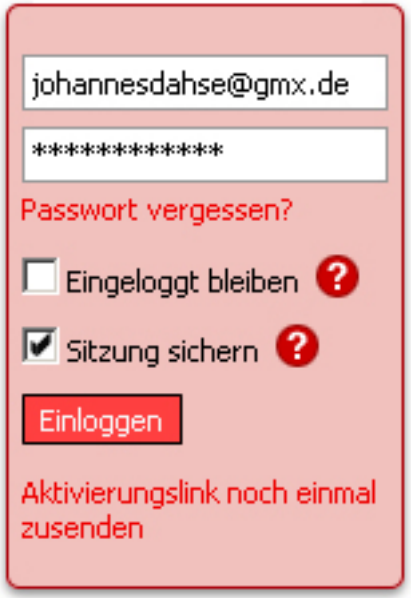
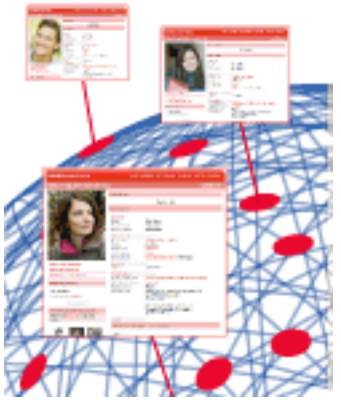


Soziale Netzwerke

Soziale Netzwerke

1. Einleitung

Was sind Soziale Netzwerke ?



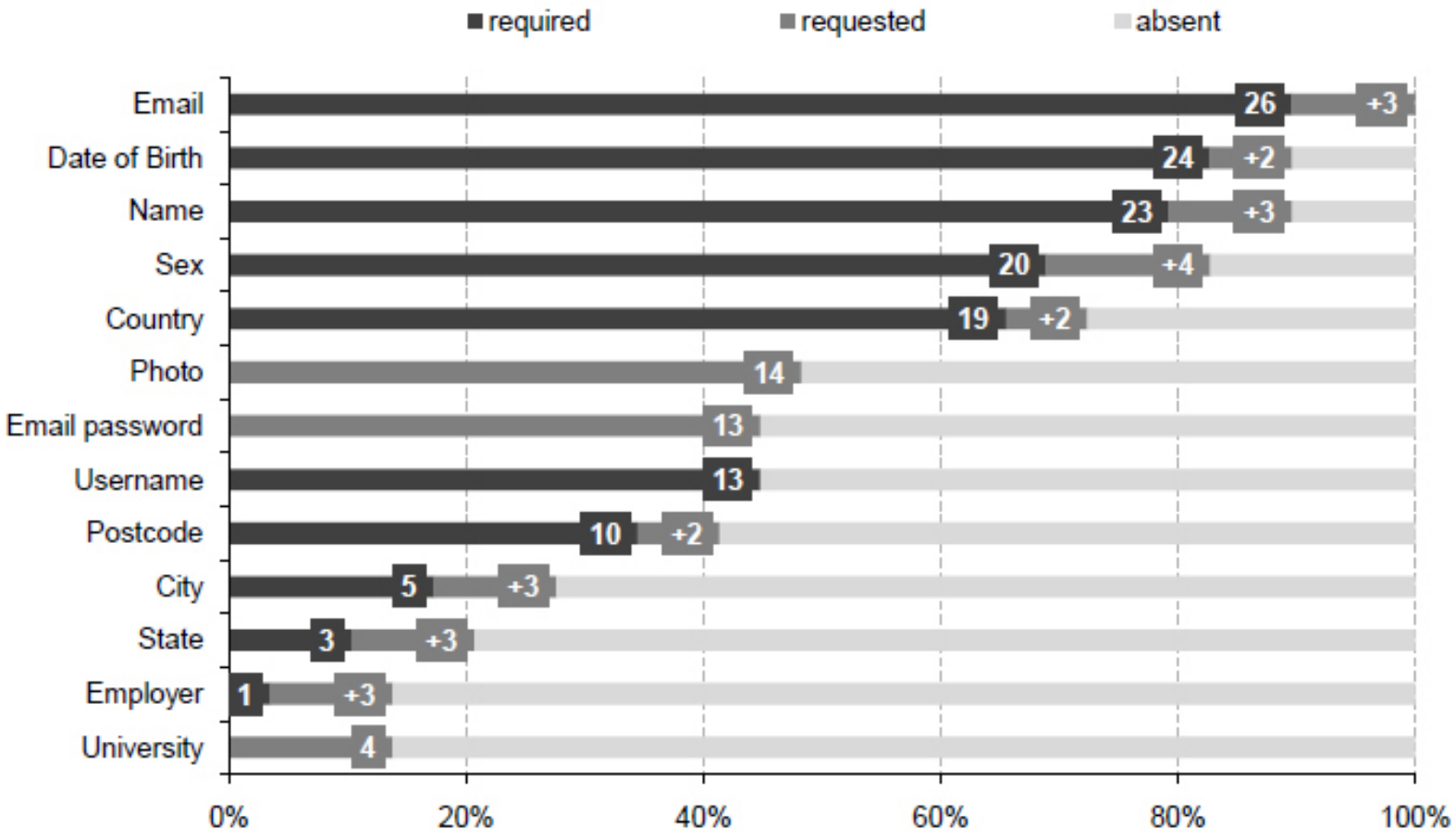
- Internetplattform bestehend aus mehreren Benutzerprofilen
- Profile sind verknüpft durch Freundschaften, Gruppen, etc.
- Benutzer stellt freiwillig persönliche Angaben auf sein Profil um Gleichgesinnte zu finden
- gehören zu den weltweit am meisten genutzten Webseiten
- mehrere hundert Millionen Benutzer

Beispiel Facebook

- ursprüngl. für amerikanische Studenten
- Statistiken heute:
  - 70% nicht-amerikanische Benutzer
  - 70 verschiedene Sprachen unterstützt
  - 400 Mio. Benutzer (Vergleich: StudiVZ 17 Mio.)
  - Zahl wächst wöchtentlich um 3%
  - Alexa Top Sites: Platz 2
  - größte Bilderdatenbank mit 1 Bill. Bilder

2. Funktionsweisen der Sozialen Netzwerke

2.1 Registrierungs-Daten



(bei 29 untersuchten Netzwerken)

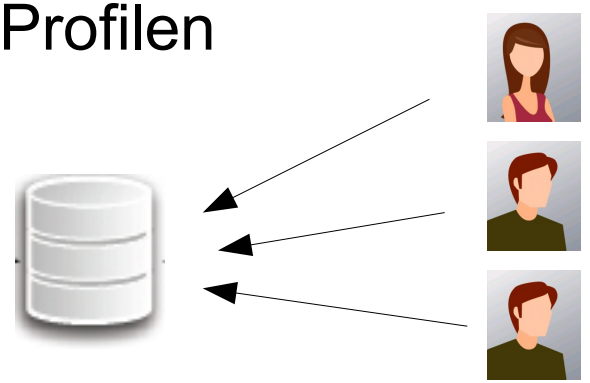
2.2 Privacy Controls und Defaults

- Profil ist für das Internet öffentlich einsehbar (41%)
- Profil ist nur für Mitglieder des Sozialen Netzwerkes einsehbar (48%)
- Profil ist nur für bestimmte Gruppen oder Sub-Netzwerke einsehbar (7%)
- Profil ist nur für Freunde und deren Freunde einsehbar (0%)
- Profil ist nur für Freunde einsehbar (3%)

3. Angriffe auf Soziale Netzwerke

3.1 Automatisiertes User Profiling

- Angreifer programmiert „Crawler“
- automatisiert und angepasst auf Netzwerk:
  - Login
  - Besuch auf Benutzerprofil
  - Extrahieren und Speichern von Informationen
  - Finden von neuen Profilen
  - Logout



3.1 Automatisiertes User Profiling

- Server-seitige Gegenmaßnahmen:
  - CAPTCHAs

  - Click-Checks

- Umgehbar durch:
  - CAPTCHA-Breaker, Halbautomatisierung
  - Parallelisierung

3.1 Automatisiertes User Profiling

- Am Beispiel der VZ-Netzwerke:
  - StudiVZ: 09.12.2006, 1 Mio. Profile, 10 PCs + 4h, http://studivz.irgendwo.org
  - StudiVZ: März .2009, 5 Mio. Profile, *iCloner* Testlauf mit CAPTCHA-Brechung
  - SchülerVZ: 16.10.2009, 1 Mio. Profile, ungeklärter Selbstmord in Haft
  - SchülerVZ: 28.10.2009, 100 000 Profile, PoC für eingeschränkte Profile
  - SchülerVZ: 04.05.2010, 1.6 Mio. Profile, Offenlegung des Crawlers *LenaML*

inhaltsVZ

Suche

Lisa als Freund hinzufügen
Lisa eine Nachricht schicken
Lisa gruscheln
Lisa Freunden zeigen
Lisa melden / ignorieren

Privatsphäre

Lisas Profilseite ist für Dich nur teilweise sichtbar.

Information

Account

Name: Lisa
Verzeichnis: studiVZ

Allgemeines

Hochschule: Ruhr-Universität Bochum

aber:
User Profiling kann keine geschützten Benutzer-Profile einlesen

inhaltsVZ

Suche

Lisa als Freund hinzufügen
Lisa eine Nachricht schicken
Lisa gruscheln
Lisa Freunden zeigen
Lisa melden / ignorieren

Privatsphäre

Lisas Profilseite ist für Dich nur teilweise sichtbar.

Information

Account

Name: Lisa
Verzeichnis: studiVZ

Allgemeines

Hochschule: Ruhr-Universität Bochum

Neue Freundschaftsanfragen

Angreifer möchte mit Dir befreundet sein.

bestätigen
ablehnen
anschreiben

inhaltsVZ

Suche

Lisa ist auf 14 Fotos verlinkt
Lisas Fotoalben (1)
Alle Freunde von Lisa
Lisa eine Nachricht schicken
Lisa gruscheln
Lisas Freunden zeigen
Lisa melden / ignorieren

Fotoalben

Lisa hat ein Album.

Verbindung


Angreifer


Lisa

Information

Account

Name:	Lisa
Verzeichnis:	studiVZ
Mitglied seit:	11.07.2006
Letztes Update:	28.03.2010

Allgemeines

Hochschule:	Ruhr-Universität Bochum (seit 2006)
Status:	Student(in)
Studiengang:	Hebamme
Geschlecht:	weiblich
Geburtstag:	07.06.

Kontakt

ICQ:	98765432
Land:	Deutschland

Persönliches

Auf der Suche nach:	netten Leuten, Partys, Was sich eben ergibt
Beziehungsstatus:	solo

inhaltsVZ

Suche

Lisa als Freund hinzufügen
Lisa eine Nachricht schicken
Lisa gruscheln
Lisa Freunden zeigen
Lisa melden / ignorieren

Privatsphäre

Lisas Profilseite ist für Dich nur teilweise sichtbar.

Information

Account

Name: Lisa
Verzeichnis: studiVZ

Allgemeines

Hochschule: Ruhr-Universität Bochum

Neue Freundschaftsanfragen

Angreifer möchte mit Dir befreundet sein.

bestätigen
ablehnen
anschreiben

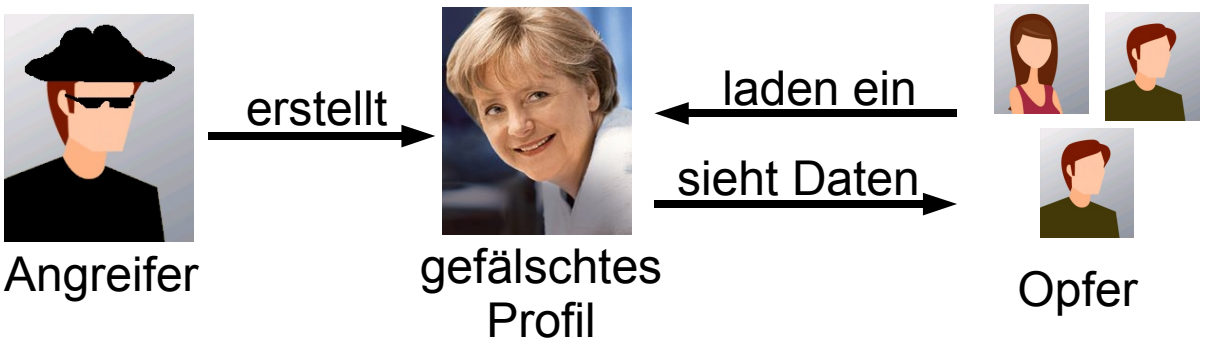
→ auffällig, Identitätsdiebstahl

3.2 Impersonating

- gefälschtes Profil einer bekannten Person mit gesammelten Infos aus dem WWW
- warte auf Freundschaftseinladungen

3.2 Impersonating

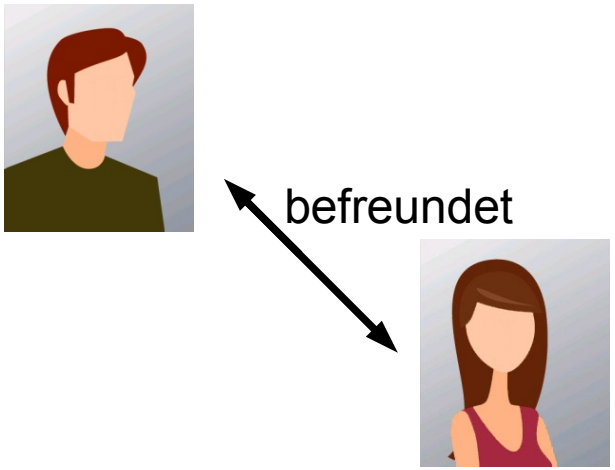
- gefälschtes Profil einer bekannten Person mit gesammelten Infos aus dem WWW
- warte auf Freundschaftseinladungen



- passiv, selbst initiierter Kontakt von bekannter Person in den meisten Fällen verdächtig
- zufällige Opfer

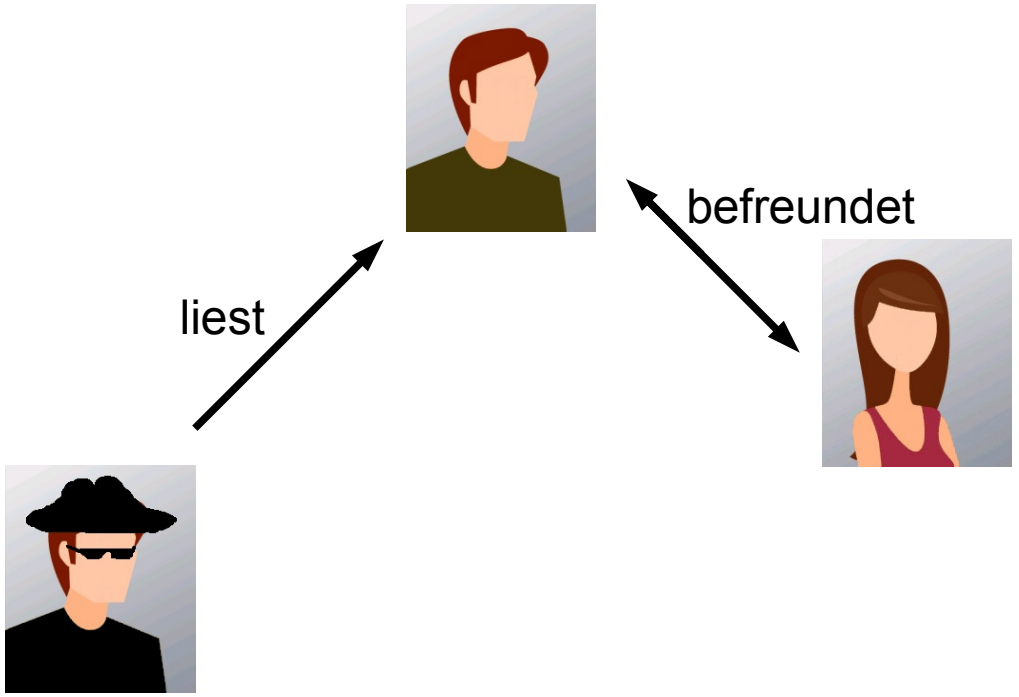
3.3 Profile Cloning

- gefälschtes Profil eines existierenden Freundes mit kopierten Informationen



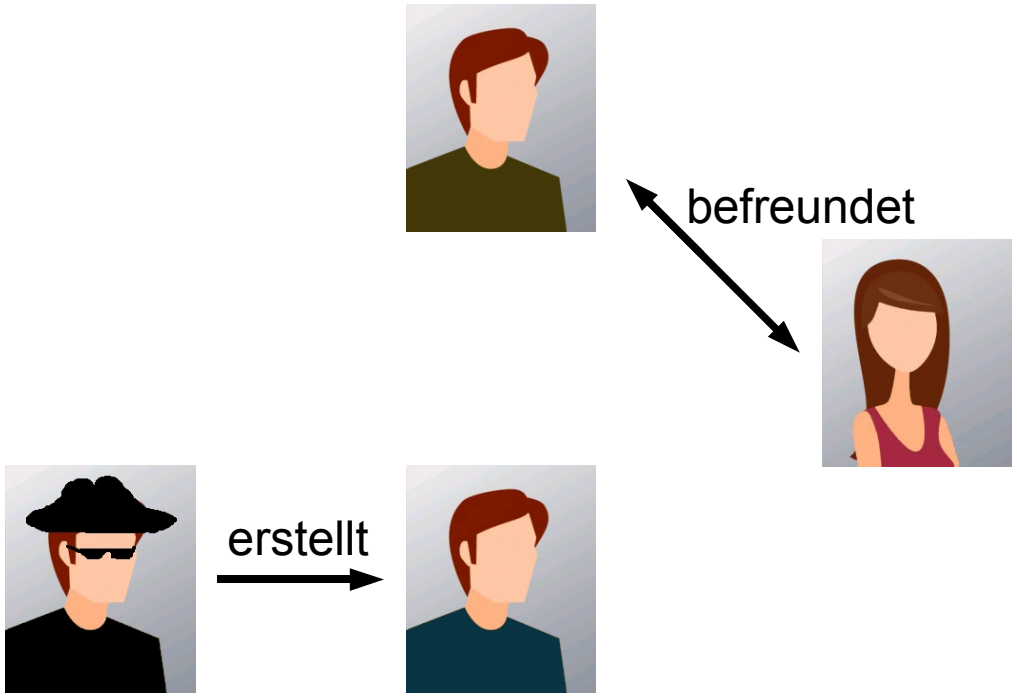
3.3 Profile Cloning

- gefälschtes Profil eines existierenden Freundes mit kopierten Informationen



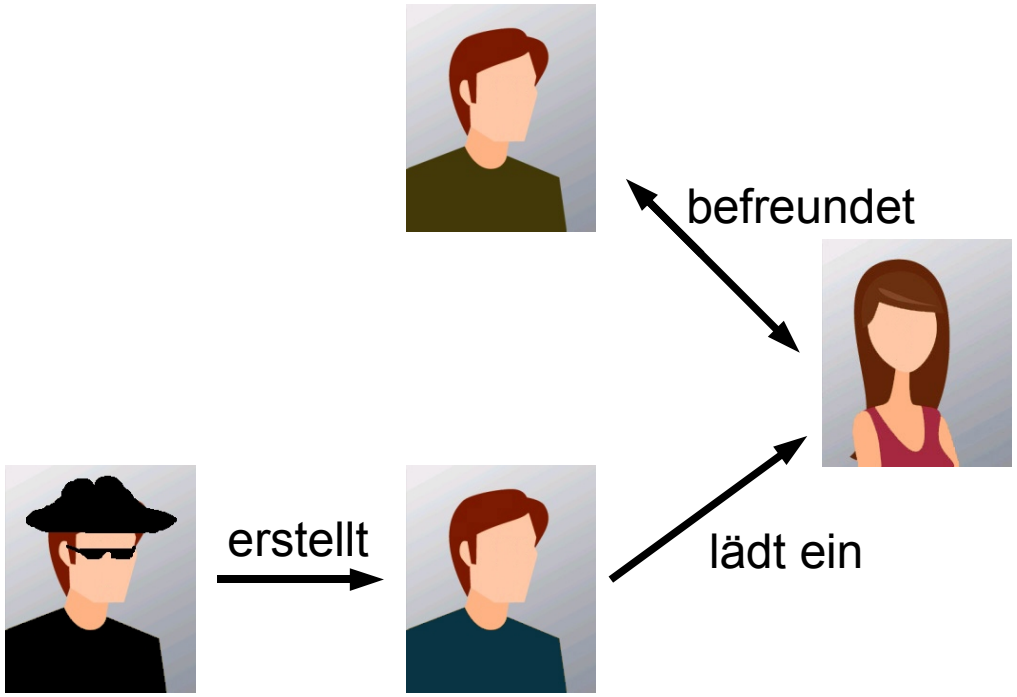
3.3 Profile Cloning

- gefälschtes Profil eines existierenden Freundes mit kopierten Informationen



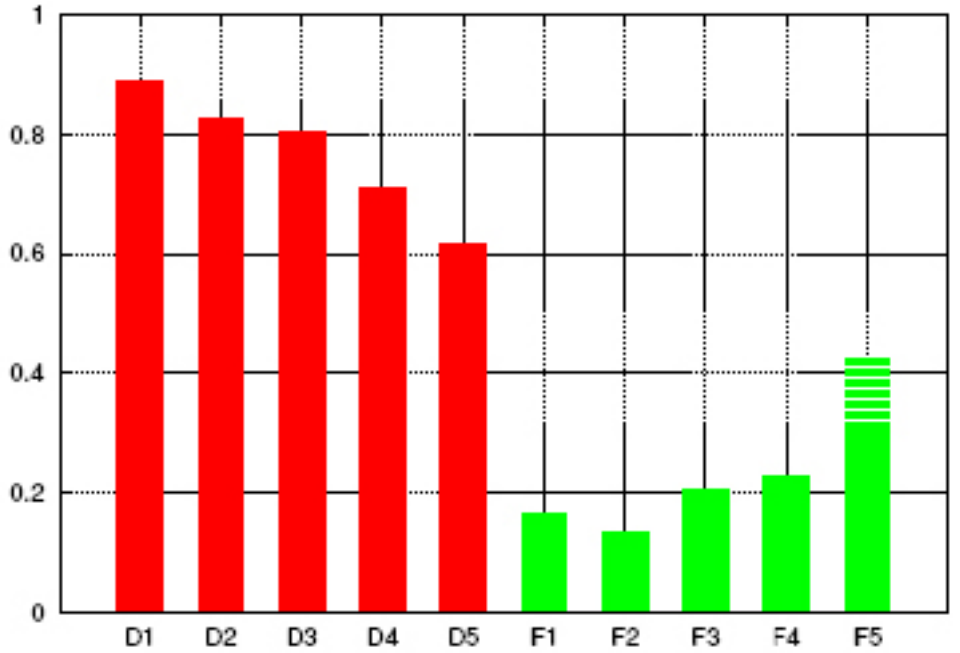
3.3 Profile Cloning

- gefälschtes Profil eines existierenden Freundes mit kopierten Informationen



3.3 Profile Cloning

- Experiment Bilge et. al.: 700 Benutzer kontaktiert. Erfolgsrate:



D1-D5: Profile Cloning, F1-F5: Zufallsangaben

3.3 Profile Cloning

- Experiment zeigt Erfolgsraten von 60-90%
- Nachteil:
  - Freund existiert bereits in der Freundesliste des Opfers
  - bei regelmäßigen Kontakt auffällig

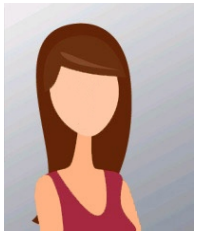
→ Cross-Site Profile Cloning

inhaltsVZ

Suche

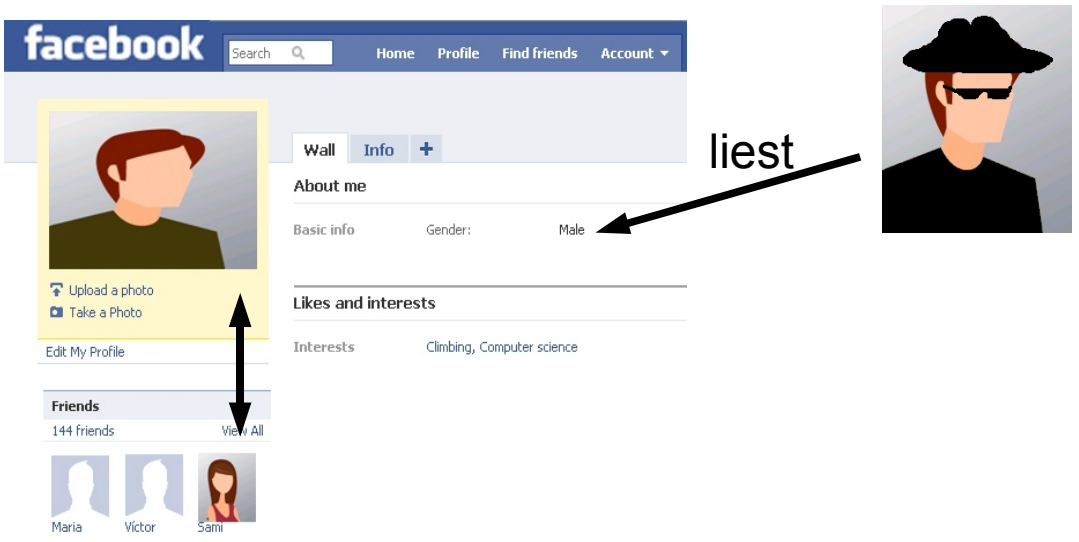
3.4 Cross-Site Profile Cloning

- Angreifer klont ein Profil, welches im gleichen Netzwerk noch nicht existiert, aber in einem anderen Netzwerk bereits mit dem Opfer befreundet ist



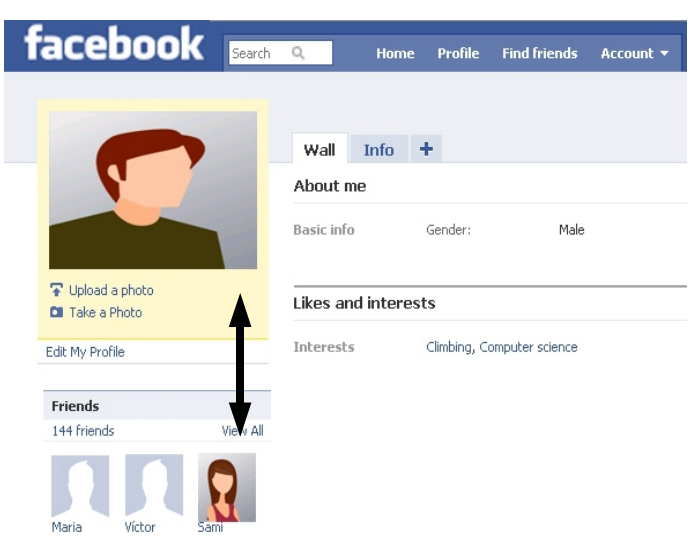
3.4 Cross-Site Profile Cloning

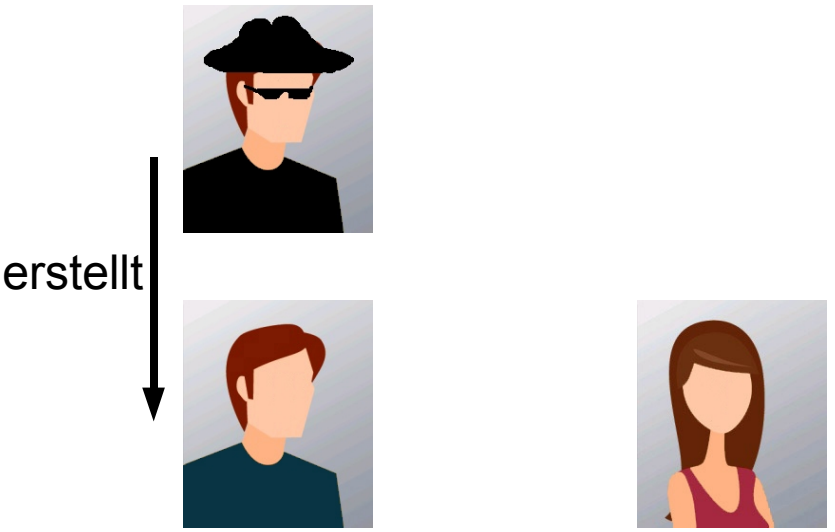
- Angreifer klont ein Profil, welches im gleichen Netzwerk noch nicht existiert, aber in einem anderen Netzwerk bereits mit dem Opfer befreundet ist



3.4 Cross-Site Profile Cloning

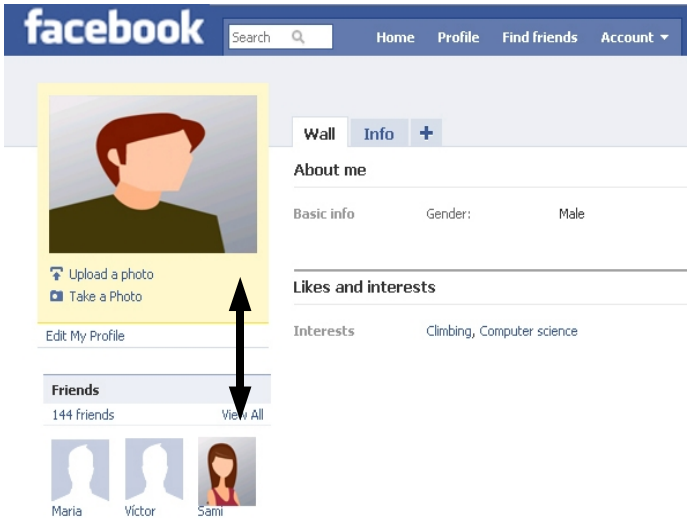
- Angreifer klont ein Profil, welches im gleichen Netzwerk noch nicht existiert, aber in einem anderen Netzwerk bereits mit dem Opfer befreundet ist



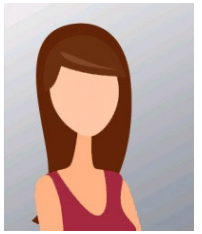


3.4 Cross-Site Profile Cloning

- Angreifer klont ein Profil, welches im gleichen Netzwerk noch nicht existiert, aber in einem anderen Netzwerk bereits mit dem Opfer befreundet ist

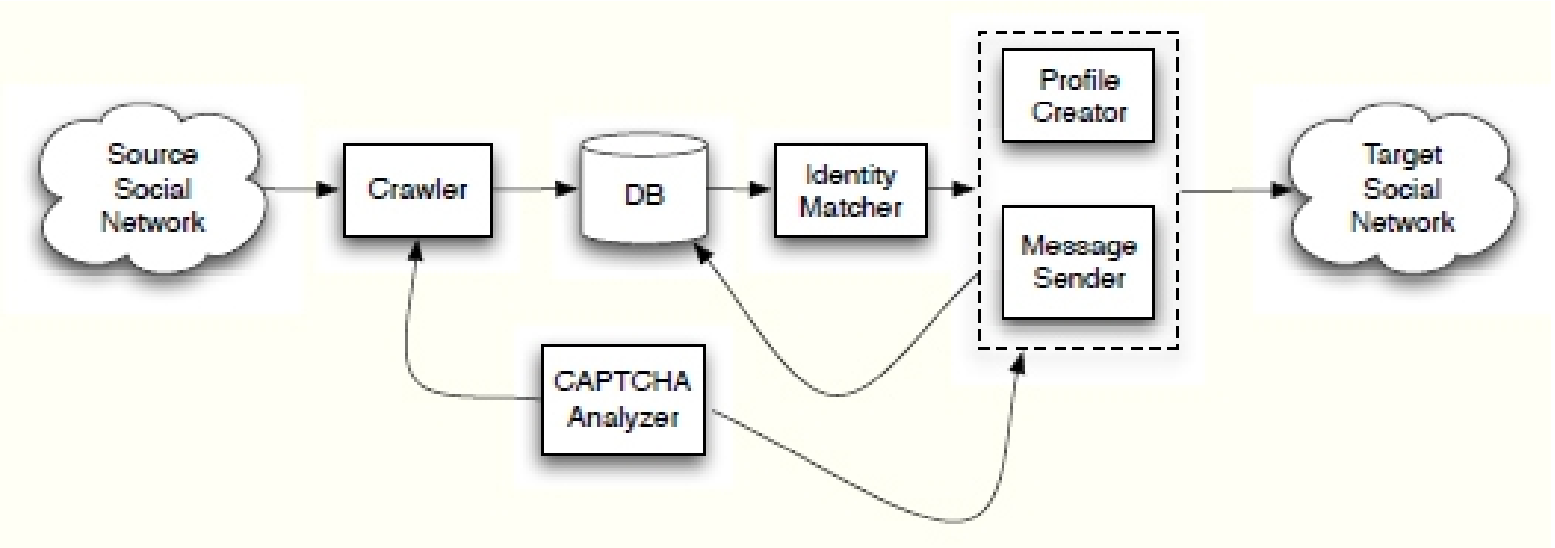


lädt ein



3.4 Cross-Site Profile Cloning

- automatisiert mit *iCloner* (Bilge et. al.)



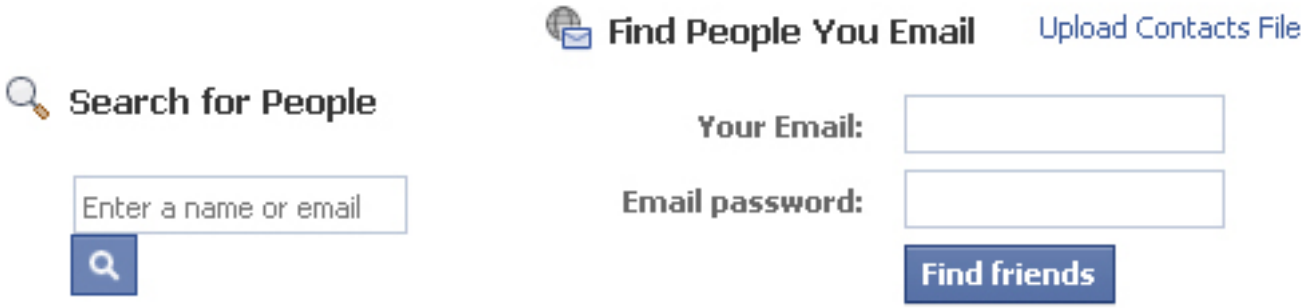
- Identity Matcher: nicht-trivial
- Experiment mit 78 Einladungen: 56% Erfolg

inhaltsVZ

Suche

3.5 Email Abusing

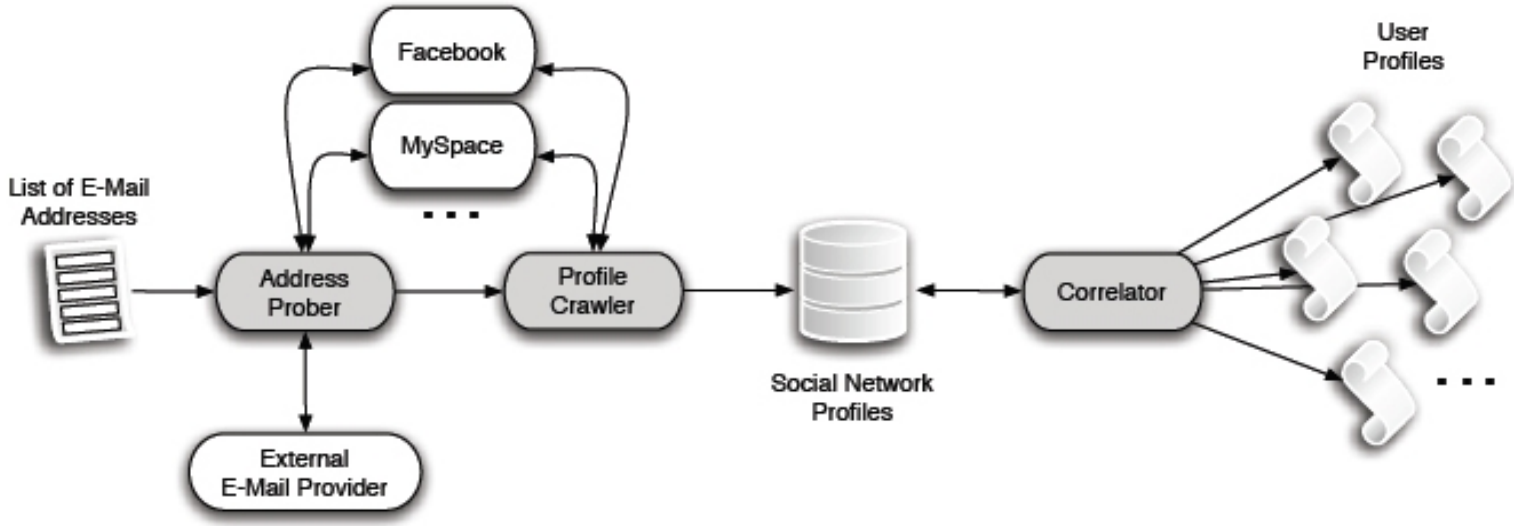
- Email-Suchfunktion zum Finden von Freunden



- Mißbrauch der Email-Suchfunktion:
  - Identity Matcher
  - Validierung von Emailadressen (Spam)
  - Email Fuzzing

3.5 Email Abusing

- automatisierter Tool implementiert von Balduzzi et. al.:



- Zusammenführen von Profil-Informationen
- Falschangaben/anonymisierte Profile enttarnen

3.6 Motivation

- Was kann ein Angreifer mit den gesammelten Daten anstellen ?

3.6 Motivation

- Was kann ein Angreifer mit den gesammelten Daten anstellen ?
  - (Statistiken erstellen)
  - Personalisierter Spam
  - Personalisiertes Phishing
  - Personalisiertes Social Engineering
  - Personalisierte Malware-Verbreitung
  - Personalisierte XSS-Wurm-Verbreitung

3.6 Motivation

- Was kann ein Angreifer mit den gesammelten Daten anstellen ?
  - (Statistiken erstellen)
  - Personalisierter Spam
  - Personalisiertes Phishing
  - Personalisiertes Social Engineering
  - Personalisierte Malware-Verbreitung
  - Personalisierte XSS-Wurm-Verbreitung

(morgen XSS-Wurm-Contest Hackerpraktikum)

3.6 Motivation

- Personalisiert == höhere Erfolgsquote, dass Link (Spam, Phishing, Malware) geklickt wird
- Social Phishing Experiment (Jagatic et. al.):
  - 16% Erfolgsrate ohne Personalisierung
  - 72% Erfolgsrate mit Personalisierung

inhaltsVZ

Suche

Spam-Mail vom letzten Monat:

To: johannesdahse@gmx.de
From: **Bastian** <bastian@privater-spass.com>
Date: Fri, 18 Jun 2010 06:42:40 +0200
Subject: **Johannes**: Das ist doch Katja?

Hallo **Johannes**,

guck mal was ich gerade gefunden habe:
http://www.privater-spass.com

Das ist doch Katja aus dem **4ten Semester**, oder??

Krasse Seite: da können Mädchen private Filme hochladen,
dass Katja einen solchen Nebenjob hat hätte ich nicht gedacht :o)

Hast Du sie gefunden?

Grüße,
Bastian

4. Fazit

- Daten sind leicht automatisiert auszulesen
- personalisierte Angriffe sind sehr effizient
- hohes Mißbrauchspotential der Daten
- dichte Angriffsfläche durch hohe Benutzerzahlen
- wenig Bewusstsein der Benutzer für Privatsphäre
- unzureichende Schutzmaßnahmen+Aufklärung

- Problem: Freizügigkeit der Benutzer mit ihren Daten ist das Geschäftsmodell

Suche

Account löschen

Möchtest Du wirklich, dass wir Dich aus studiVZ löschen?

Alle Deine Freunde werden Dich vermissen!
... und wir auch!

Wenn Du möchtest, kannst Du uns hier einen Grund für Deine Abmeldung nennen:

- ○ Kein Grund
- ○ Ich finde studiVZ sinnlos
- ○ Ich bin mit den Nutzungsbedingungen nicht einverstanden
- ◉ Ich fühle mich nicht sicher im studiVZ
- ○ Ich wollte nur mal schauen, wie das auf studiVZ so ist
- ○ Ich komme mit der Bedienung von studiVZ nicht zurecht
- ○ Die Nutzung von studiVZ belastet mich sozial
- ○ Ich bekomme zu viele E-Mails von studiVZ
- ○ Das ist nur vorübergehend, ich melde mich wieder an
- ○ Ich habe noch einen anderen studiVZ-Account
- ○ Anderer Grund: `"><script>document.location.href="http://www.fluxfingers.n`

Meinen Account löschen | Vergiss es

johannesdahse@gmx.de

****

Passwort vergessen?

Eingeloggt bleiben

Sitzung sichern

Einloggen

Aktivierungslink noch einmal zusenden

Vielen Dank für Ihre Aufmerksamkeit !

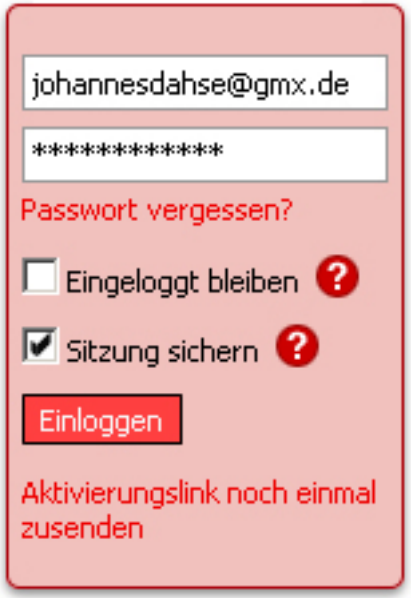
Danke, dass Du studiVZ genutzt hast.
Schade, es war schön mit Dir!

Falls Du doch zurückkommen möchtest – Du weißt ja, wo Du uns findest.

Immatrikulieren
Jetzt einschreiben

Entdecke studiVZ
Was bringt mir das?

Fragen ?



Quellenangaben

Leyla Bilge, Thorsten Strufe, Davide Balzarotti, und Engin Kirda.
All your contacts are belong to us: Automated identity theft attacks on social networks. In WWW 09.

Marco Balduzzi, Christian Platzer, Thorsten Holz, Engin Kirda, Davide Balzarotti, und Christopher Kruegel.
Abusing social networks for automated user profiling. In RAID 2010.

Joseph Bonneau und Sören Preibusch.
The privacy jungle: On the market for data protection in social networks. In WEIS 2009.

facebook, *statistics,* http://www.facebook.com/press/info.php?statistics

Vzblog, *VZ baut Marktführerschaft in Deutschland mit 17 Millionen Nutzern weiter aus*, http://blog.studivz.net/2010/07/14/

Projekt Datenschutz, *Datenschutzvorfälle,*
http://projekt-datenschutz.de/search/node/schülerVZ