

Social Networking Sites Security

Social networks contain plethora of personal information:

- ▶ Real name, profile picture, email address
- ▶ Friends, social surrounding, locations
- ▶ Events, "Likes", hobbies
- ▶ Possibly much, much more

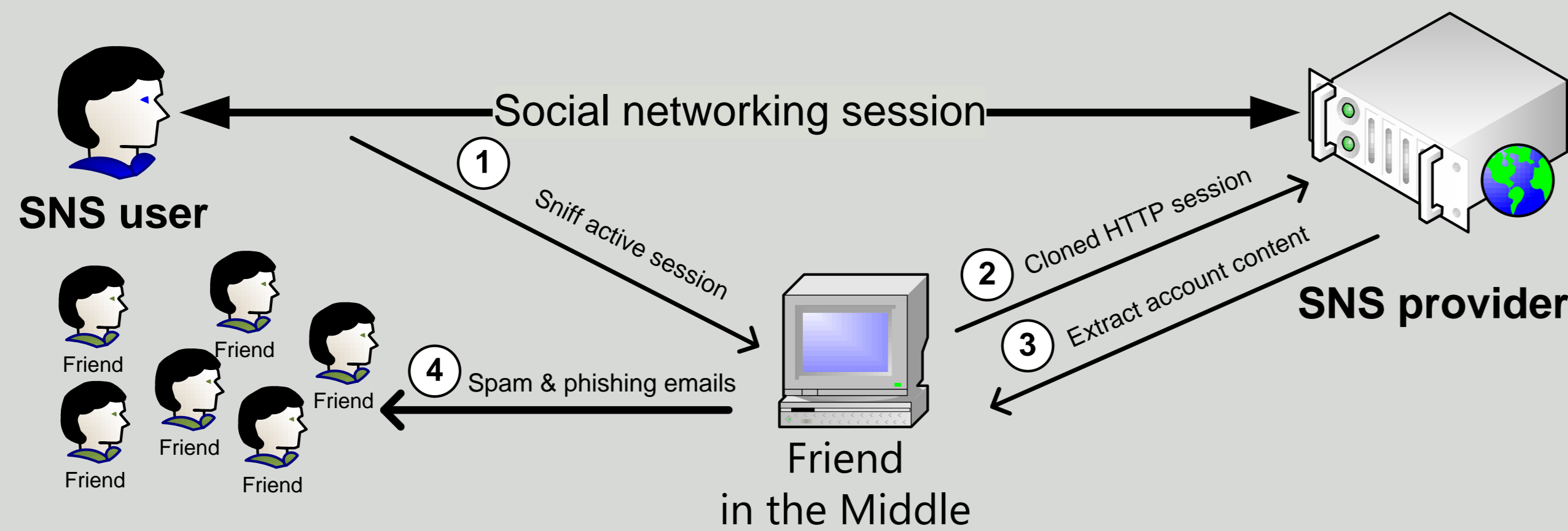
All networks have only weak security on the network layer:

- ▶ No encryption (HTTPS)
- ▶ Weak session management
- ▶ Only "reactive" security

Social Networking Site		
Name	Claimed users	HTTPS
Facebook	500×10^6	Login only
Friendster	110×10^6	No
Orkut	100×10^6	Login only
hi5	80×10^6	No
LinkedIn	60×10^6	Login only

Table: Top five social networking sites and their support for HTTPS.

Our FITM Attack



FITM - Friend in the Middle Attack

- ▶ Traditional session hijacking for social network communications
- ▶ Either actively (Botnet, ...) or passively (unencrypted Wifi, ...)
- ▶ Undetectable to the
 - ▷ client
 - ▷ social network operator
- ▶ Can be used to *retrieve* or *publish* social network data
- ▶ Foundation for further attacks on the users

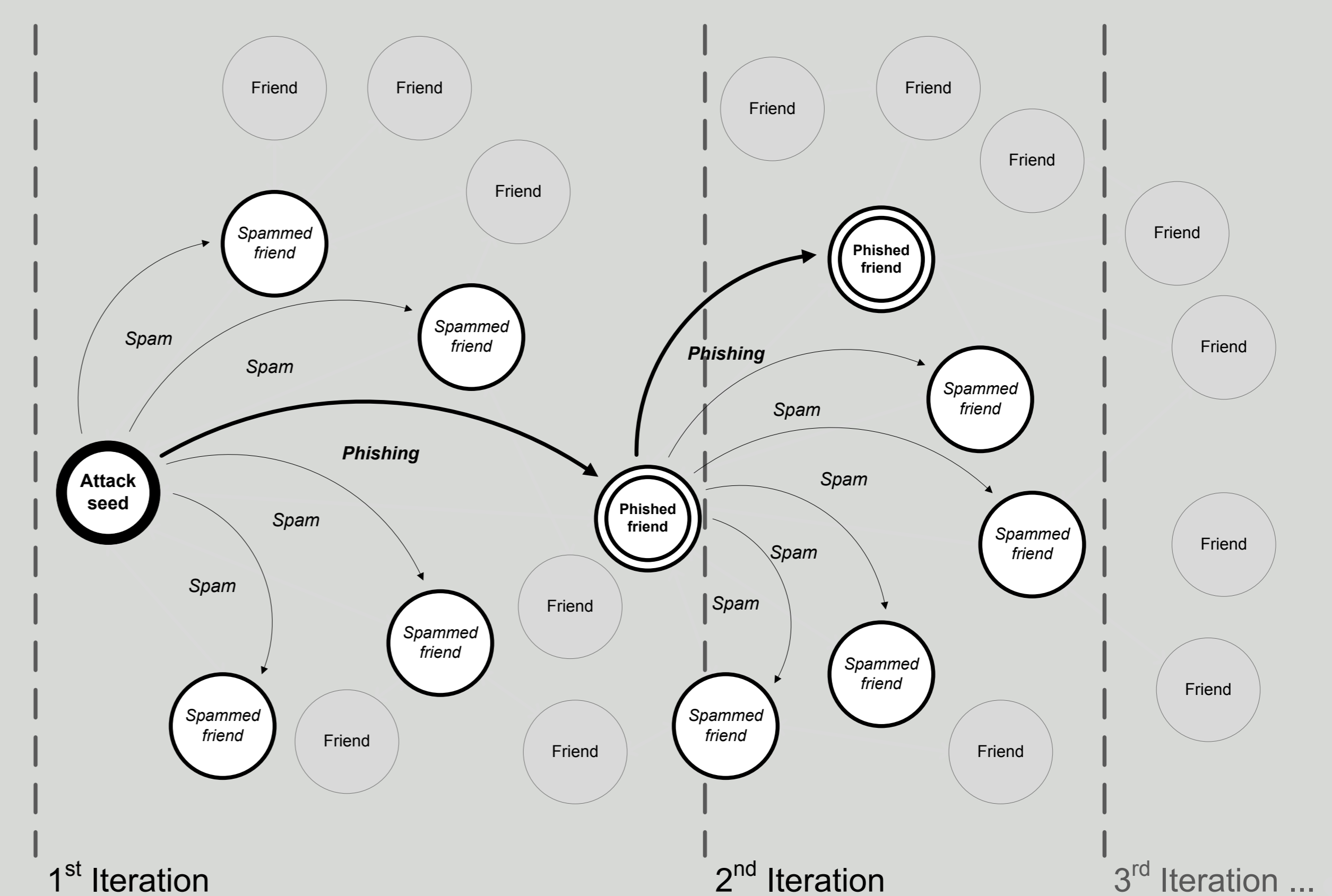
Attack Cycle

Attack cycle:

1. Sniff network for social network connection
2. Clone HTTP header and authentication cookies
3. Acquire all available data, either by
 - ▷ installing custom third-party application, or
 - ▷ adding malicious account with full data access
4. Generate tailored spam & phishing messages
 - ▷ publicly to all friends e.g., comments or wall posts
 - ▷ social network private messages
 - ▷ "offline", e.g., email or IM
5. For every successfully phished friend: start from 1

Countermeasures:

- ▶ Secure social network architecture
- ▶ User education



Consequences

Social Phishing

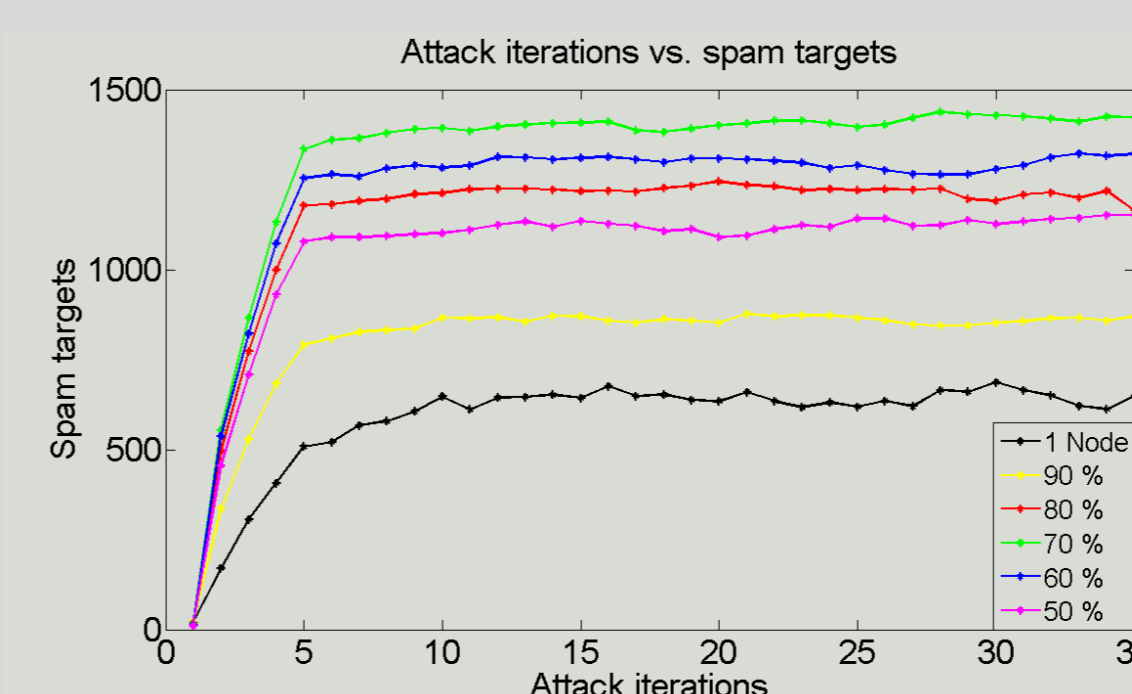
- ▶ "Social" information increases effectivity, 16% to 72% according to [Jagatic et al., 2009]
- ▶ Based on the social graph
- ▶ Improves with "friendship metadata", like recent communications or shared events
- ▶ Basically automated social engineering

Context-Aware Spam

- ▶ Relationship-based attack
- ▶ Unshared-attribute attack
- ▶ Shared-attribute attack
- ▶ according to [Brown et al., 2005] e.g., electronic birthday card, picture gallery, ...

Modelling propagation strategies

- ▶ Simulating social graph with a *configuration model*
- ▶ Graph properties:
 - ▷ no loops
 - ▷ degree of nodes according to power law distribution
 - ▷ number of nodes: 10^4



Conclusion

Problems in Research

- ▶ Impossible to do "in the wild"
- ▶ Social networking sites have no incentives to release social graph
- ▶ Legal questions
- ▶ Ethical questions:
 - ▷ How to obtain "attack seeds"
 - ▷ How to get consent from users?
- ▶ Simulation can only solve parts of the problems

Conclusion

- ▶ Powerful attack method
- ▶ Hard to defend against
- ▶ All deployed social networks vulnerable

Future research:

- ▶ Are future generation social networks (Peerson, Diaspora, ...) secure by design?
- ▶ Are people really falling for social phishing?