profile

- Done in an automated way by searching for comments left by the target user in various OSN applications

12. *Fake Profiles and Sybil Attacks*

- OSN users can creates several profiles under possibly different identities and contents in various platforms
- Lack of proper authentication makes creation of *fake profiles becomes easy*
- *It* paves way for *Sybil attacks that may serve different purposes*
- fake profile owners establish new connections without disclosing their real identities
- It allows to obtain more information than using some real account
- Sybil accounts can be misused for – distribution of spam messages, illicit content such as malware, phishing links, illegal advertisement, bias of deployed reputation systems, etc.

13. *Group Metamorphosis*

- *Group metamorphosis is an attack where group administrators change* the group subject to persuade own interests, e.g. Political

- Group earlier may remain unaware of this change, which in turn may have negative impact on their reputation

- **Countermeasures:**

- To restrict control of administrators over the interest groups, from modifying any information that may have impact on the group as a whole

14. *Ballot Stuffing and Defamation*

- *Ballot stuffing we understand an attack by which the* attacker wishes to increase public interest to some target OSN user

- Increase personal messages resulting target user in a DoS attack on the physical resources, may place victim in embarrassing discussions

- Conversely, increases popularity of the profile belonging to the attacker

- Achieved through recommendations submitted by the attacker using fake profiles

Contd...

- *Defamation attacks aim at decreasing* public interest of a target user, in particular by tarnishing the reputation of the latter

- leads to blacklisting of the user in contact lists – not allowing communications

- Further have negative impact on the user’s life in the real world

- Another form of defamation is the anti-advertising against companies aiming to damage the reputation of the latter on the market

15. Censorship

- It is the ability to prevent dissemination of illicit content
- Applied without substantial reasons have negative impact on users
- Misuse of censorship – Ex. Advertisement of expertise of business contacts users, misused to favor some users over their competitors
- Other facets of censorship - target manipulation of search engines within the network
- Censorship applied by administrators of shared interest groups also
- Chances to modify or drop messages of group members
- Restricting group administrators not effective measure as it contradicts the responsibility of group administrators for the content disseminated within the group

16. Collusion Attacks

- Several users join their malicious activities to damage other OSN users or mount attacks against applications of the OSN platform
- Colluding users - start defamation or ballot stuffing campaigns, increase each over reputations, bias the outcome of public polls or influence public discussions
- Have valid OSN profiles creation of fake profiles not needed
- IP trace-back not possible if colluding users do not deploy any additional proxies