On the New Threats of Social Engineering Exploiting Social Networks

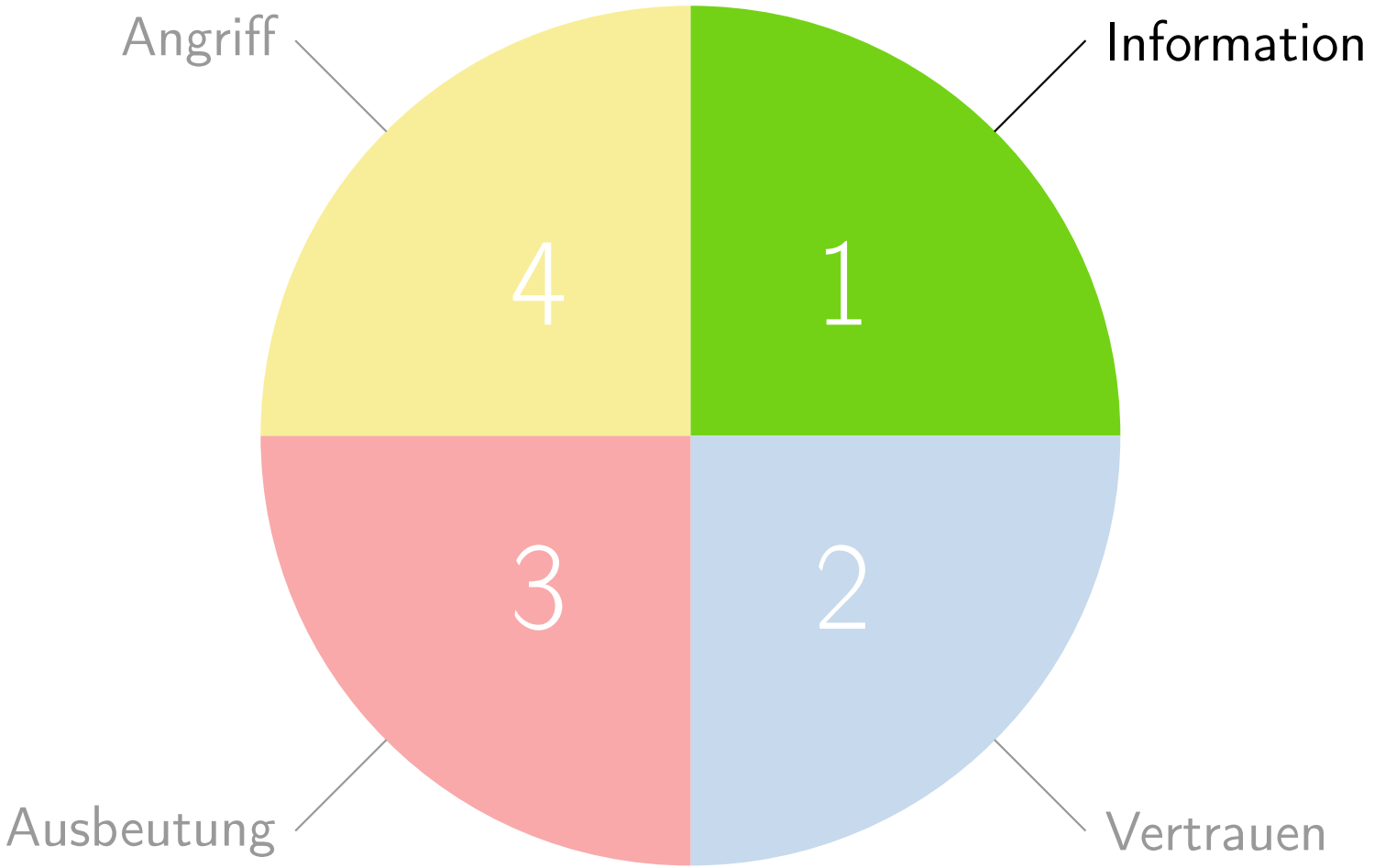
Daniel Siegel

13. August 2009

Inhalt

- Motivation & Problemstellung
- Social Engineering
- Soziale Netzwerke
- Ein konkretes Soziales Netzwerk: Twitter
- Prototyp
- Evaluation & Ausblick

Ausgangssituation



Problemstellung

Wie können Daten bestimmter Individuen bzw. Unternehmen über Soziale Plattformen automatisch extrahiert und so dargestellt werden, dass sie für einen Social Engineering Angriff benutzt werden können. Zudem sollen Gegenmaßnahmen zu diesen Angriffen erarbeitet werden.

Definition: Social Engineering

Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.

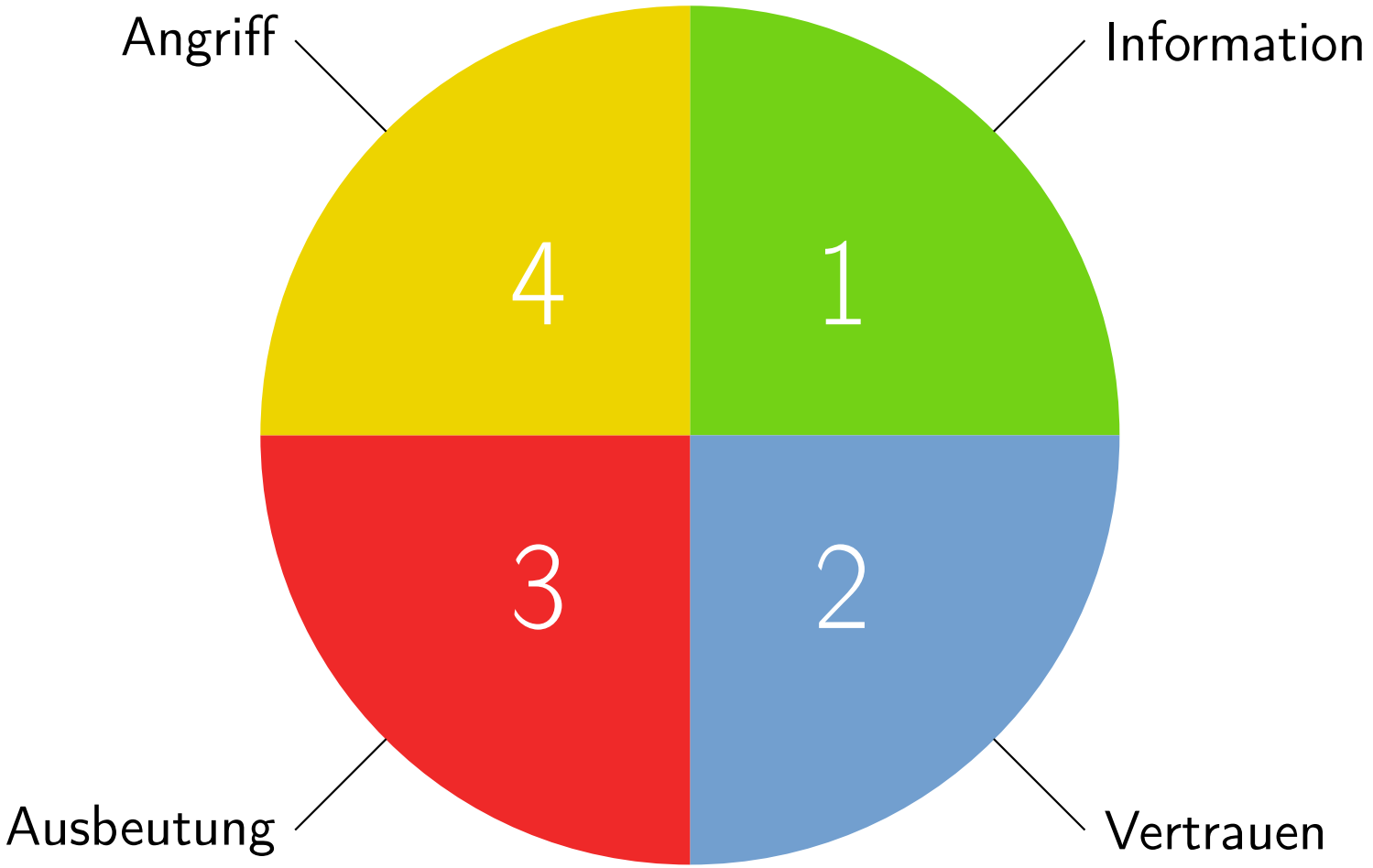
Kevin D. Mitnick and William L. Simon. „The Art of Deception“

Definition: Social Engineering

Social Engineering uses influence and persuasion to **deceive** people by **convincing** them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to **take advantage** of people to **obtain information** with or without the use of technology.

Kevin D. Mitnick and William L. Simon. „The Art of Deception“

Verlaufszyklus eines Angriffes



Ziele

- Finanzielle Bereicherung
- Industriespionage
- Spass - Macht
- Identitätsdiebstahl
- Datendiebstahl
- Soziale Überlegenheit

Informationen sammeln

- Möglichkeiten der Informationsgewinnung
  - Firmen-Website
  - Persönliche Homepage
  - Dumpster Diving
  - Phishing
  - Trojanische Pferde
  - Newsgroups & Mailinglisten
  - Job Sites
  - ...
- Ziel: Informationen $\Rightarrow$ Vertrauen

Vertrauen erarbeiten

- Informationen
- Verantwortung der Handlungen des Opfers entnehmen
- Hilfestellung
- Beziehung
- Stellung
- ...

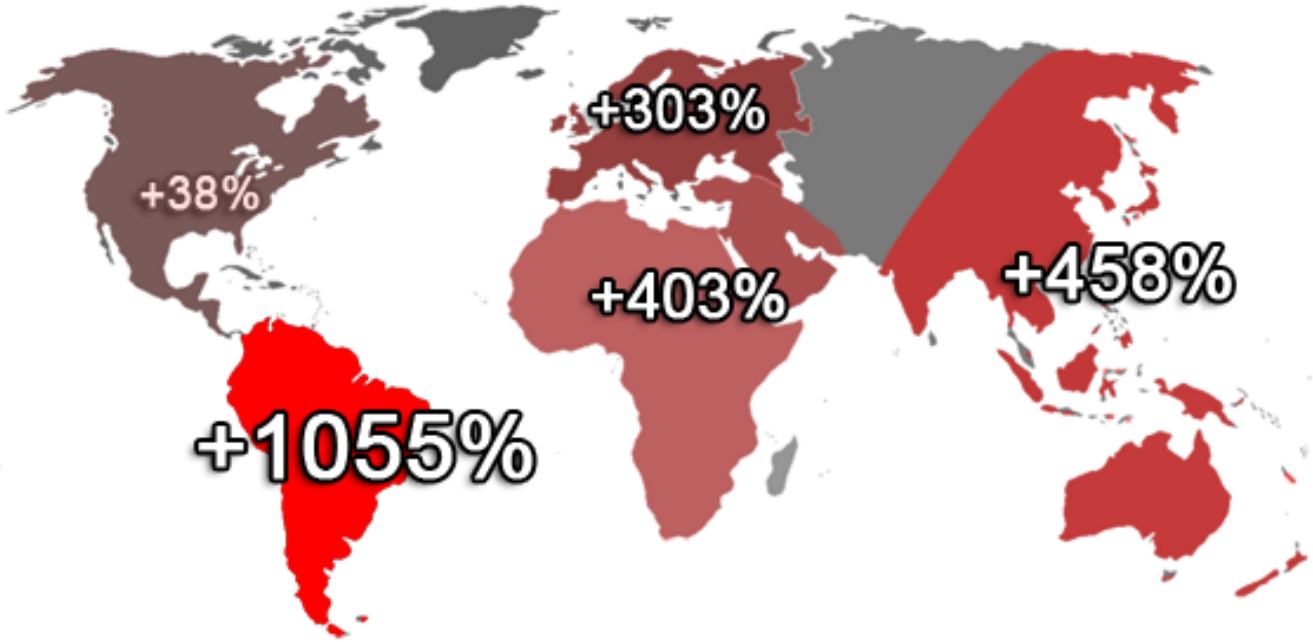
Ausbeutung, Manipulation & Angriff

- Human Based Attacks
  - Identitätsdiebstahl
  - Vortäuschen von Ermächtigungen
  - Technischer Support
  - Reverse Social Engineering
  - Shoulder-Surfing
  - Dumpster-Diving
  - Persönlicher Auftritt

Ausbeutung, Manipulation & Angriff

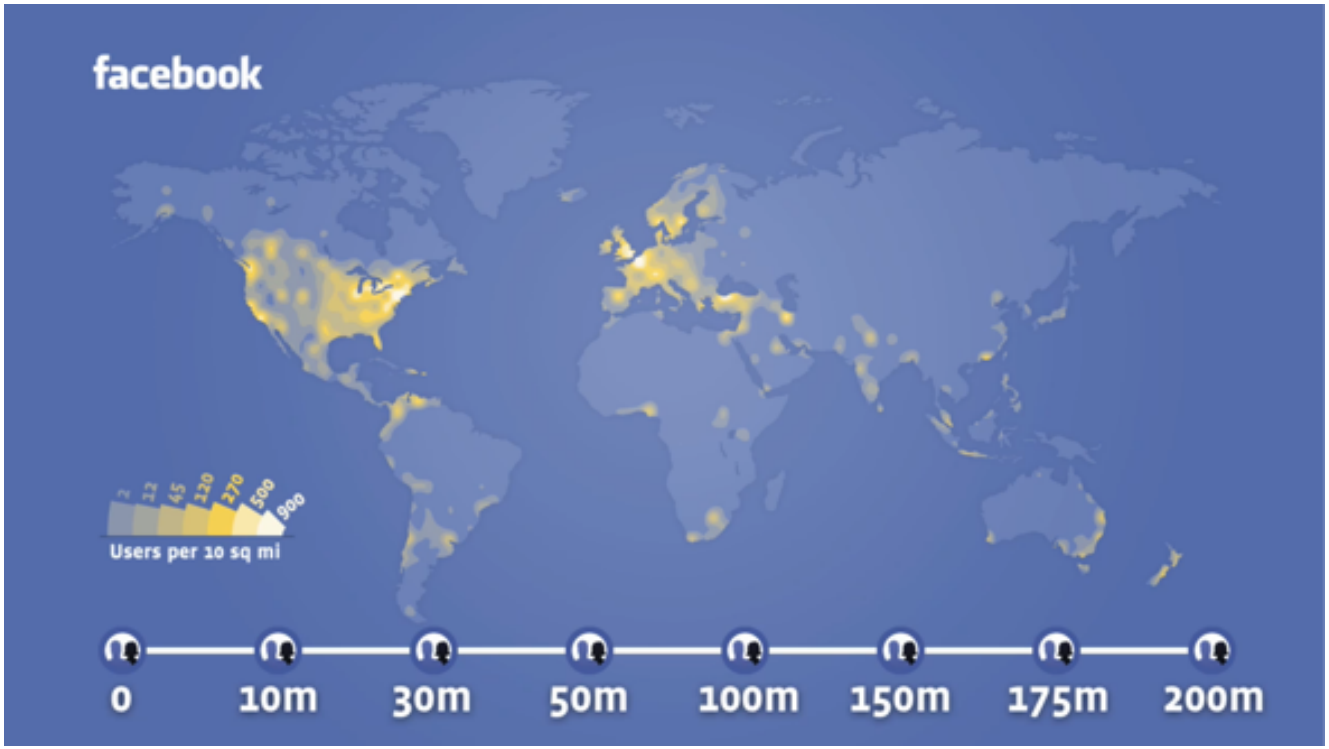
- Human Based Attacks
  - Identitätsdiebstahl
  - Vortäuschen von Ermächtigungen
  - Technischer Support
  - Reverse Social Engineering
  - Shoulder-Surfing
  - Dumpster-Diving
  - Persönlicher Auftritt
- Computer Based Attacks
  - Phishing
  - Spam
  - Malware
  - Suggestion vertrauenswürdiger Quelle

Soziale Netzwerke



http://www.techcrunch.com/2008/08/12/facebook-is-not-only-the-worlds-largest-social-network-it-is-also-the-fastest-growing/

Soziale Netzwerke



http://www.venturebeat.com/2009/04/08/trying-to-analyze-facebooks-latest-statistics-more-status-updates-more-content-sharing/

Ein konkretes Soziales Netzwerk: Twitter

- Soziales Netzwerk & Microblogging Anbieter
- Gegründet 2006
- Mehr als $\sim$ 1.780.000 User
- Genutzt von Privatpersonen & Unternehmen
- `http://www.twitter.com/`*`[username]`*

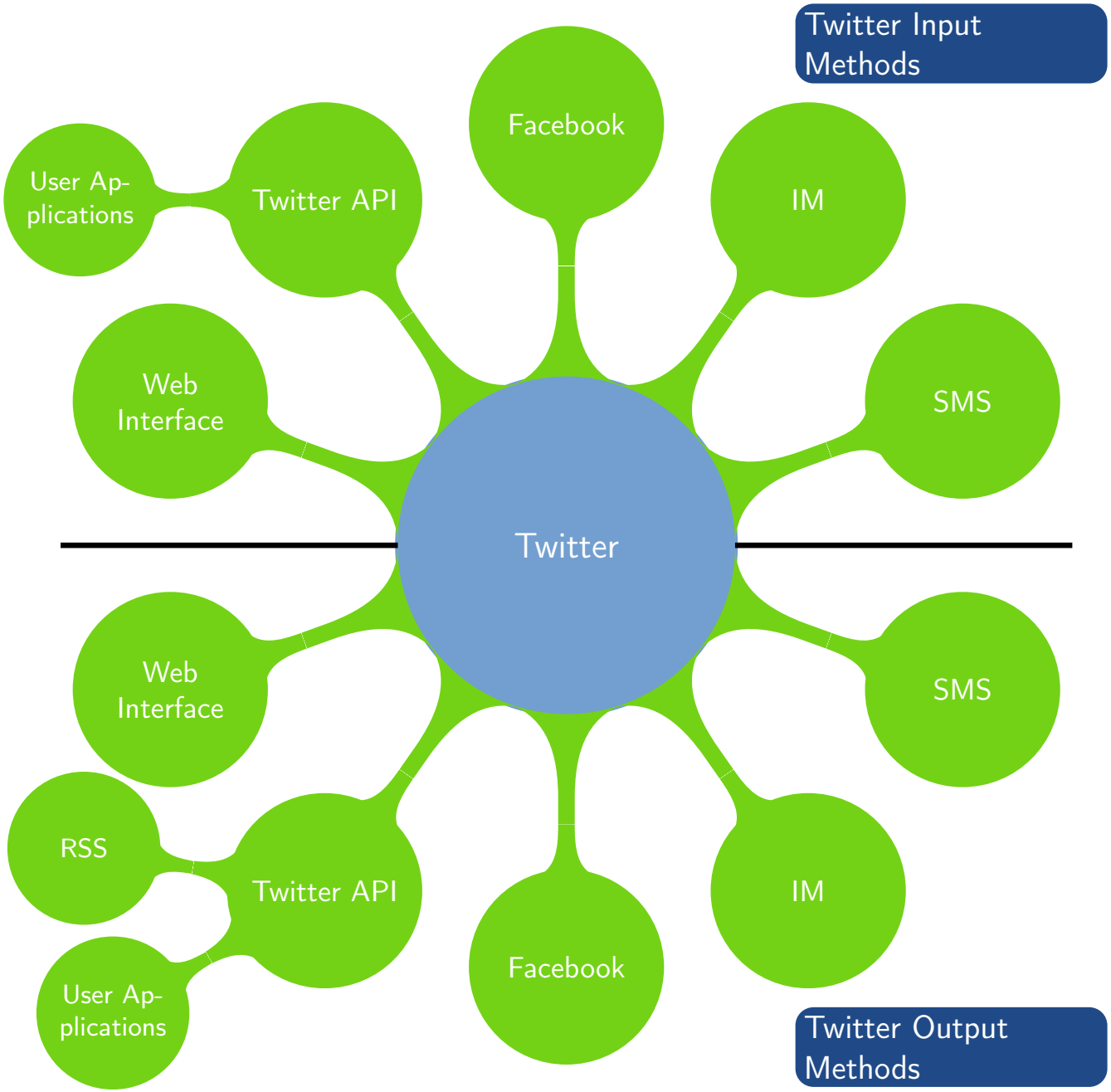

twitter
Home Profile Find People Settings Help Sign out
twitter
Follow
Maintenance window rescheduled
http://tinyurl.com/qb8y99
ungefähr 15 Stunden ago from twitterfeed
Password reset emails not working, fix on the way http://tinyurl.com/qz3t3h
ungefähr 16 Stunden ago from twitterfeed
Back from site maintenance; working on site latency issues http://tinyurl.com/pdsojj
5:17 PM May 8th from twitterfeed
Heading into maintenance mode: http://tinyurl.com/c6ngsa See you in a bit!
1:54 PM May 8th from web
Planned maintenance tomorrow, Monday http://tinyurl.com/c6ngsa
3:16 PM May 7th from twitterfeed
Search running behind http://tinyurl.com/dgjtv3
6:17 PM May 4th from twitterfeed
Welcoming @akshay_adb and @ded to the team today. Also, our new office (next to the old office)!
4:00 PM May 4th from web
Updating your status via a URL Param (http://bit.ly/tweet-in-param) has been fixed!
5:18 PM Apr 30th from web
Display issues during code changes http://tinyurl.com/cy6k2u
2:46 PM Apr 30th from twitterfeed
Bringing back disabled features (sidebar trends, background image uploads) http://tinyurl.com/d75q4g
10:47 AM Apr 30th from twitterfeed
Fixing the elevated error rate http://tinyurl.com/cpwc73
Name Twitter
Location San Francisco, CA
Web http://twitter.com
Bio Always wondering what everyone's doing.
31
following_profile
1,091,962
followers_profile
Updates 351
Favorites
Actions
block twitter
Following
RSS feed of twitter's updates

Tweet

„@max you should check the weather forecast, see http://tinyurl.com/plmr3m“

9:34 AM August 11th from web in reply to max

- 140 Zeichen
- @username, #topic, . . .
- Uhrzeit & Datum
- Benutzte Infrastruktur
- reply, new message


Twitter Input Methods
Facebook
User Ap-plications
Twitter API
IM
Web Interface
SMS
Twitter
Web Interface
SMS
RSS
Twitter API
IM
Facebook
User Ap-plications
Twitter Output Methods

Twitter API

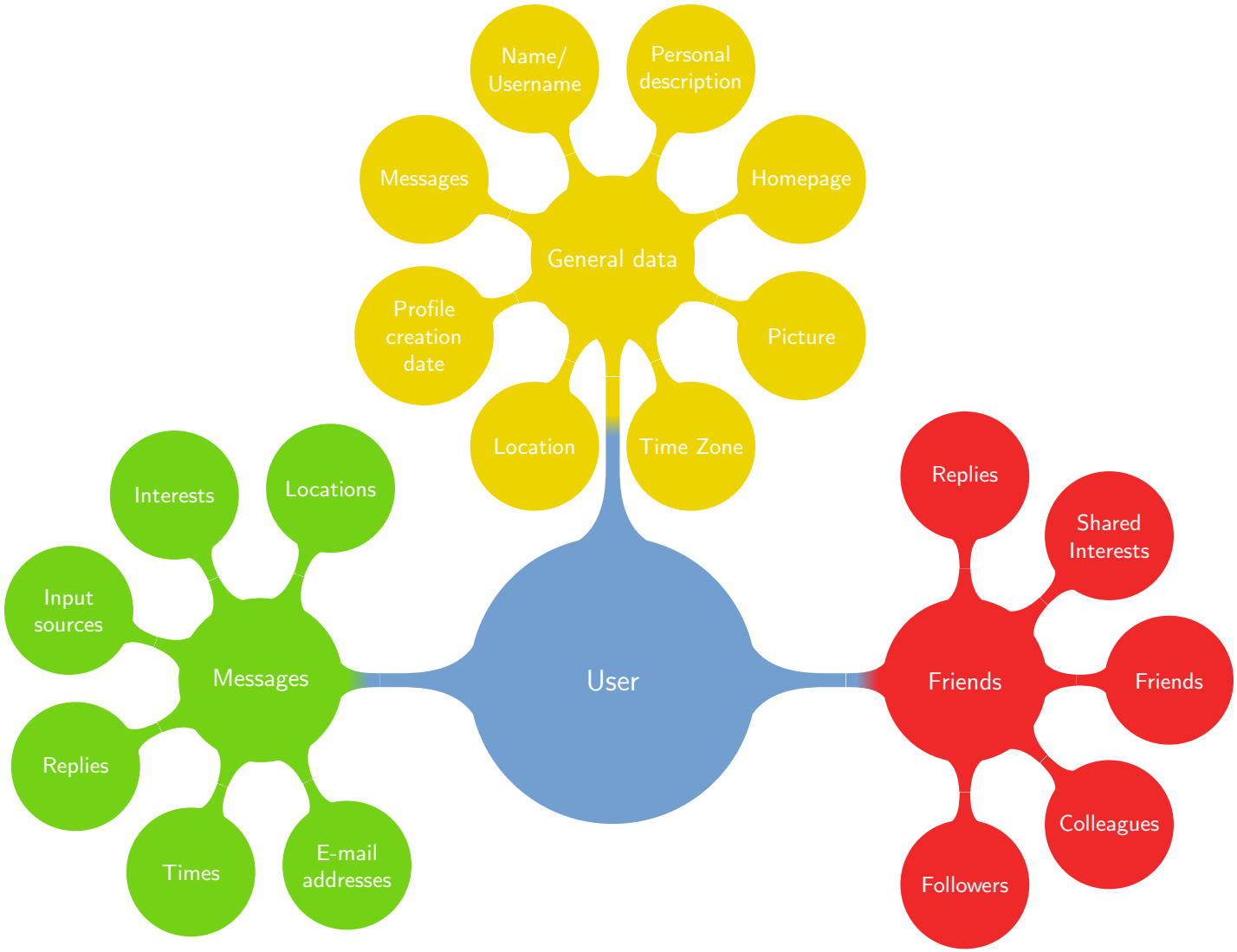
- http://apiwiki.twitter.com/Twitter-API-Documentation
- GET, POST HTTP-Methoden
- GET Anfragen beschränkt auf 150 Requests pro Stunde
- JSON, XML, RSS, Atom

```
GET http://twitter.com/users/show/barackobama.json
```

Twitter API (2)

```
created_at:        "Mon Mar 05 22:08:25 +0000 2007"
description:       "The president of the United States of America"
favourites_count:  0
followers_count:   1221122
friends_count:     776706
Id:                813286
location:          "Chicago, IL"
name:              "Barack Obama"
profile_image_url: "http://s3.amazonaws.com/twitter_production/ ↪
                   profile_images/219314140/obama_4color_omark_normal.jpg
protected:         false
screen_name:       "BarackObama"
statuses_count:    272
time_zone:         "Central Time (US & Canada)"
url:               "http://www.barackobama.com"
```

Prototyp


Name/
Username
Personal
description
Messages
Homepage
General data
Profile
creation
date
Picture
Location
Time Zone
Interests
Locations
Input
sources
Messages
Replies
Times
E-mail
addresses
User
Replies
Shared
Interests
Friends
Friends
Colleagues
Followers

DEMO

Evaluation

- Neue Gefahren
  - Informationsphase wird ersetzt bzw. erleichtert
  - Geringes Risiko entdeckt zu werden
  - Firmen & Privatpersonen verwundbar
  - Automatisierte Angriffe
- Ausblick
  - Zusätzliche Quellen
  - Genauere Informationsanalyse
  - Weitere Automatisierung

Related Work (1)

- The Art of Deception
  - K. Mitnick, W. Simon
  - ISBN 076454280X
- Social Engineering: The "Dark Art"
  - T. Thornburgh
  - http://doi.acm.org/10.1145/1059524.1059554
- Social Phishing
  - T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer
  - http://doi.acm.org/10.1145/1290958.1290968
- Social Networks and Context-Aware Spam
  - G. Brown, T. Howe, M. Ihbe, A. Prakash, K. Borders
  - http://doi.acm.org/10.1145/1460563.1460628

Related Work (2)

- Information Revelation and Privacy in Online Social Networks
  - R. Gross, A. Acquisti, H. John
  - http://doi.acm.org/10.1145/1102199.1102214
- A Few Chirps About Twitter
  - B. Krishnamurthy , P. Gill, M. Arlitt
  - http://doi.acm.org/10.1145/1397735.1397741
- Why We Twitter
  - A. Java, X. Song, T. Finin, B. Tseng
  - http://doi.acm.org/10.1145/1348549.1348556

Fragen?

```
git clone http://home.cs.tum.edu/siegel/dev/thesis.git
```