Research Overview

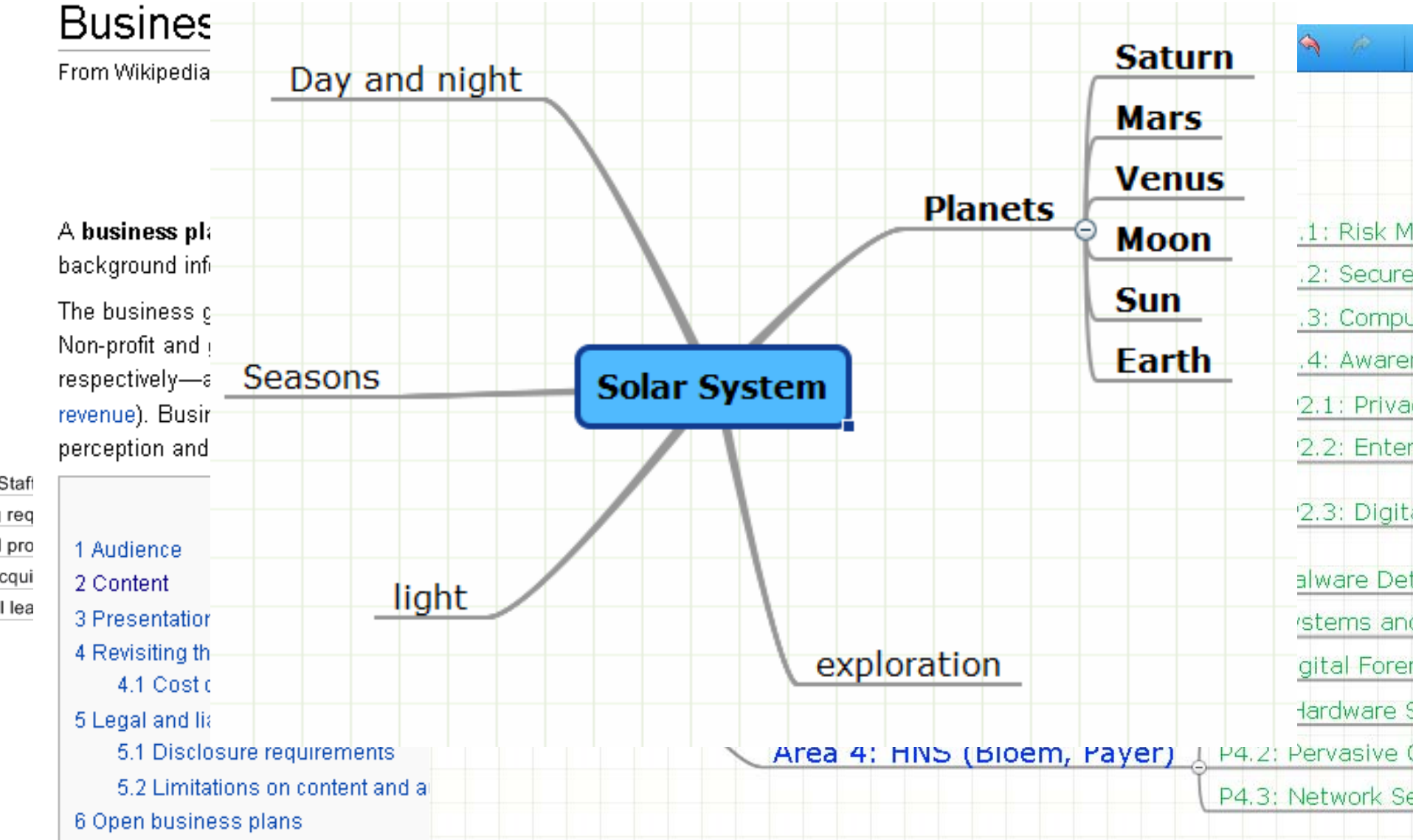
SBA Research
Edgar R. Weippl

Secure Information Sharing & Self-Monitoring

Amin Anjomshoaa, Vo Sao Khue, Nick Amirreza Tahamtan, Edgar Weippl

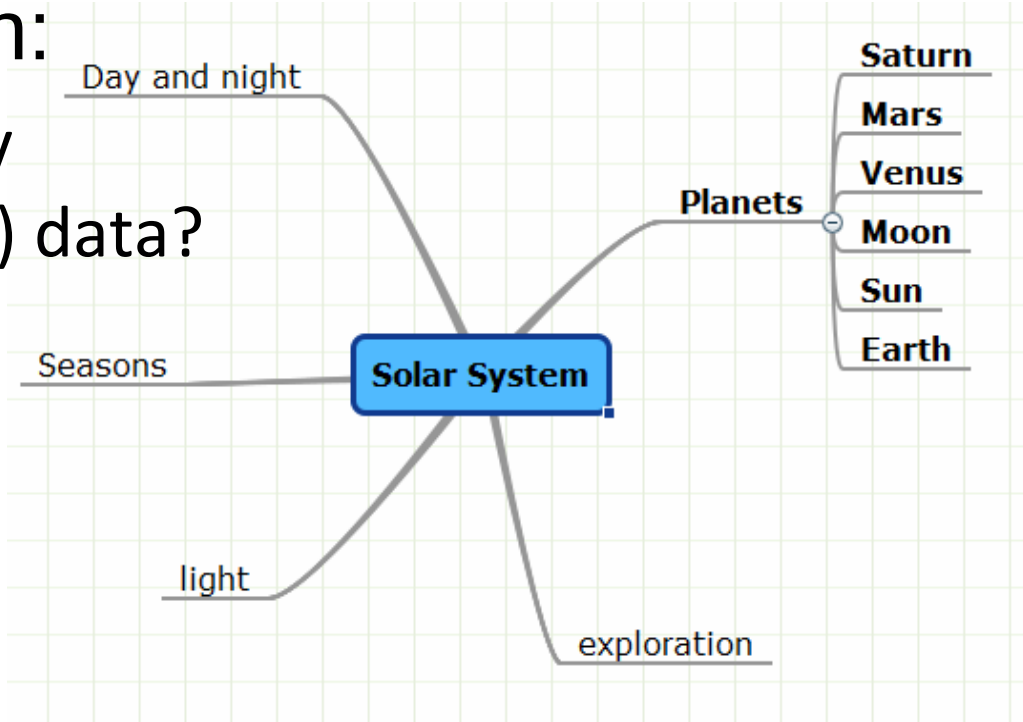
Resource Sharing

Resource Sharing



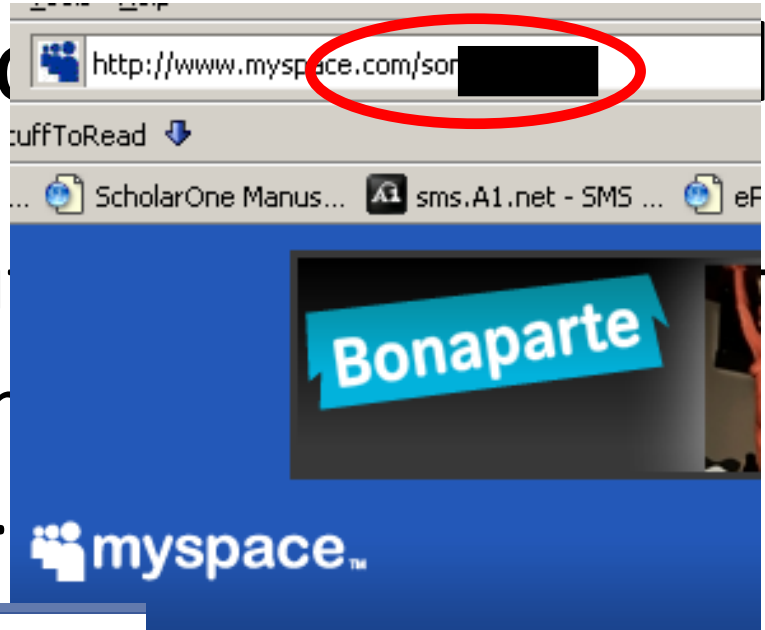
Resource Sharing

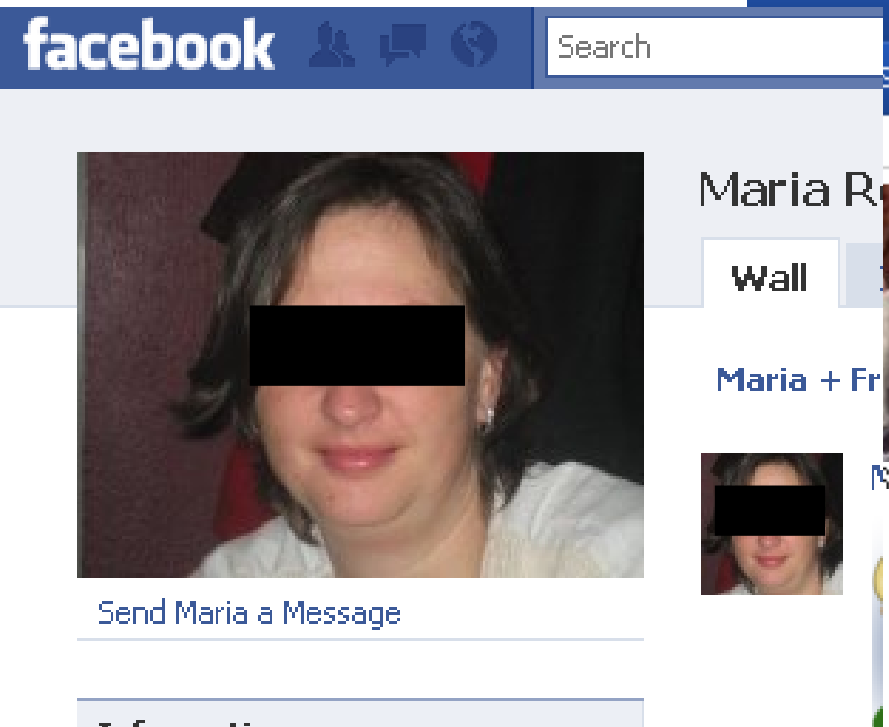
- Integration with data leakage prevention
- Research Question:
  - How can we identify sensitive (i.e. secret) data?



Which inf[redacted]ic?

- Web 2.0 is abou[redacted]t.
- If you create cor[redacted]a lot about yourself…

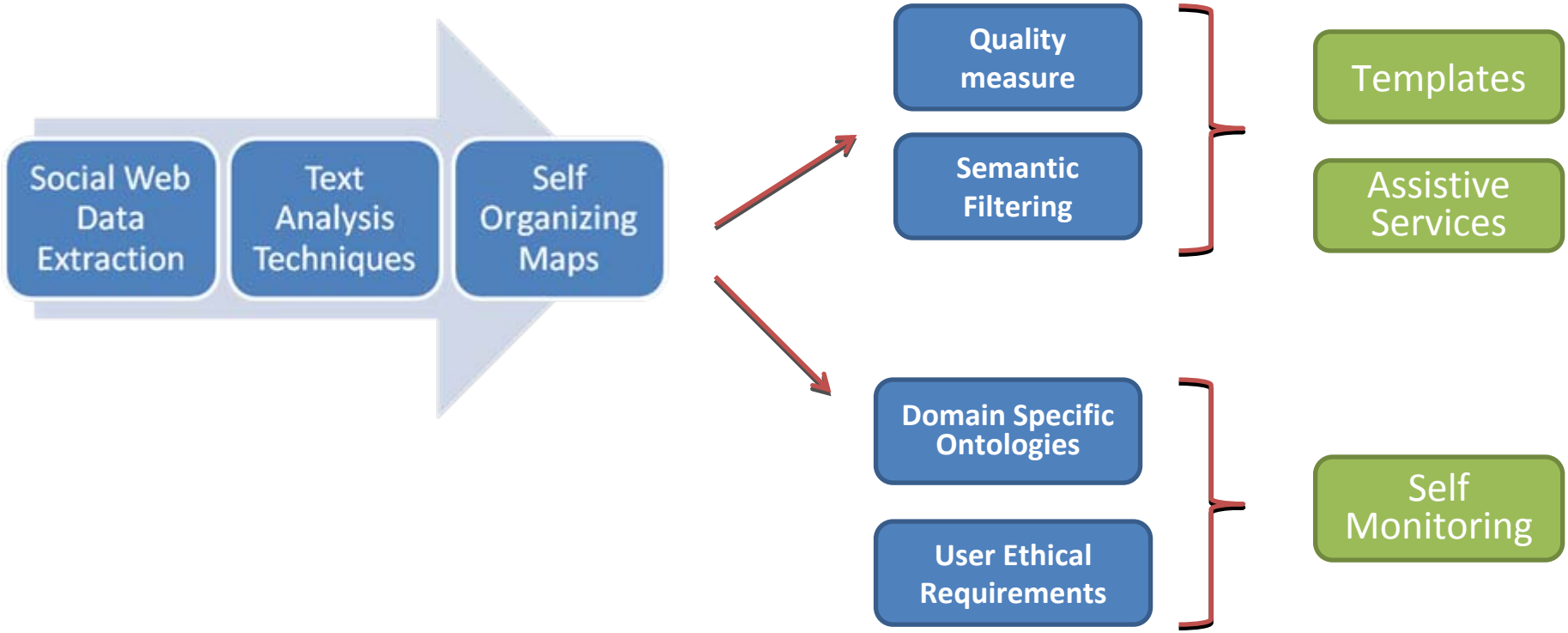




r ist als die Wut, darf
ıst wär ich im Häfn, u
bei Ausländern: zurü
ngnisse, bei Inländern
he Schadenszahlung u
4 Leser s

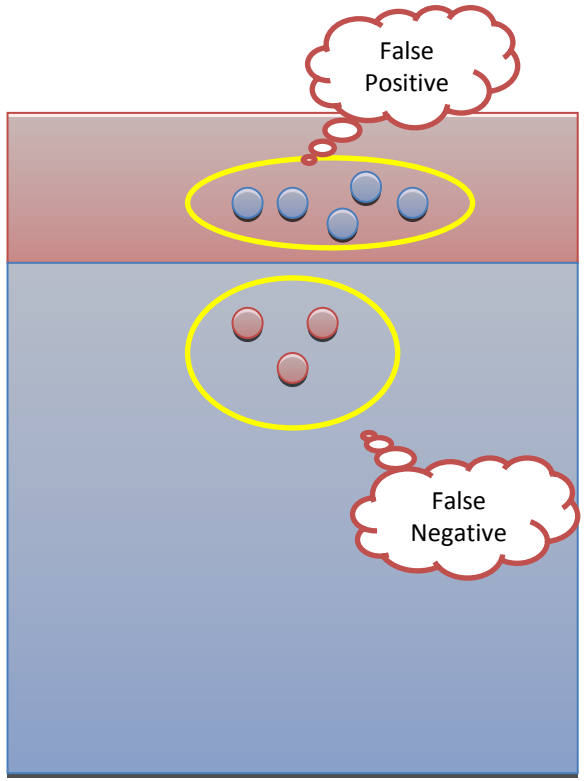
Für diese Scheißkanacken gibt es nur

Vision / Big Picture



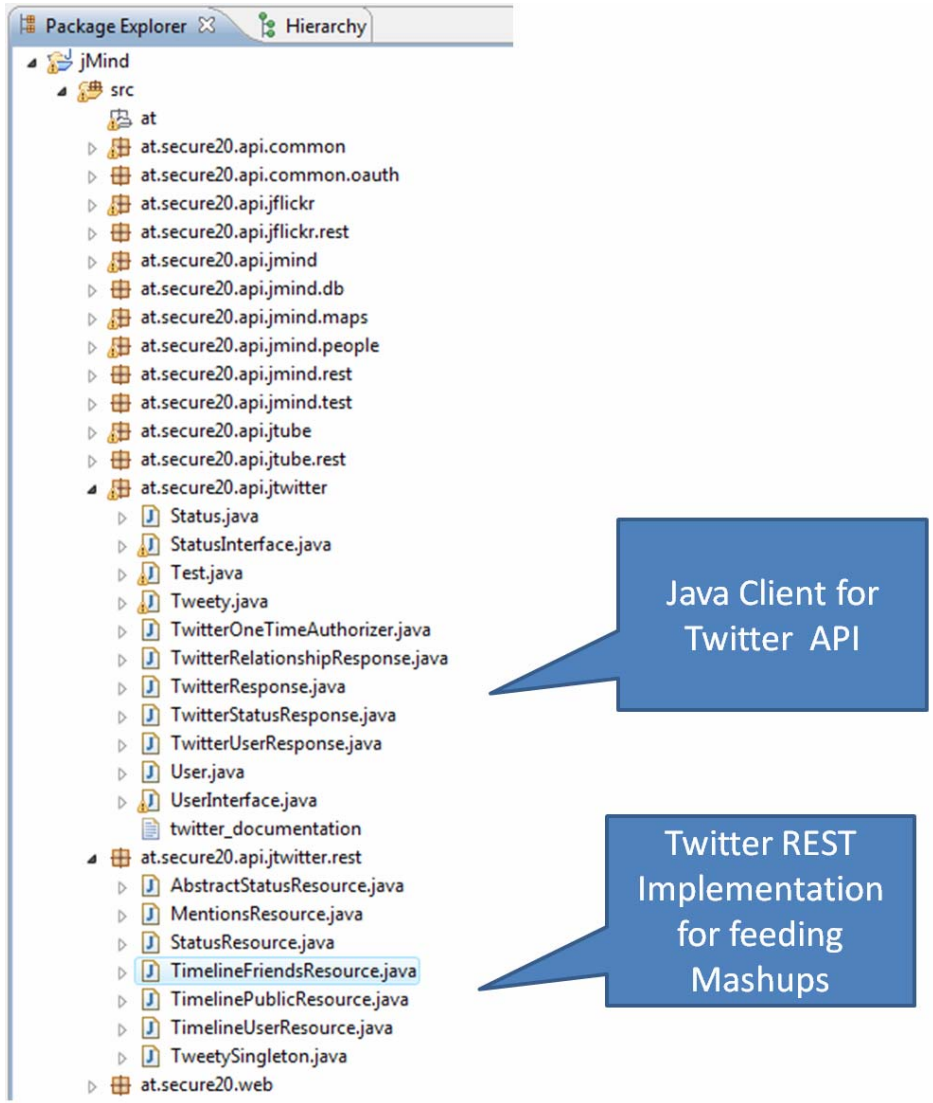
Identifying Project‘s Target Group

- In many binary classifications a group of people are incorrectly classified
- With lower specificity more „good“ people will be labeled „bad“
- With lower sensitivity more „bad“ people will be labeled „good“
- A major use case of Secure 2.0 project is aiming to prevent classifying „good“ people as False Positives candidates via providing a self-monitoring tool



Social Web Data Extraction (Task I)

- YouTube
- Flickr
- Twitter
- MindMeister
- FaceBook



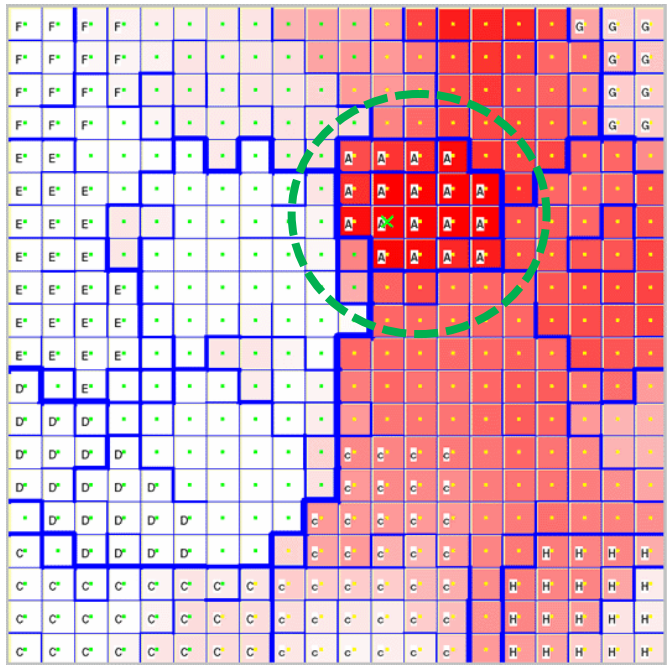
Self Monitoring Scenario

facebook

Extract
List of friends

Extract and annotate
List of interests

Visualization of high-risk groups according to user ethics



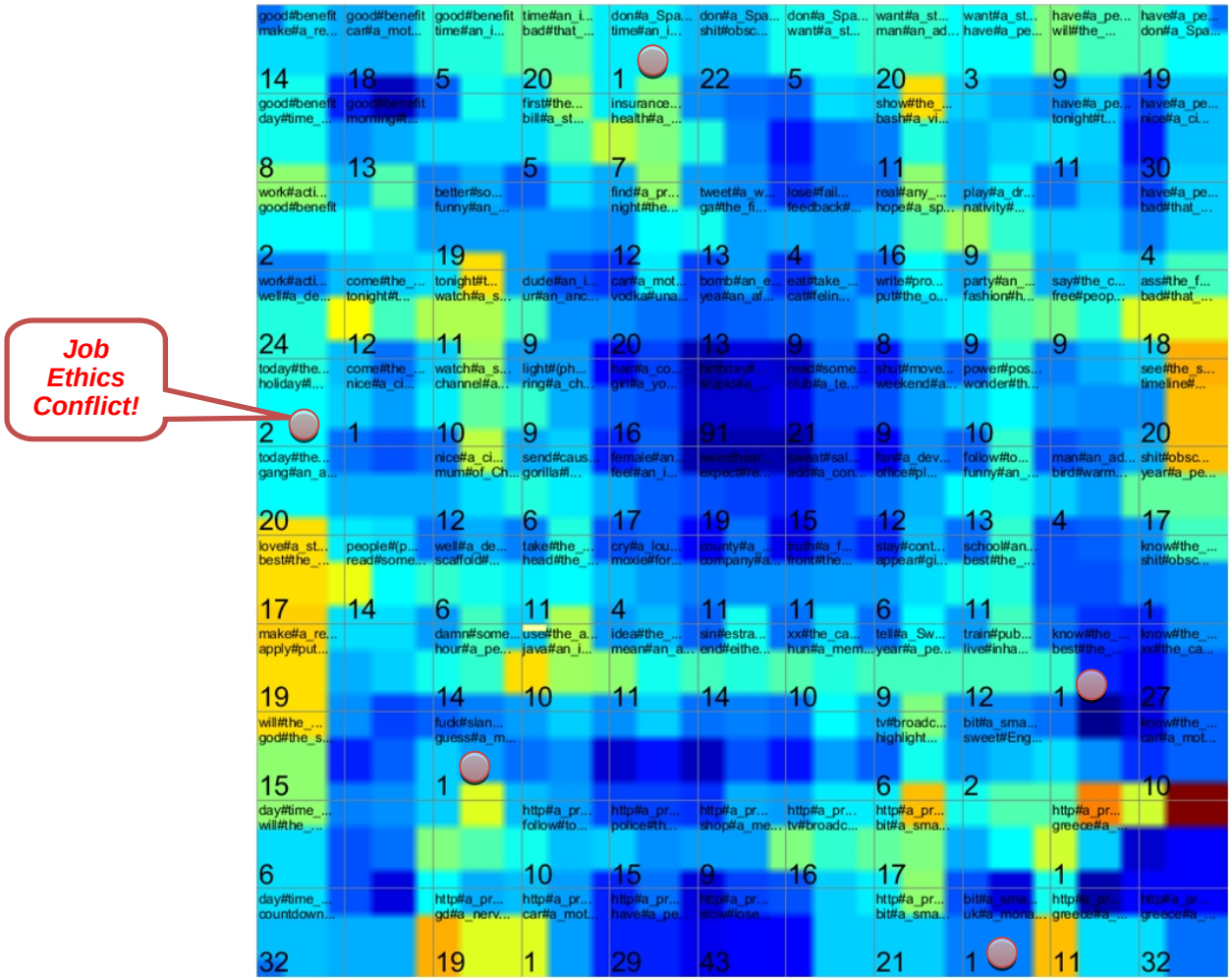
Experiments: Facebook Data

- Data extracted from Facebook including interests of friends (names are anonymized)
- In order to protect the privacy of the users only the following categories have been considered: *Books, Music, Movies and Television*
- Other categories which may provide information about personal attitudes, political views and sexual orientation have been ignored and removed

Experiments: Facebook Data (cont.)

- Several Views on the extracted data have been constructed:
  - A map showing the interest of each friend
  - An aggregated view on interests of all friends
  - A classification of friends according to their interests

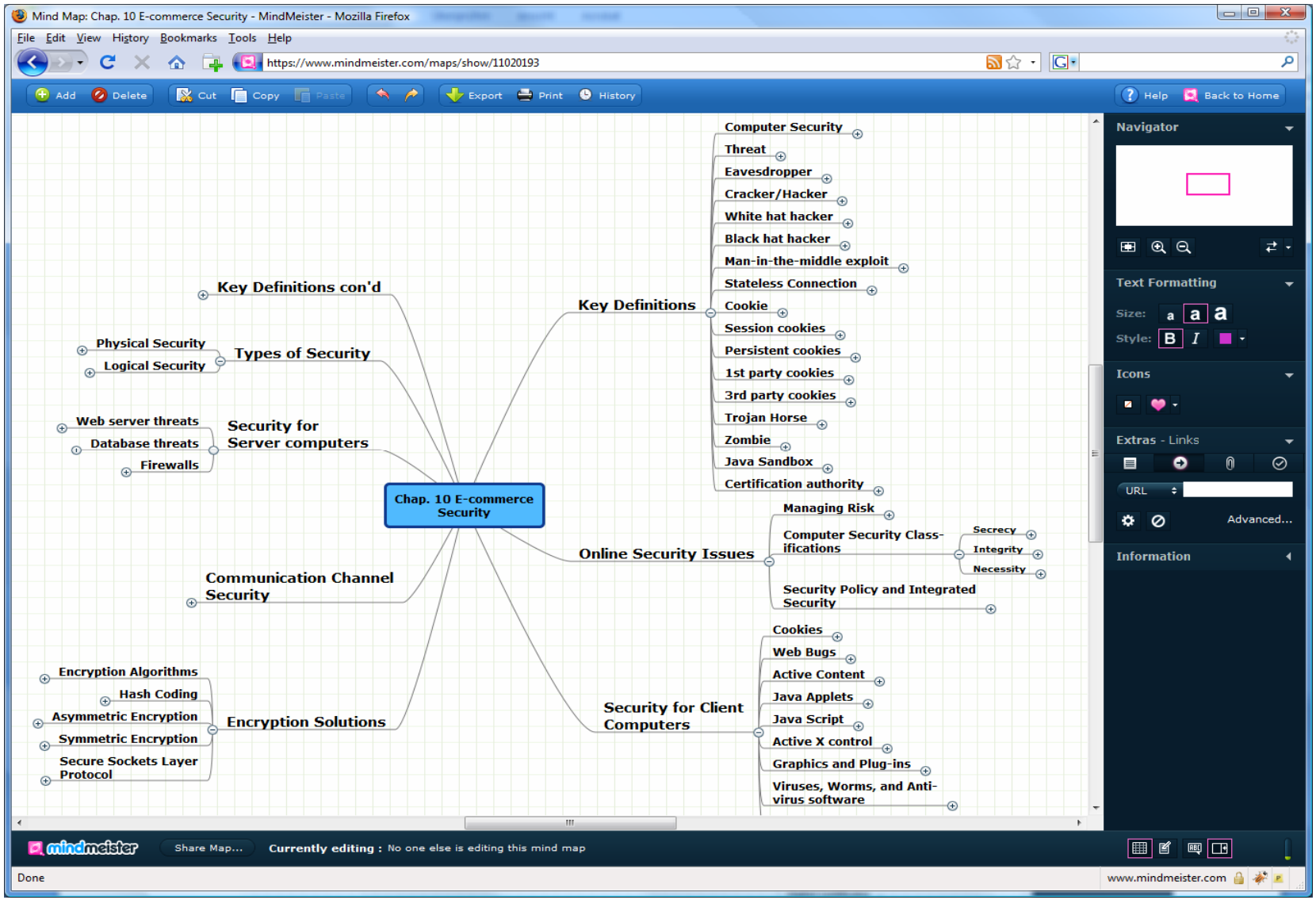
Twitter Map



MindMeister Use Cases

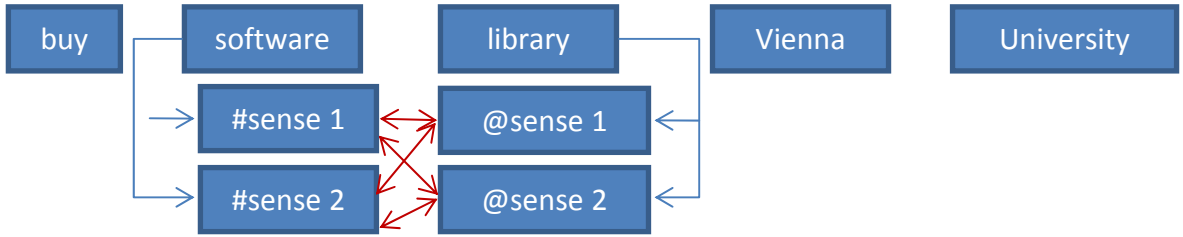
- **Trustworthy data (Mind Map) sharing**:
  - take care of filtering of private and sensitive data
  - hinder the unwanted disclosure of such data based on some predefined data sharing policies
- **Assistive services** :
  - Shared mind maps should be analyzed and ranked based on **quality of map**, then transformed to mind map templates for reuse
  - provide assistance for users who create similar contents, or in diverse knowledge domains

MindMeister

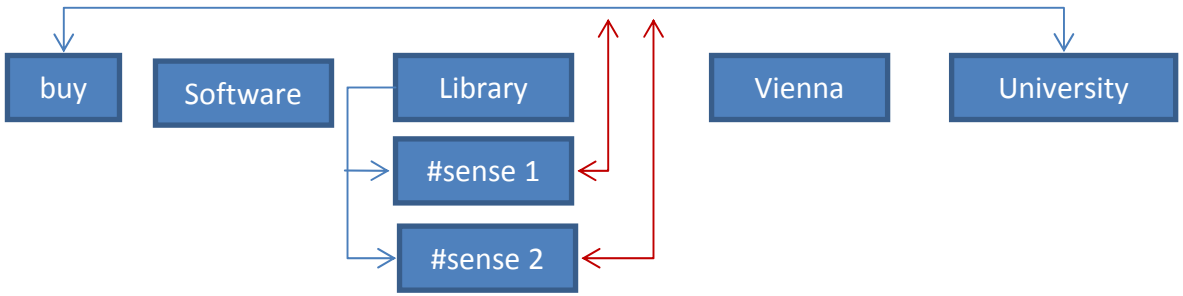


WSD – Gloss-Based

- **Lesk algorithm:**
  - Retrieve from dictionaries all sense definitions of the words to be disambiguated
  - Determine the definition overlap for all possible sense combinations
  - Compute the **highest overlaps between senses**

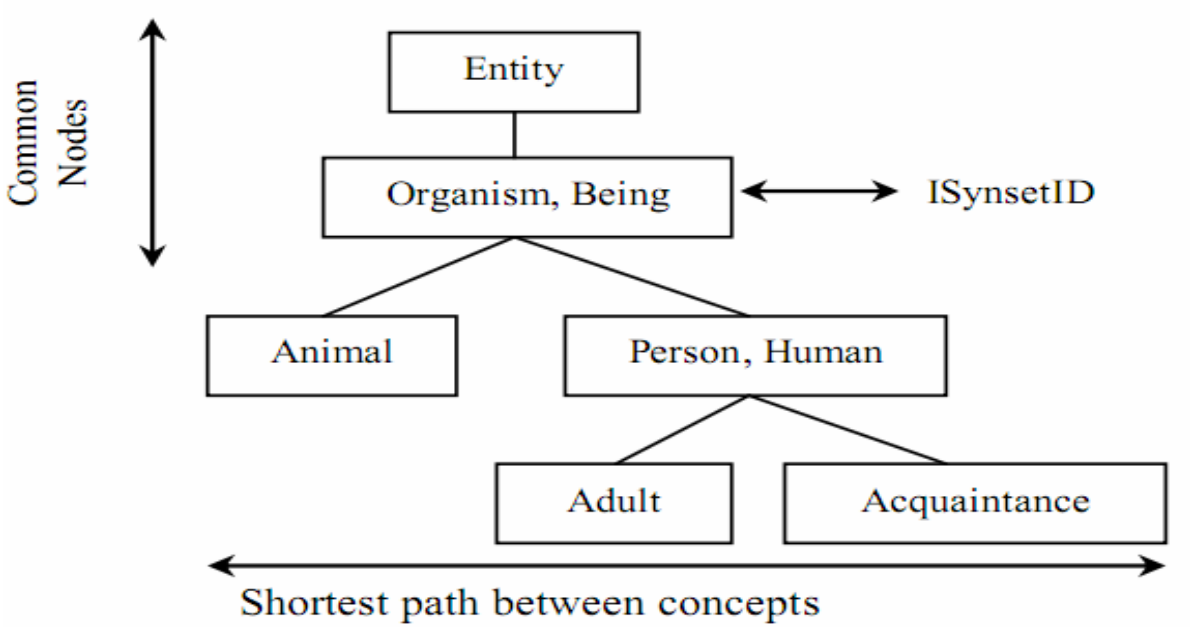


- **Simplified Lesk algorithm:**
  - Compute the **highest overlaps between sense and main context**

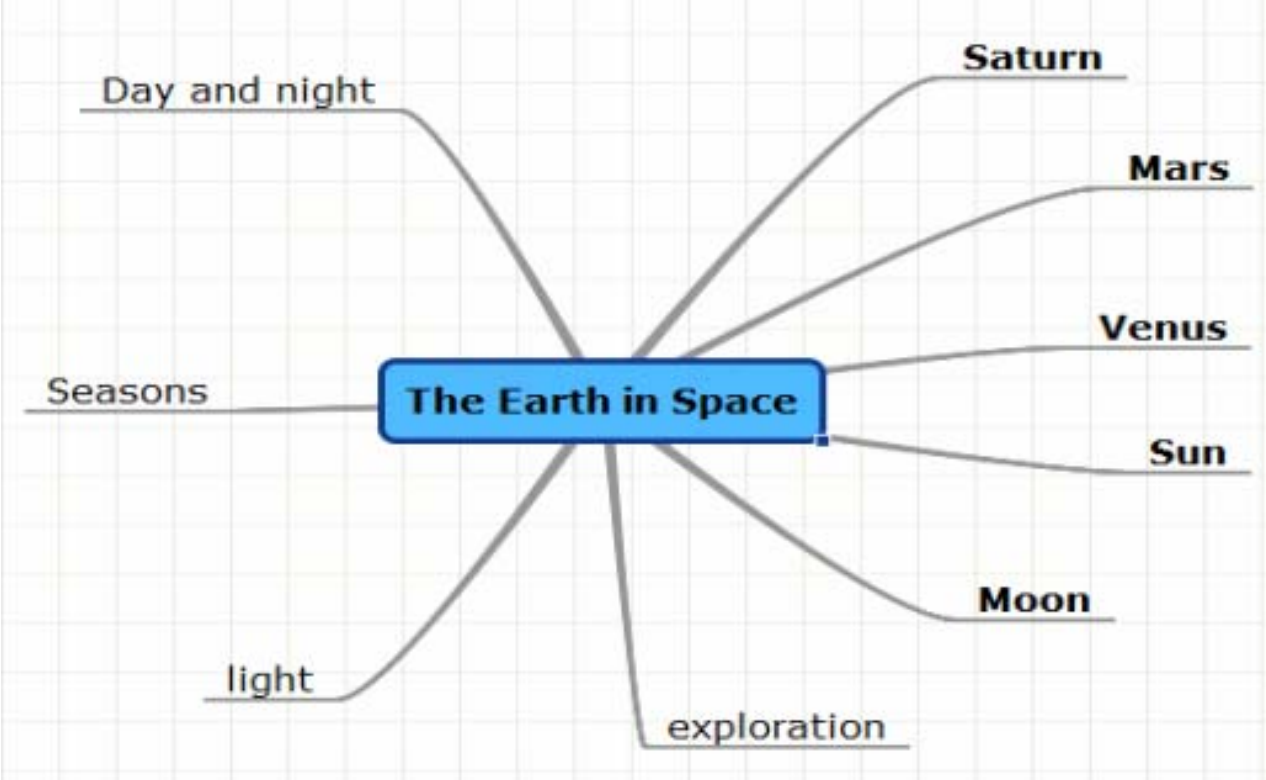


WSD – Semantic-Based

- Wu and Palmer: 2*d(lcs)/[d(c1)+d(c2)]
  - d(lcs): depth of the least common subsumer (LCS)
  - d(c1),d(c2): depth of concept1 and concept2 respectively

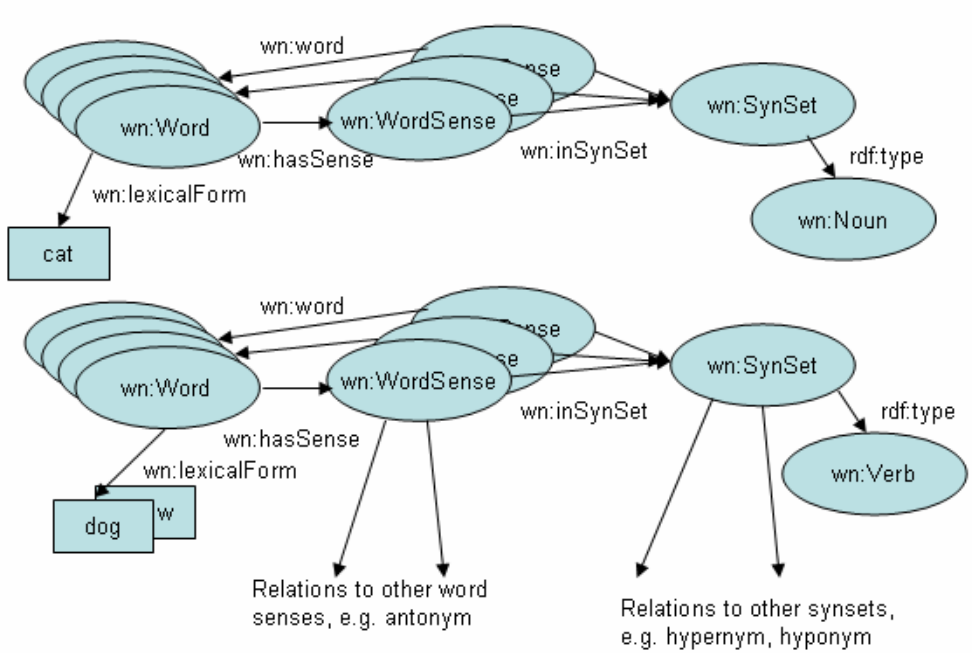


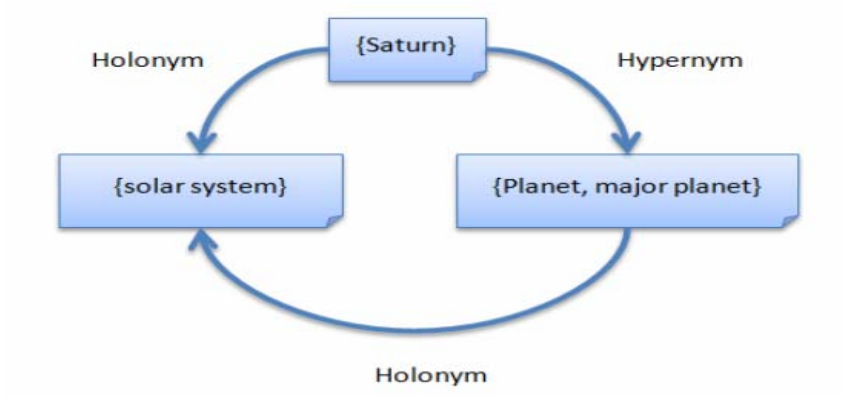
Word Sense Disambiguation + Map Quality Measure



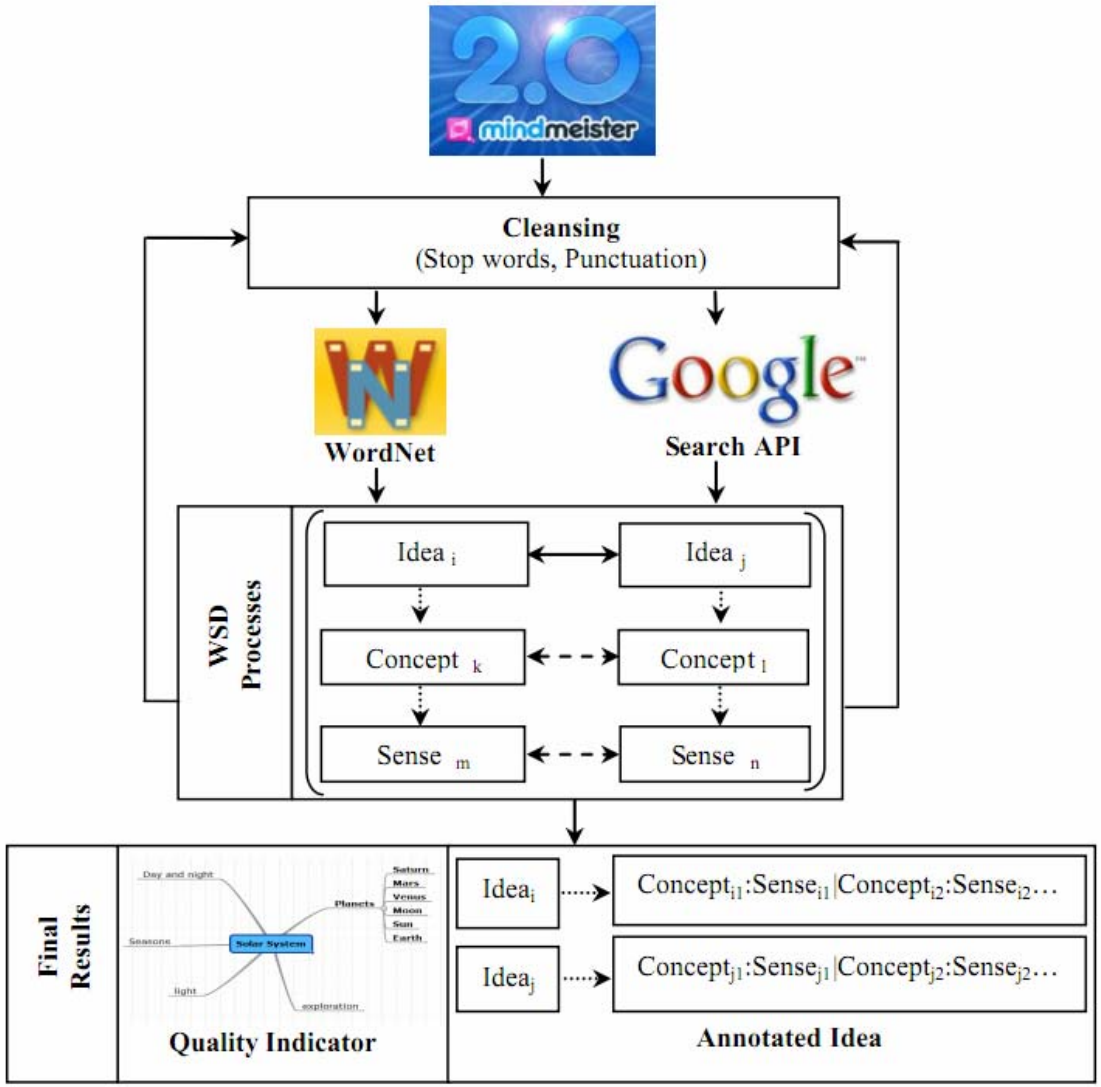
Word Net –Free Large Lexical Dictionary

- only contains "open-class words“ (Noun, Verb, Adjective, & Adverb)
- offer semantic relations between words
  - Hypernymy
  - Hyponymy
  - Holonym
  - Meronymy
  - Antonymy





Approach


mindmeister
Cleansing
(Stop words, Punctuation)
WordNet
Google
Search API
WSD Processes
Idea i
Idea j
Concept k
Concept l
Sense m
Sense n
Final Results
Quality Indicator
Idea_i
Concept_i1:Sense_i1|Concept_i2:Sense_i2…
Idea_j
Concept_j1:Sense_j1|Concept_j2:Sense_j2…
Annotated Idea

Social Networking Sites
An information security case-study on basis of Facebook

Markus Huber, Martin Mulazzani, Sebastian Schrittwieser, Peter Kieseberg, Edgar Weippl

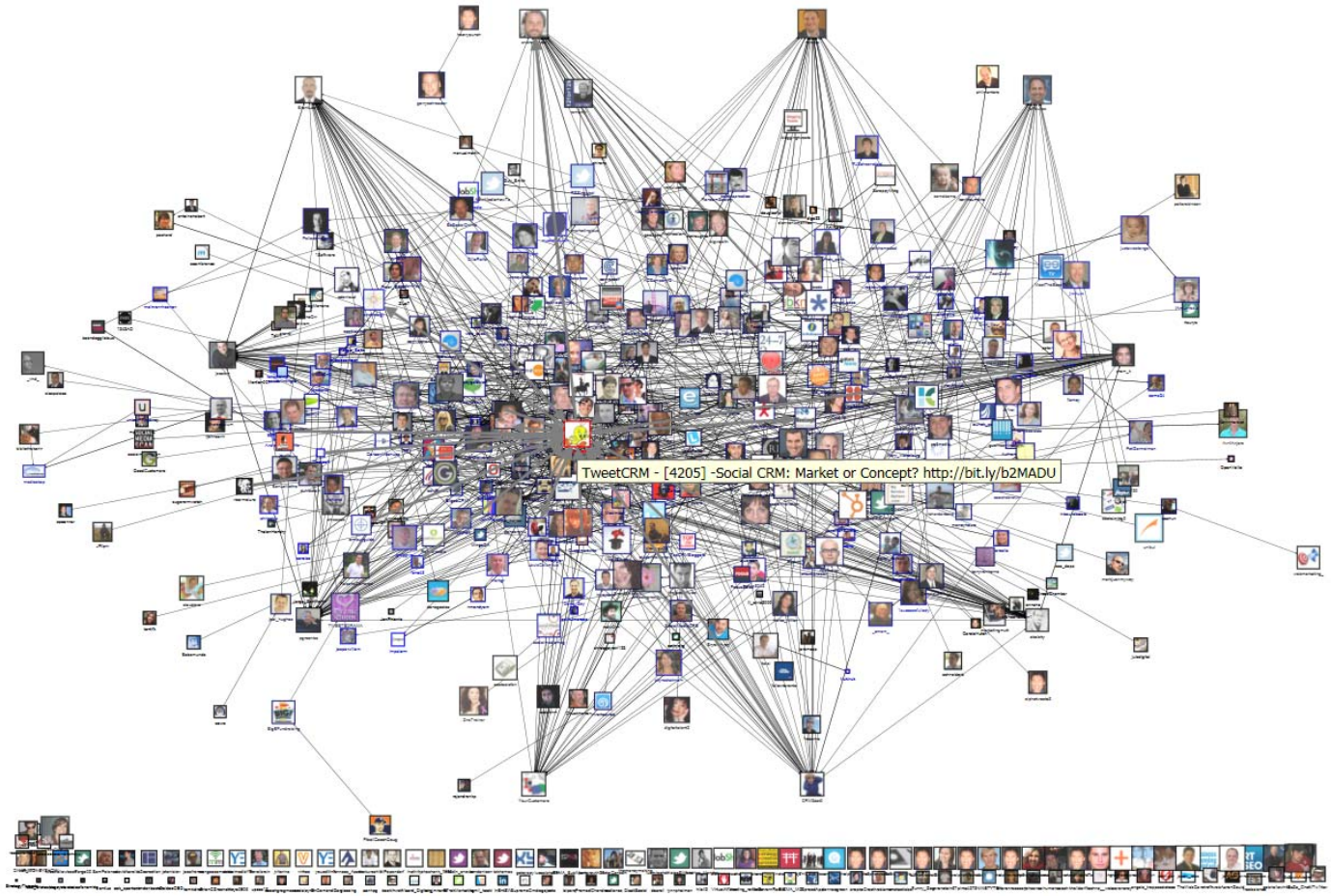
What you should remember

- External View
  - Know about your public image
  - Active management
  - Gathering evidence
- Improved Social Engineering
  - Spear phishing
  - Context sensitive spamming

Background

- Social networking sites (SNSs) became very popular services
  - Web services to foster social relationships
  - Share personal information
  - Free of charge
- SNSs like Facebook, XING, studivz etc. contain a pool of sensitive information
- Extraction of sensitive information poses non-trivial challenge
  - Simple crawlers (libwww etc.) [10, 5]
  - Profile cloning [2]
  - Induction from public information [3]

Figure: social network example



Nothing to hide?

Information from SNSs can be misused

- Social phishing [9]: Emails that seem to be send by a friend
- Context-aware spam [4]
- Automated social engineering based on chatterbots [6]

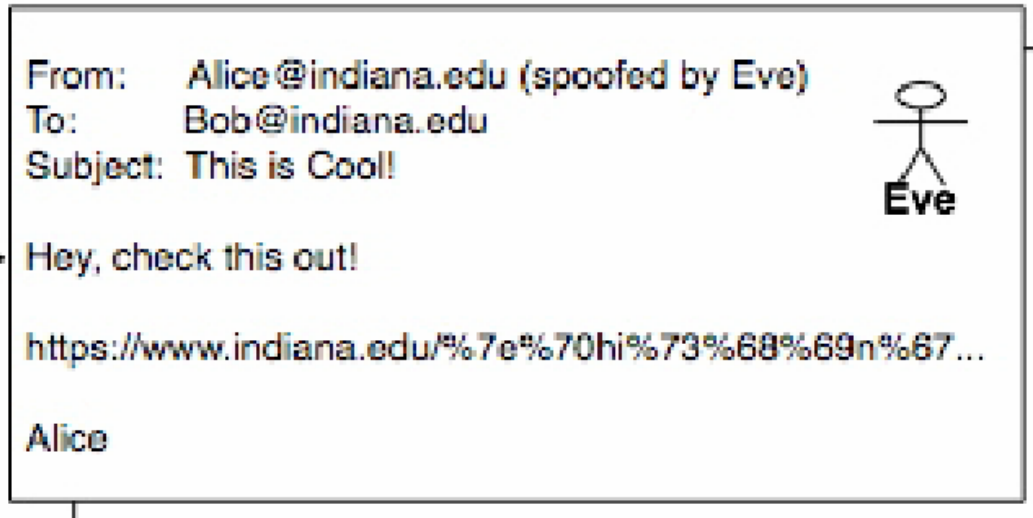
Social Phishing

Phishing

- Steal login information via fake websites
- Online banking, ebay, university accounts, etc.
- Quite ineffective

Social phishing [9]

- Using information harvested from social networks
- Emails appear to be coming from a friend
- Response rate rose from 16 to 72 per cent



Context-aware spam

Hi [FIRSTNAME],
[SENDERNAME] ([SENDEREMAIL]) has sent you an online greeting card from BirthdayCards.com!

To pickup your card, please click on the following link:
http://www.birthdaycards.com/pickup?ID= A222-FHRE
(Link to attacker-controlled site)

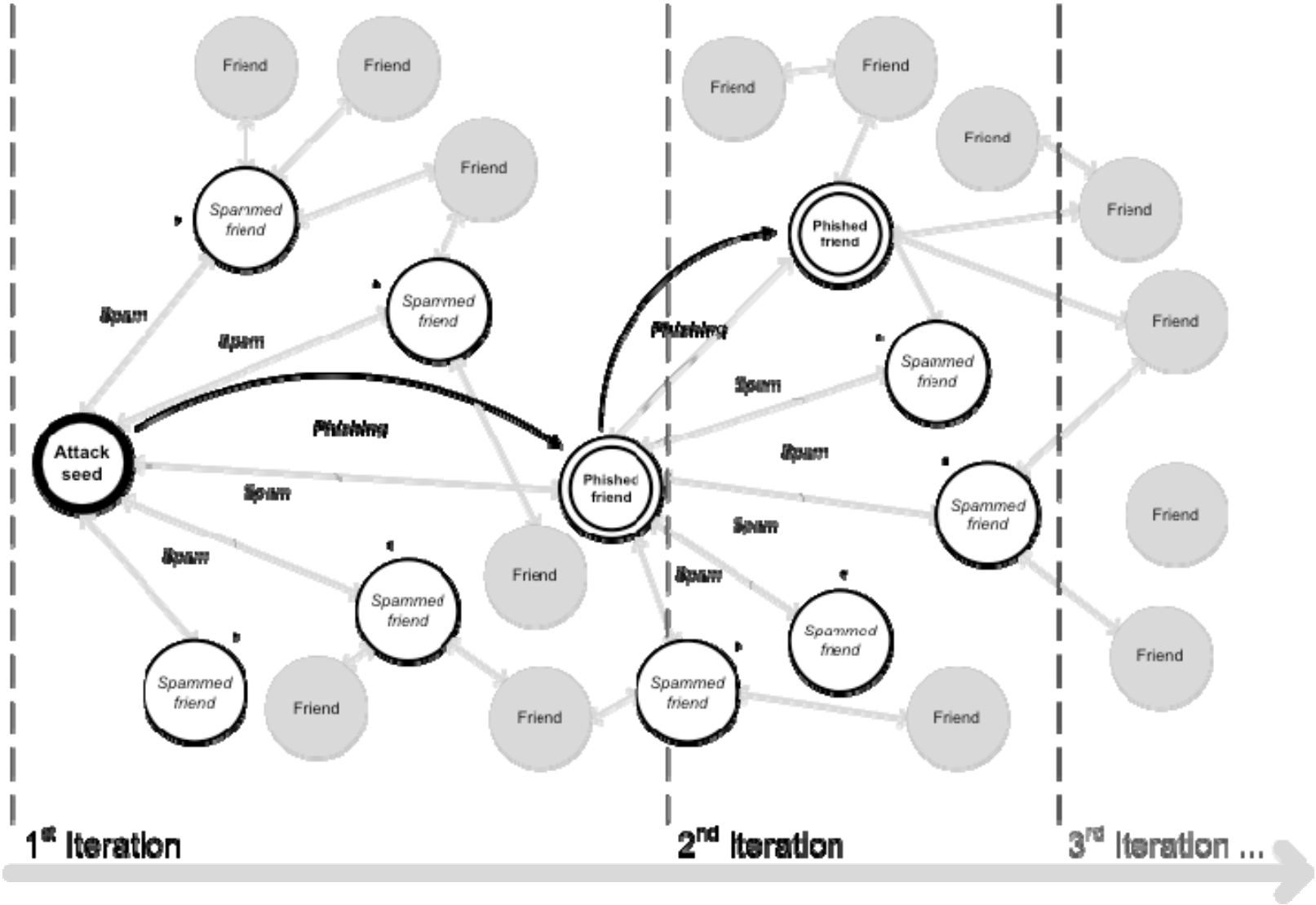
If you are unable to click on the link above, please try cutting and pasting the URL into the address bar of your web browser. You may also go to our website at: http://www.birthdaycards.com **(Link to attacker-controlled site)** and choose the "Pickup" option at the top of the page.
Your Pickup ID is: A222-FHRE

BirthdayCards.com - High Quality Greetings for All Occasions.
If you have any other questions or problems, please visit our support page at:
http://www.birthdaycards.com/support.momd

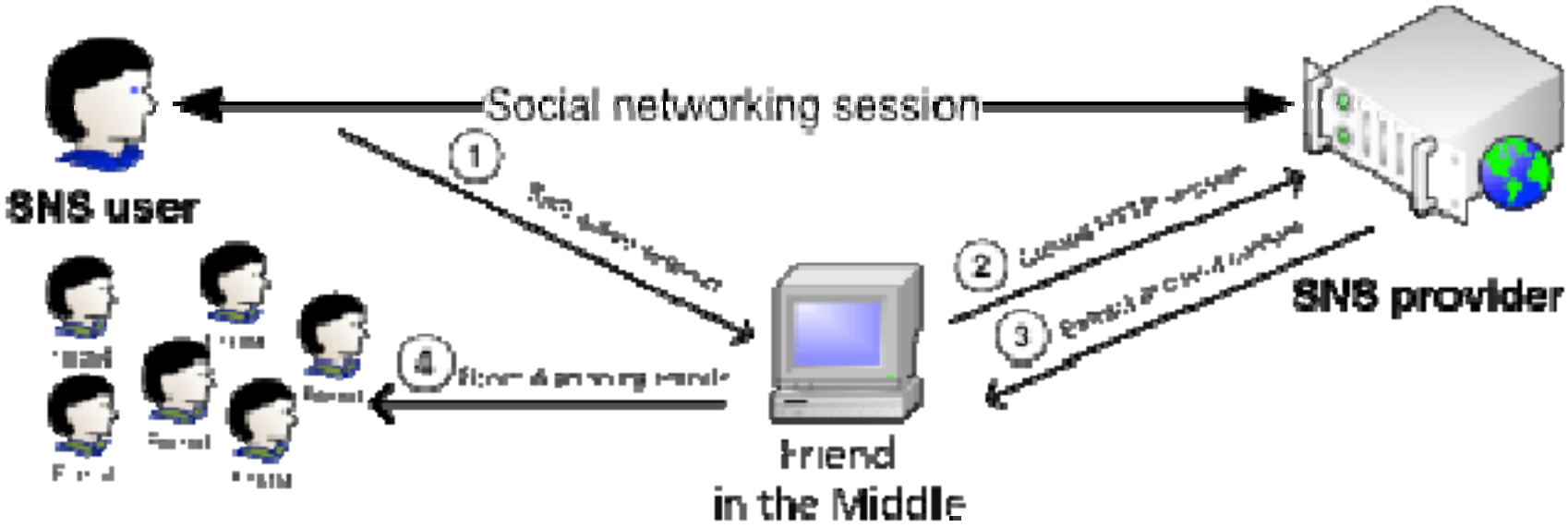
Information security case-study

- Estimate the impact a large-scale spam and phishing attack would have on SNSs users.
- Brief description
  1. An attacker uses a security hole to extract information of a SNS user.
  2. The extracted information is used for spam and phishing messages targeted at the SNS user's friends
  3. Phishing is used to further extract information which is again used to spam/phish (iteration from (2))

Attack scenario



Friend-in-the-middle (FITM) attacks

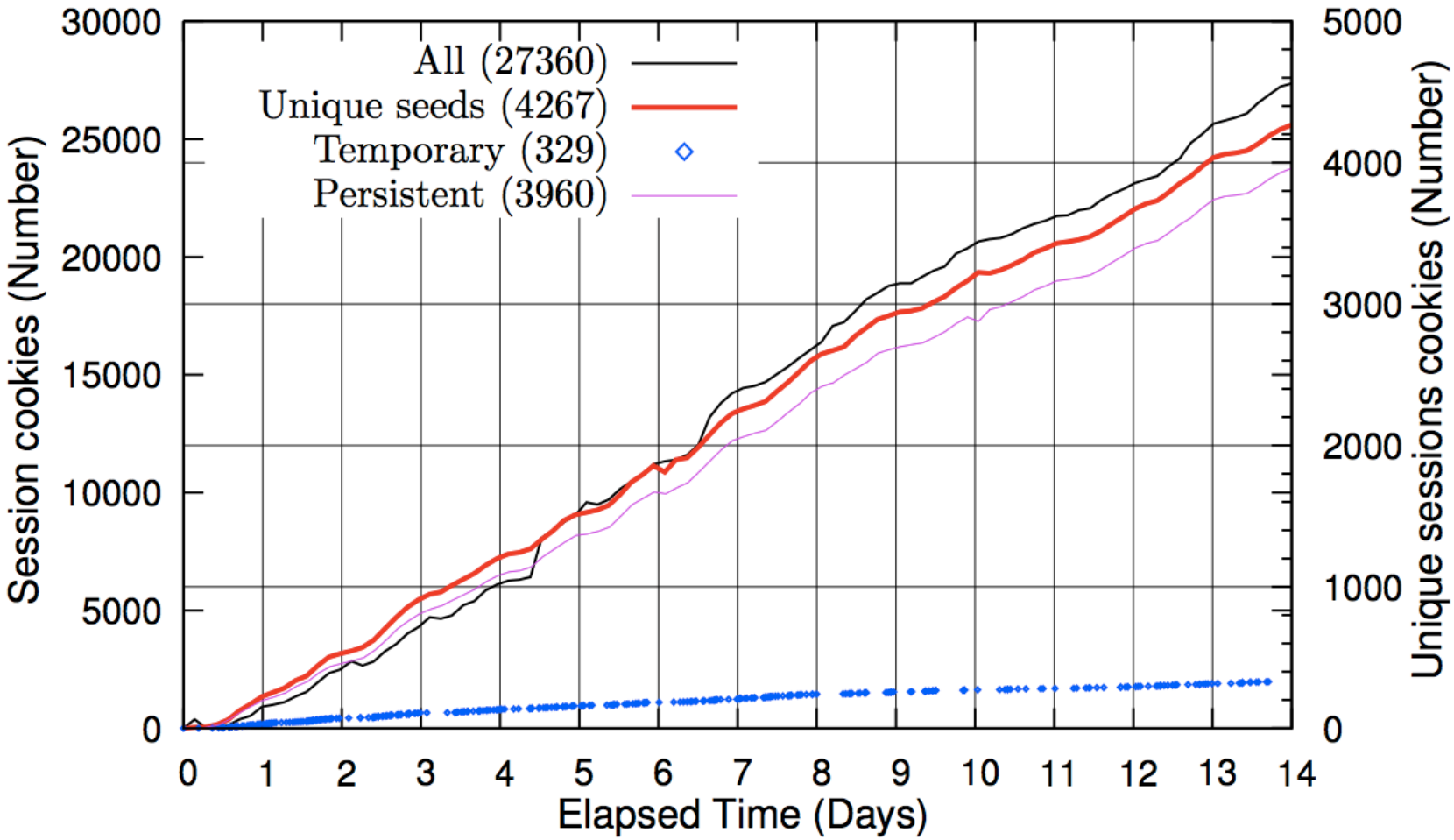


- Hijack social networking sessions
- Attack surface: unencrypted WLAN traffic, LAN, router etc.
- User impersonation

Methodology and ethics

- How to get realistic results?
  - Closed lab experiments
  - Ethics of in-the-wild evaluations
- Finding attack seeds via Tor
  - Tor exit node with a bandwidth of 5 Mbit/s
  - Exit node only allowed port 80 (HTTP)
  - Collect information on Facebook cookies
- Attack simulation
  - Based on social graph model of Facebook
  - Estimate the impacts

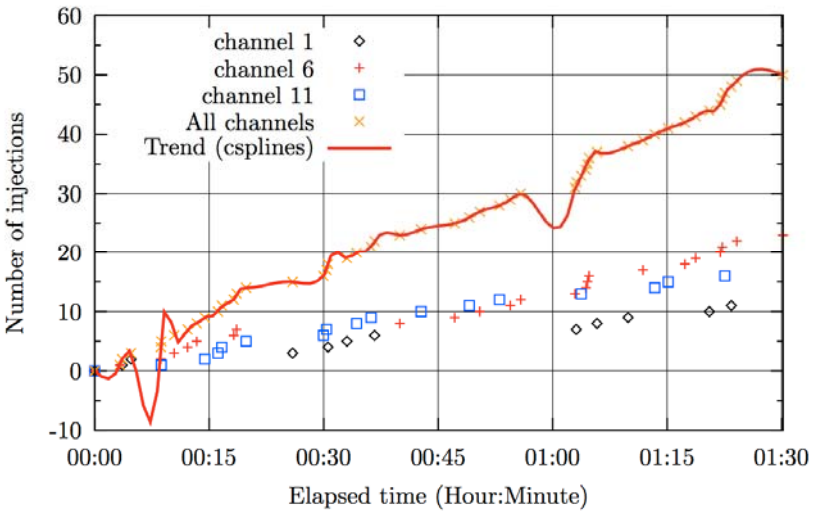
Results I: Tor exit node server



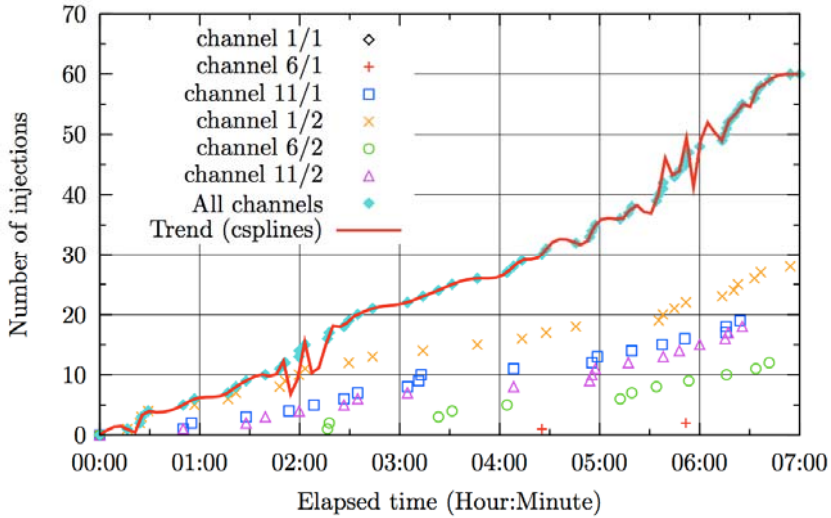
Number of sessions found through Tor exit node (14 days)

Results II: WLAN experiment

Injections during WLAN peak-time (1.5 hours)

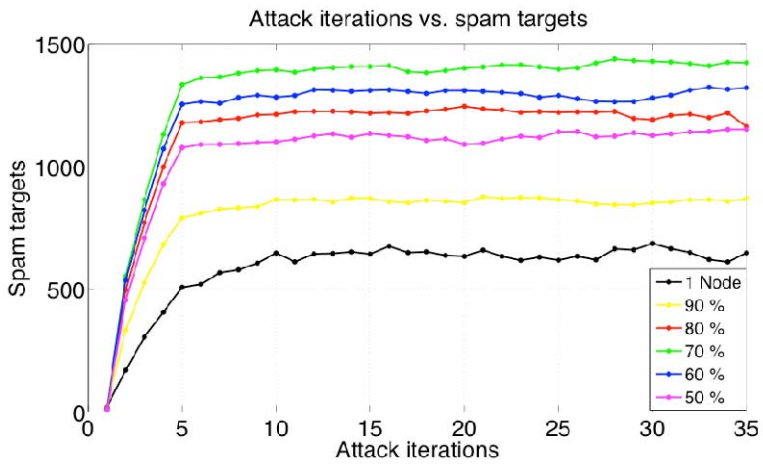


Injections during average WLAN usage (7 hours)

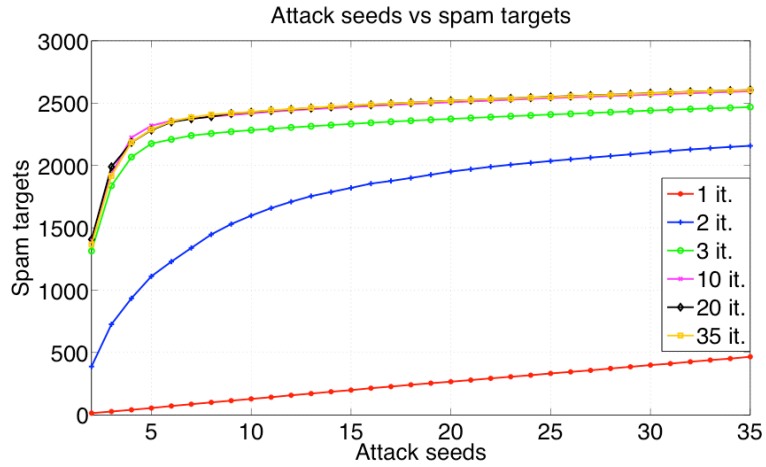


Results III: Simulation results

Strategy 1: Spam targets vs. Attack iterations



Strategy 2: Spam targets vs. Attack seeds (jumps)



Mitigation strategies

- On the user-side
  - Usage of VPN tunnel, encrypted WLAN, etc.
  - Browser extensions like ForceTLS
- On the provider-side
  - Full SSL/TLS support (e.g. XING)

Top five social networking sites

Social Networking Site		
Name	Claimed users	HTTPS
Facebook	400×10^6	Login only
Friendster	110×10^6	No
Orkut	100×10^6	Login only
hi5	80×10^6	No
LinkedIn	60×10^6	Login only

Conclusion

- Big dilemma for SNS providers and their users
  - Majority of providers are vulnerable to our novel attack
  - Large-scale attacks require little resources
  - Injection attacks are hard to detect
- Full SSL/TLS is so far the only effective technical countermeasure

Dropbox

Markus Huber, Martin Mulazzani, Sebastian Schrittwieser, Peter Kieseberg, Edgar Weippl

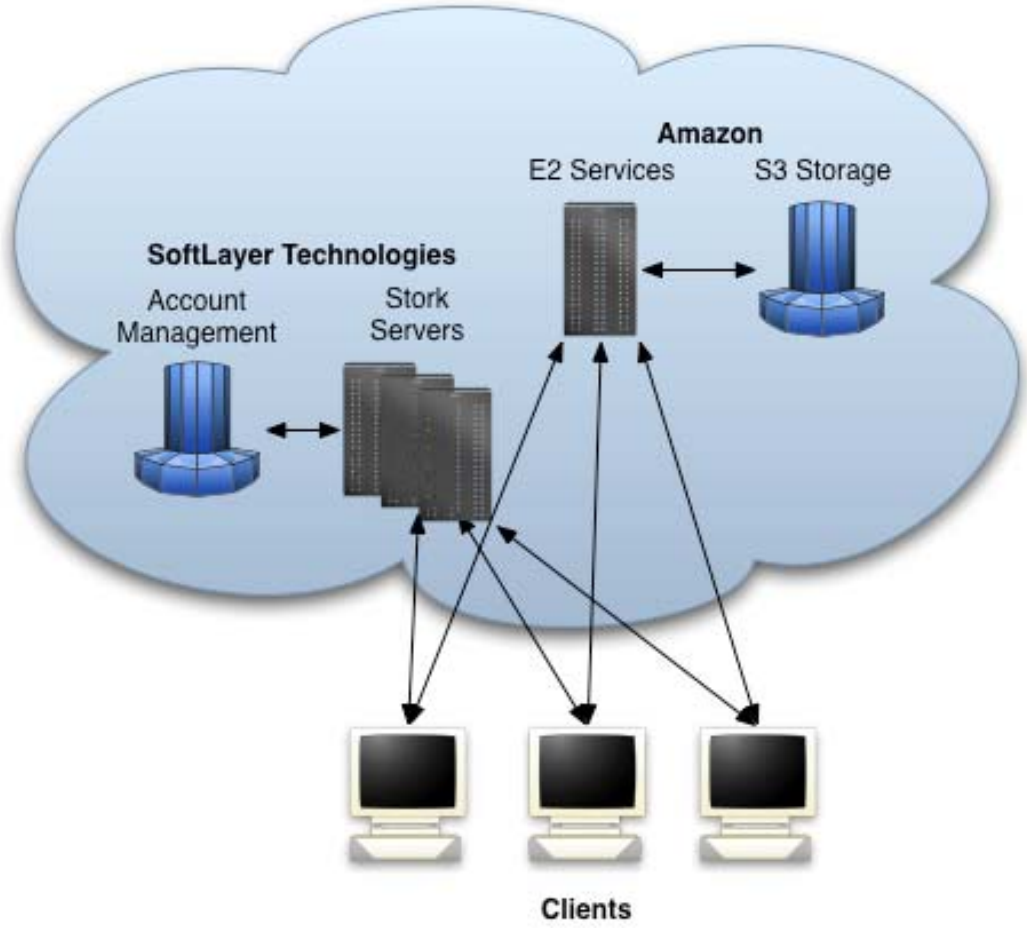
Dropbox Attacks

- document the functionality of an advanced online file storage service, Dropbox
- show under what circumstances unauthorized access to files stored with Dropbox is possible
- evaluate if Dropbox is used to store filesharing data and briefly outline how the distribution of hash values may be used as a new way of sharing content.
- explain countermeasures, both on the client and the server side, to mitigate the resulting risks for user data

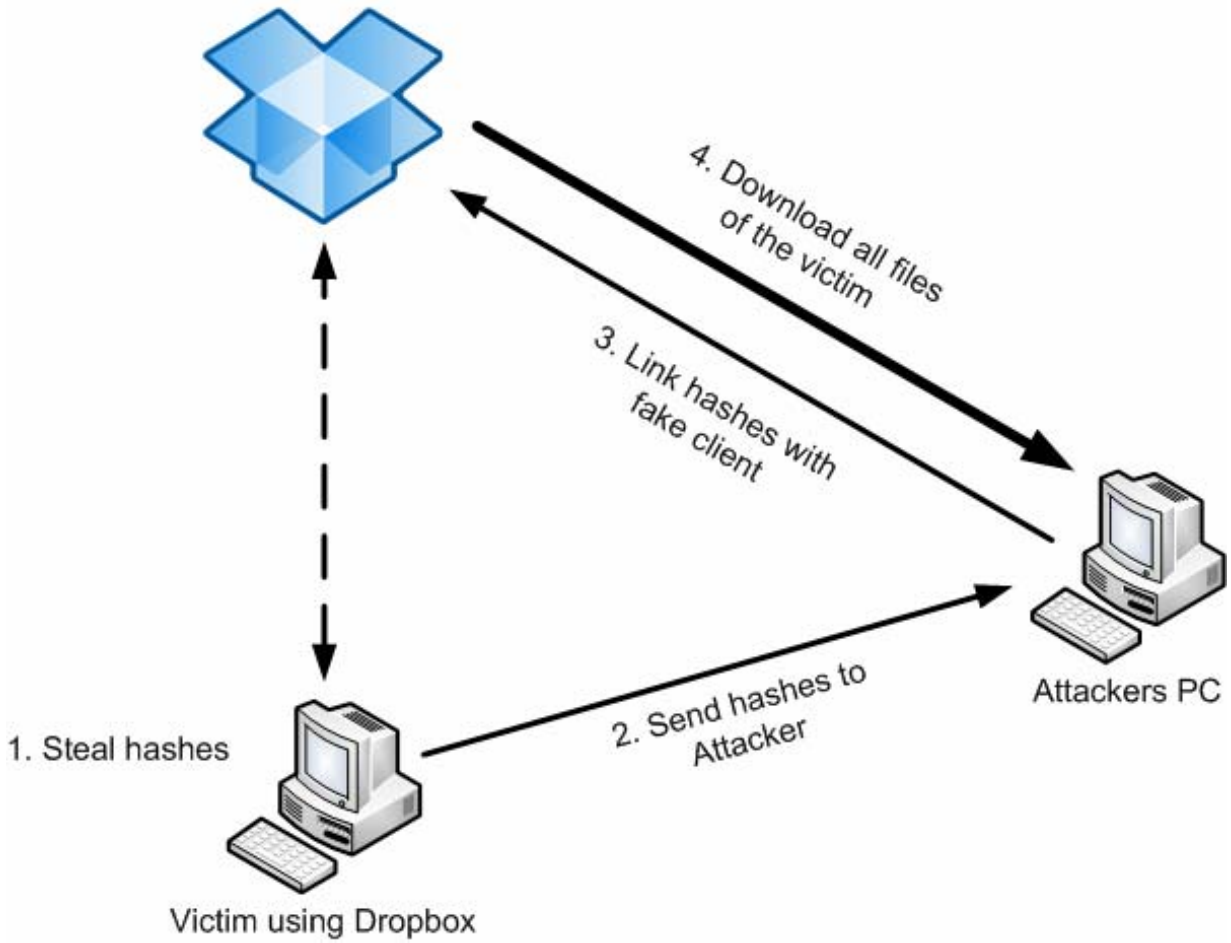
Online Storage Providers

Name	Protocol	Encrypted transmission	Encrypted storage	Shared storage
Windows Live Skydrive	browser-based	yes	?	no
Apple iDisk	WebDAV	no	no	no
Ubuntu One	u1storage	yes	no	no
Box.net	WebDAV	no	no	no
Wuala	?	yes	yes	no
TeamDrive	many	depends on protocol	yes	no
Dropbox	proprietary	yes	yes	yes

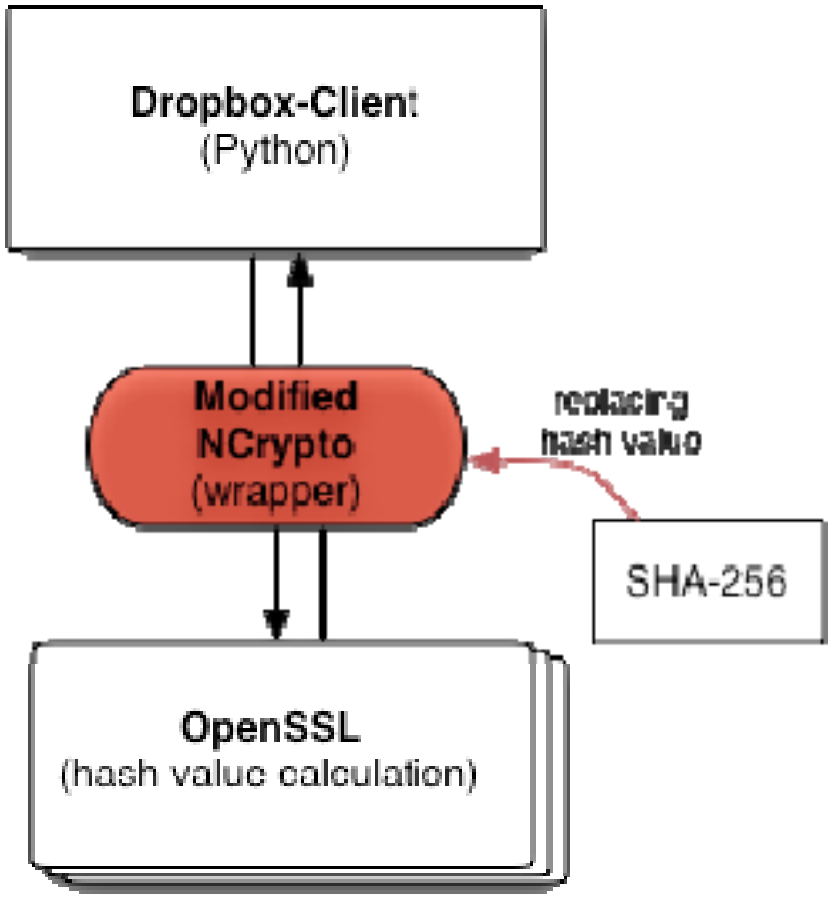
Dropbox Network Infrastructure



Covert Channel Attack



Hash Value Manipulation



Distribution of Tested Torrents

Category	Quantity
Application	3
Game	5
Movie	64
Music	6
Series	29
Sum	107

Variants of the Attack

Method	Detectability	Consequences
Connect with stolen host ID	Dropbox only	Get all user files
Stolen hashes & arbitrary host ID	Dropbox only	Unauthorized file access
Upload with manipulated hash value	Undetectable	Unauthorized file access

SBA Research
Edgar R. Weippl