
Social Network Security

Internet Security [1] VU

Paolo Milani Comparetti, Christian Platzer,
Gilbert Wondracek, **Markus Huber**, Edgar Weippl
inetsec@iseclab.org

News from the Lab

Int. Secure Systems Lab
Vienna University of Technology

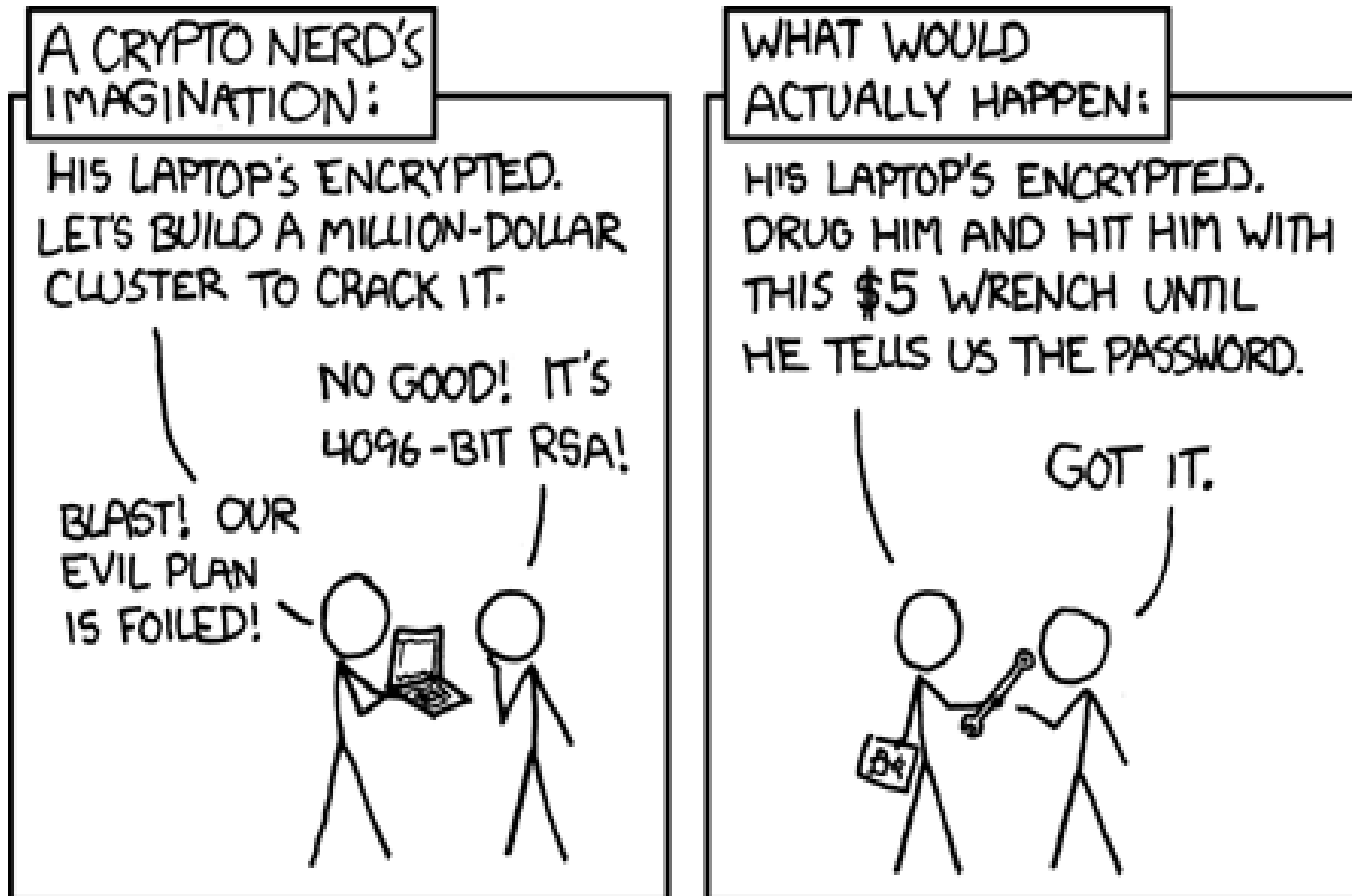
- *Challenge 6 – Stack Buffer Overflow*
 - continues one more week
 - so far, solved by 14 people
 - *respect!*
 - If you have some spare time, give it a shot :-)

Outline

- Today ... Social Network Security or “nothing to hide”?
- Socio-technical attacks on Social Networking Sites
 - (Automated) social engineering
 - Chatterbots
 - Cross-profile cloning
 - Friend-in-the-middle attacks
 - User de-anonymization
- Recent cases and tools

Security <http://xkcd.com/538/>

Int. Secure Systems Lab
Vienna University of Technology



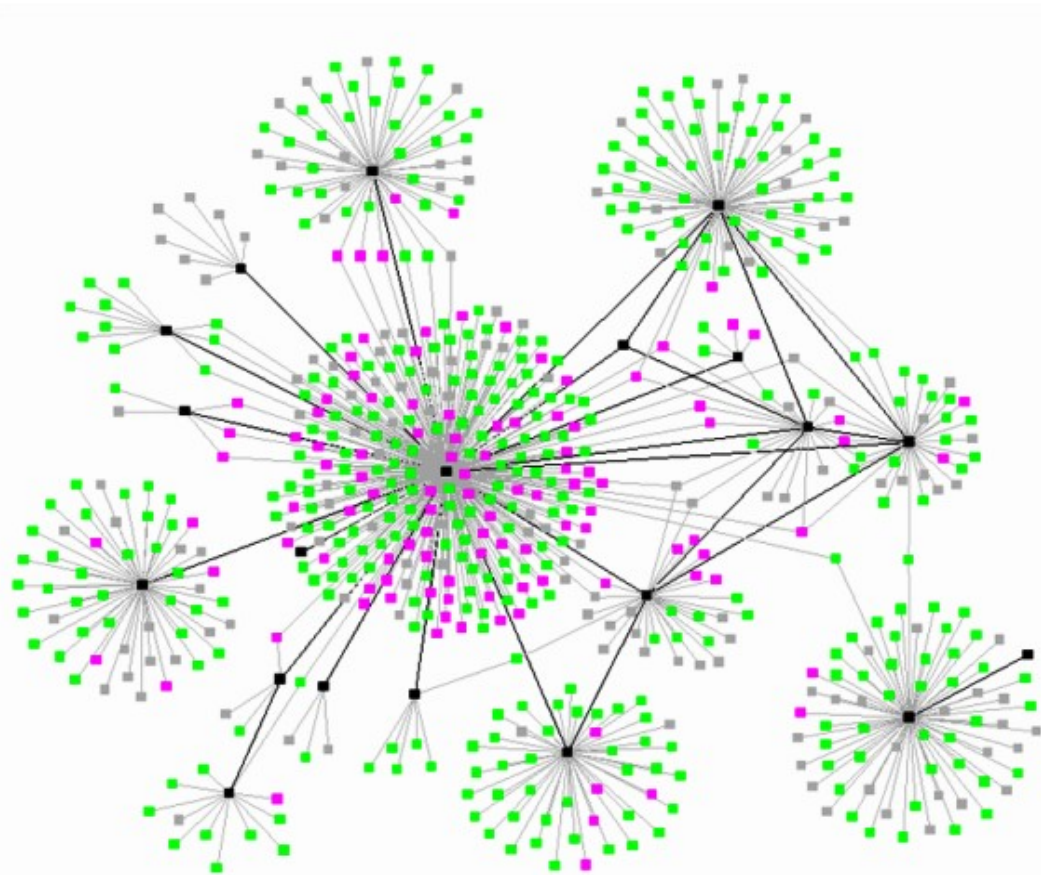
Social Networking Sites

*Int. Secure Systems Lab
Vienna University of Technology*

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

Social graph example

*Int. Secure Systems Lab
Vienna University of Technology*



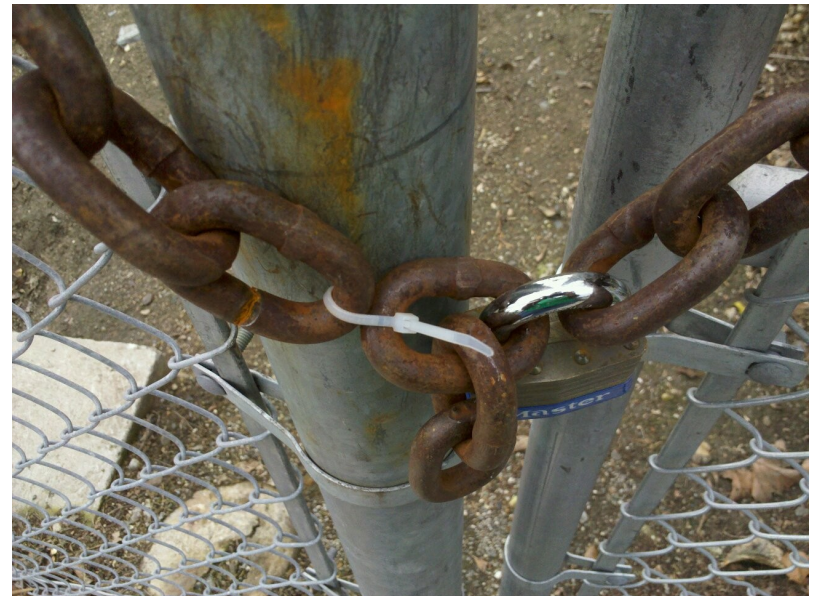
Nothing to hide?

- Information from SNSs can be misused
- Automated Social Engineering
 - Social phishing
 - Context-aware spam
 - Chatterbots
 - Cross-profile cloning
 - Friend-in-the-middle attacks
- De-anonymization
 - “On the Internet nobody knows you are a dog”
 - Face recognition

Social Engineering

Int. Secure Systems Lab
Vienna University of Technology

- Exploiting weakest link in information systems:
the people using them
- *Deception* is main tool
- Non-technical hacking
- Nowadays often in combination with technology e.g. baiting

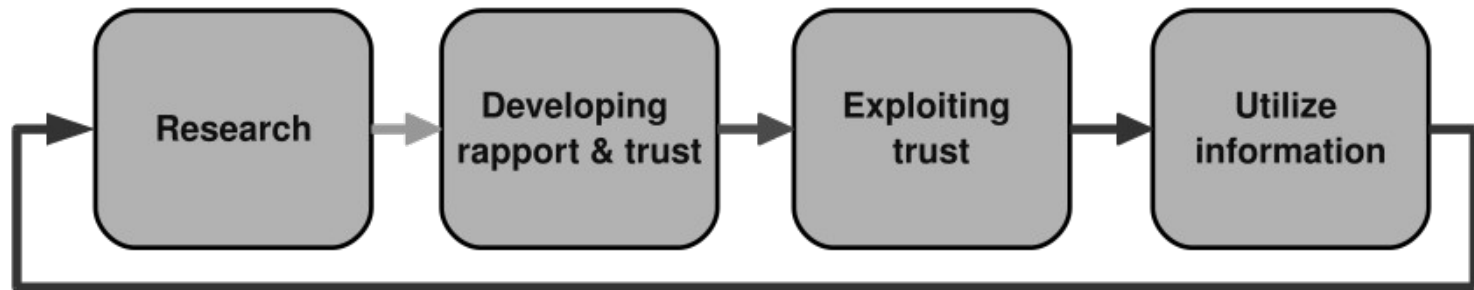


Spot the weakest link ;-)

Social Engineering Cycle by Mitnick

*Int. Secure Systems Lab
Vienna University of Technology*

- Research
 - Dumpster diving, phone calls
- Developing rapport and trust
 - E.g. authority, referring to supervisor
- Exploiting trust
 - Ask for credentials, favors etc.
- Utilize information
 - Use credentials to penetrate the system, ...



Example for Social Engineering

*Int. Secure Systems Lab
Vienna University of Technology*

Social engineering scene from Hackers

Social engineering scene from Hackers

*Int. Secure Systems Lab
Vienna University of Technology*



http://www.youtube.com/watch?v=_G3NT91AWUE

Social Engineering + Social Networking Sites = Automated Social Engineering

Int. Secure Systems Lab
Vienna University of Technology

- Traditional Social Engineering
 - Effective but costly (time, resources, etc.)
- Automated Social Engineering
 - Initial background information from social networks
 - Automate social engineering = cheap, effective attack

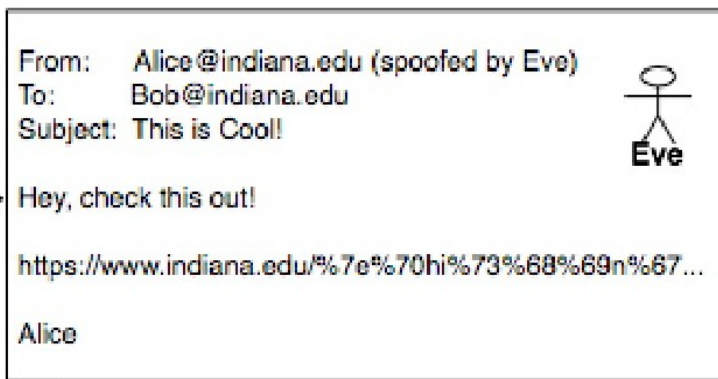
Savage Chickens

by Doug Savage



Social Phishing

- Phishing
 - Steal login information via fake websites
 - Online banking, ebay, university accounts, etc.
 - Quite ineffective
- Social phishing (Jagatic et al.)
 - 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

Int. Secure Systems Lab
Vienna University of Technology



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>

Photo sharing invitation [3]

Birthday card [3]

Automated Social Engineering

Int. Secure Systems Lab
Vienna University of Technology

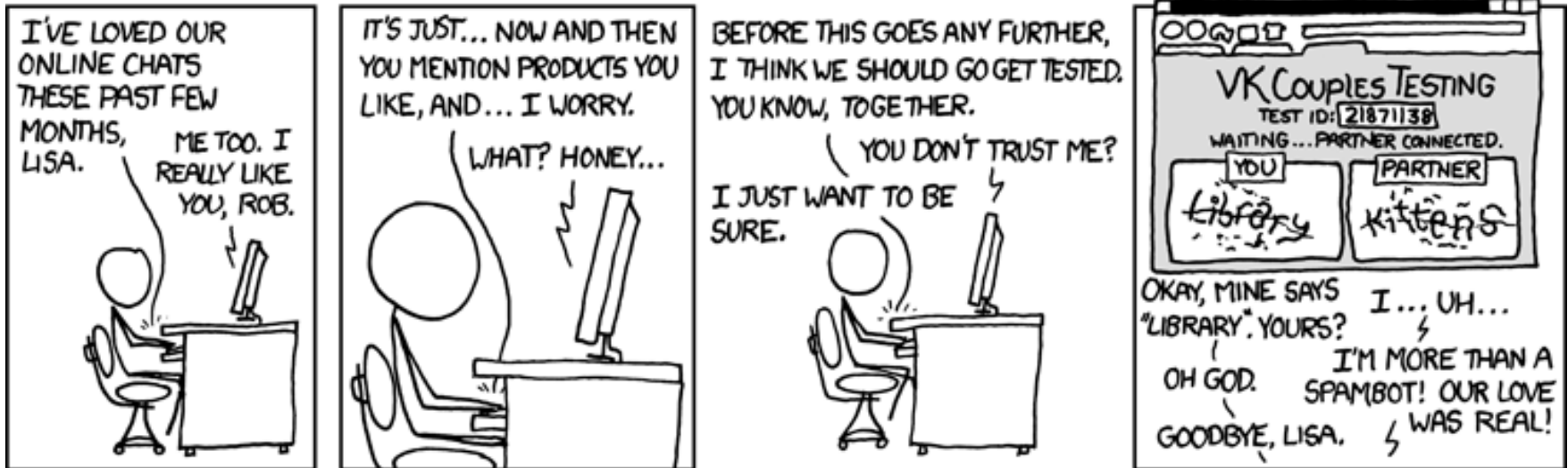
Initial challenge: **Access to private information**

- *Three case studies*
 - Chatterbots (Facebook's weak privacy defaults)
 - Cross profile cloning (limited information required)
 - Friend-in-the-middle attacks (transport layer security)

Automated Social Engineering Chatterbots

Int. Secure Systems Lab
Vienna University of Technology

- Use chatterbots to social engineer employees
- Initial search for targets on Facebook
- E.g. Chatterbot pretends to be female and looks for male singles



<http://xkcd.com/632/> XKCD suspicion

Chatterbots

*Int. Secure Systems Lab
Vienna University of Technology*

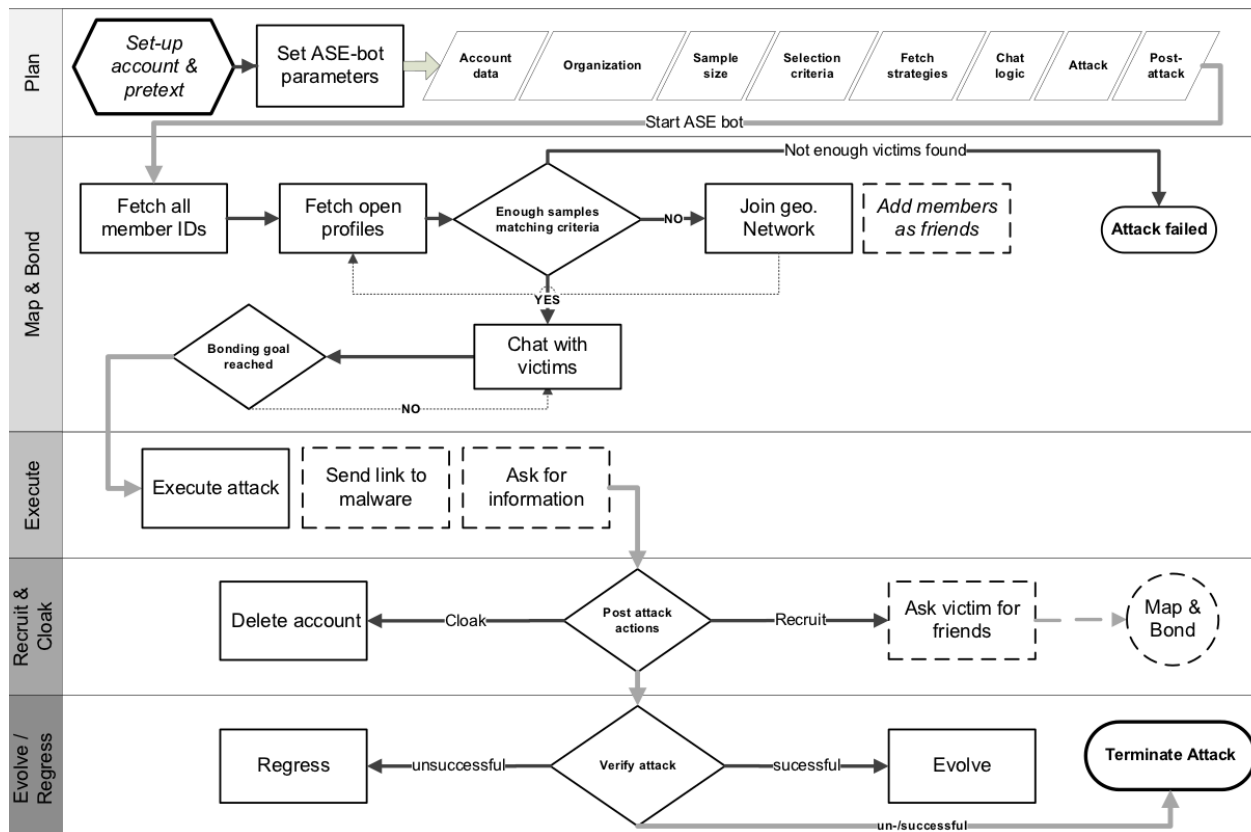
“Towards automating social engineering using social networking sites.”

Computational Science and Engineering, IEEE International Conference on, 3:117–124, 2009

- Automated social engineering with chatterbots
- Proof-of-concept implementation in Python with PyAIML
- Twofold experiment
 - Searching possible targets of five Swedish multinationals
 - Chatting in SNSs: A Turing test with the ASE bot
 - Turing’s imitation game
 - Probability / number of replies

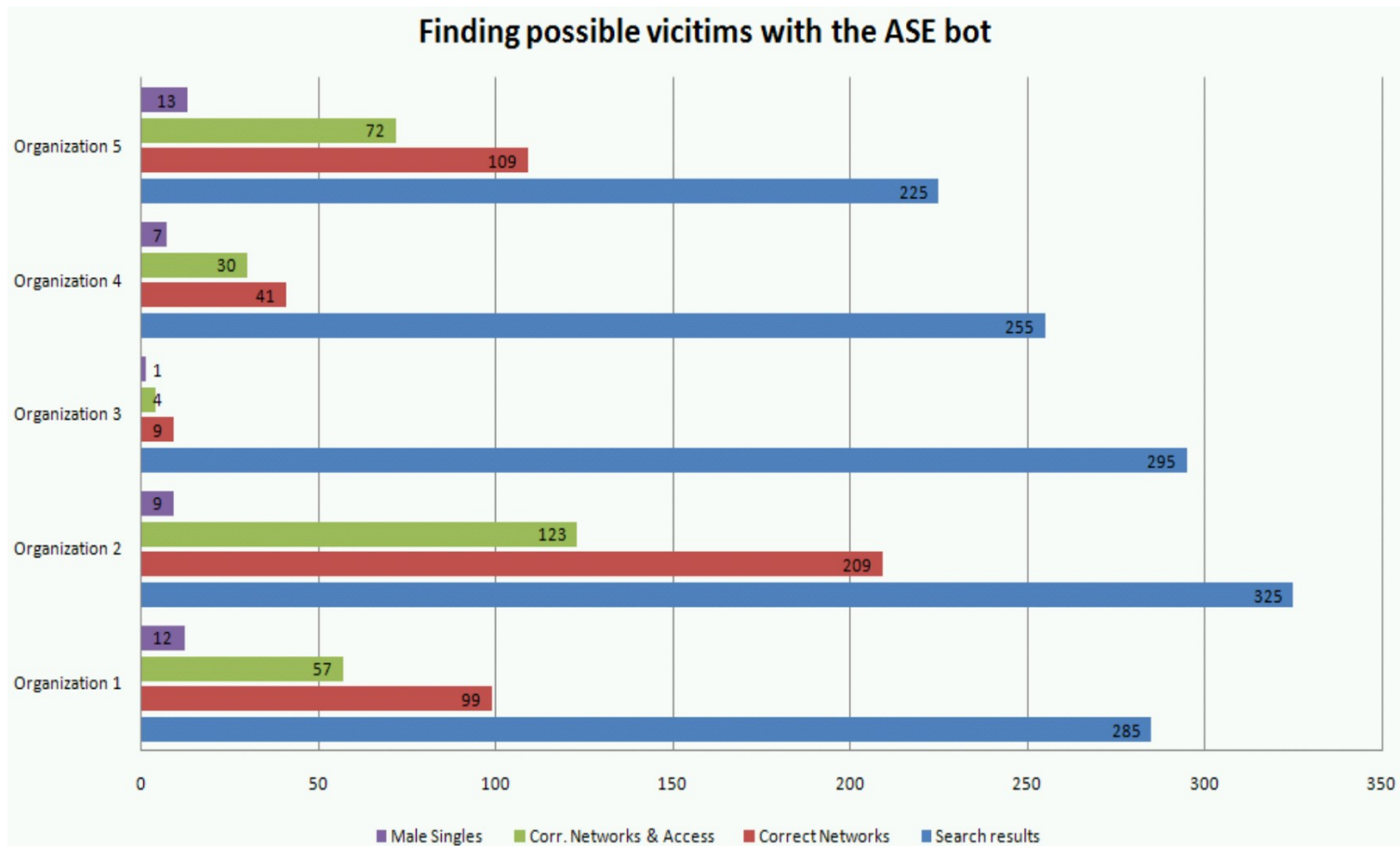
Chatterbot Attack Cycle

ASE bot – Attack cycle



Chatterbot: Finding targets

Int. Secure Systems Lab
Vienna University of Technology



Chatterbot: Turing Test

*Int. Secure Systems Lab
Vienna University of Technology*

- Results: Control group “Julian”
 - On average “Julian” rated 3.27 per cent artificial
 - Typing errors influenced outcome
- Results: ASE bot “Anna”
 - On average “Anna” 85.1 per cent artificial
 - Five test subjects rated “Anna” 100 per cent artificial after three replies
 - Expected trend with three test persons

Cross-profile cloning

*Int. Secure Systems Lab
Vienna University of Technology*

Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda, All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks, 18th International World Wide Web Conference (WWW 2009), Madrid, April 2009

- automated crawling and identity theft attack
- automatically create a forged profile in a network where the victim is not registered yet and contact the victim's friends who are registered on both networks

Cross-profile cloning: iCloner

Int. Secure Systems Lab
Vienna University of Technology

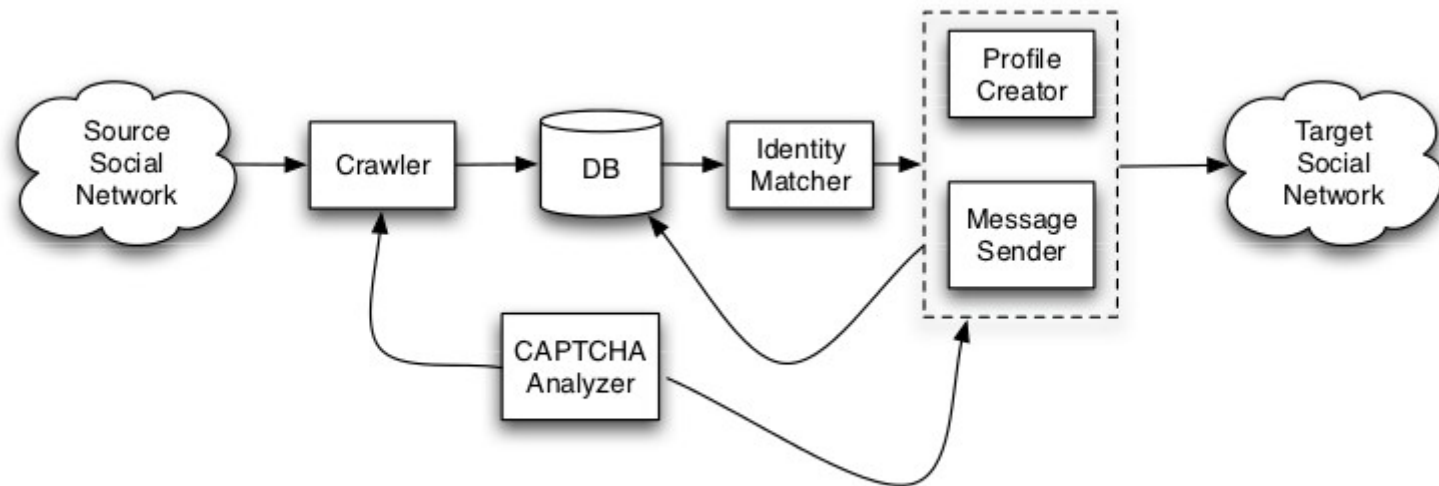


Figure 1: An architectural overview of iCloner

Cross-profile cloning: identical users

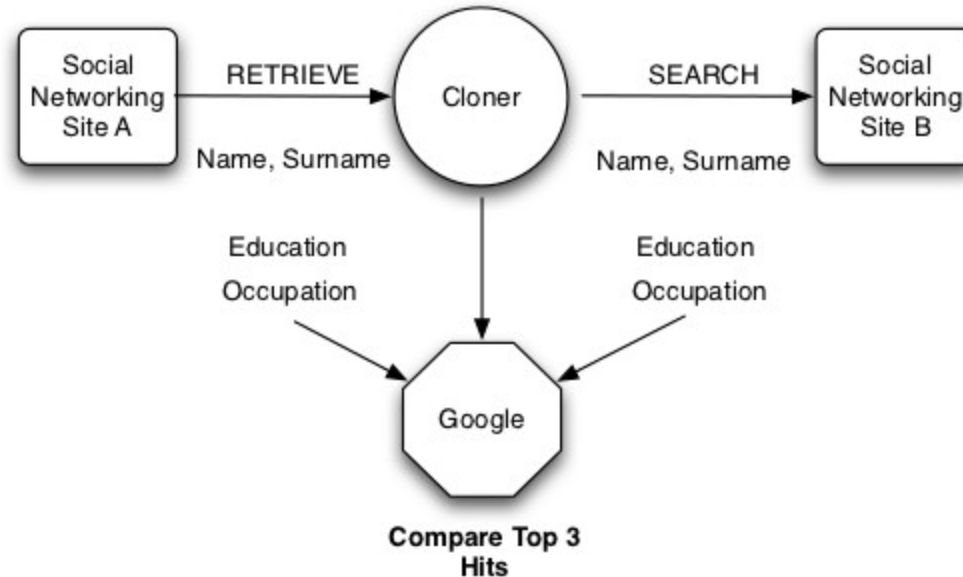


Figure 2: Process used to identify an identical user on two different social networking sites

Cross-profile cloning: results

*Int. Secure Systems Lab
Vienna University of Technology*

- Account cloning
 - 5 Facebook user cloned
 - Contact friends with forged profile
 - Over 60% accepted requests from forged profiles
- Cross-profile cloning
 - Consent of 5 XING users to clone their accounts to LinkedIn
 - iCloner identified that 78 out of their 443 XING friend contacts were also registered on LinkedIn and sent contact requests
 - 56%, in total 44, were accepted

Friend-in-the-middle (FiTM) Attacks

*Int. Secure Systems Lab
Vienna University of Technology*

M. Huber, M. Mulazzani, E. Weippl, G. Kitzler, and S. Goluch. Friend-in-the-middle attacks: Exploiting social networking sites for spam. IEEE Internet Computing: Special Issue on Security and Privacy in Social Networks, 2011

- Temporarily hijack social networking session and extract account data
- Exploit hijacked account data for large-scale context-aware spam campaign
- Estimate impact with simulation

FiTM attacks: session hijacking

*Int. Secure Systems Lab
Vienna University of Technology*

- In 2009 we found that unencrypted social networking sessions are observable virtually everywhere
- Missing HTTPS support means social networking sessions can be easily hijacked by cloning the authentication cookie
- Firesheep in October 2010, extension for Firefox
 - First proof-of-concept script kiddie tool
- Faceniff in June 2011, Android app for Smartphones
 - Support for WPA2 PSK, WEP, etc.
 - Easy to use man-in-the-middle tool

Session hijacking: Uni WiFi

- First experiments Jan. 2010 at university library

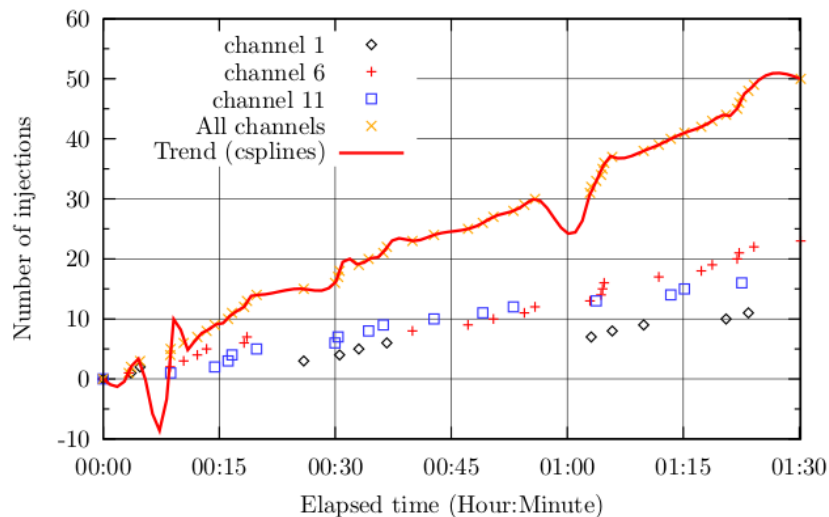


Figure: Injections during WLAN peak-time (1.5 hours)

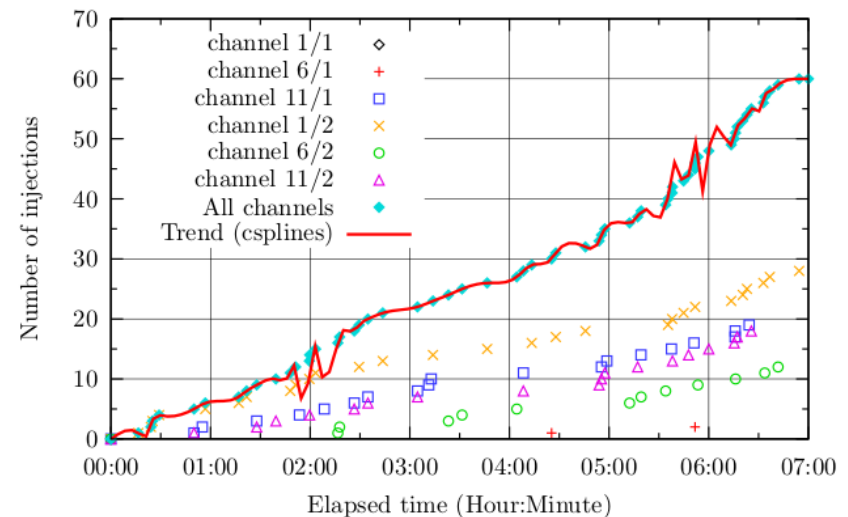


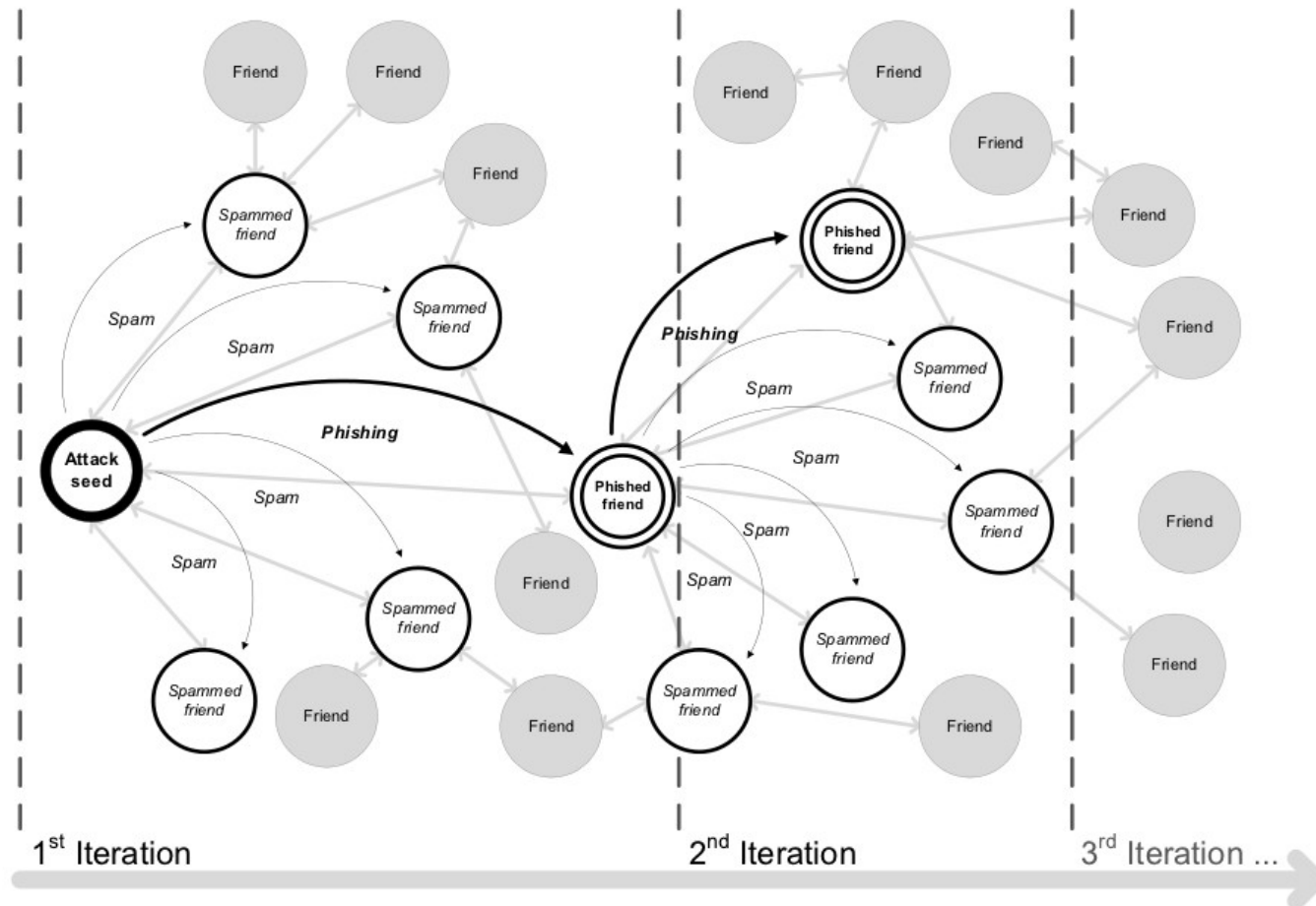
Figure: Injections during average WLAN usage (7 hours)

FiTM attacks

- **Attack outline**

- 1) An attacker uses a security hole to extract information of a SNS user. In the case study: session hijacking with injected third-party app.
- 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))

FiTM attack outline



Estimate impact of FiTM attacks

*Int. Secure Systems Lab
Vienna University of Technology*

- 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
 - Anonymous regional network collected by Wilson et al.
 - Estimate the impact

FiTM attacks: Finding attack seeds

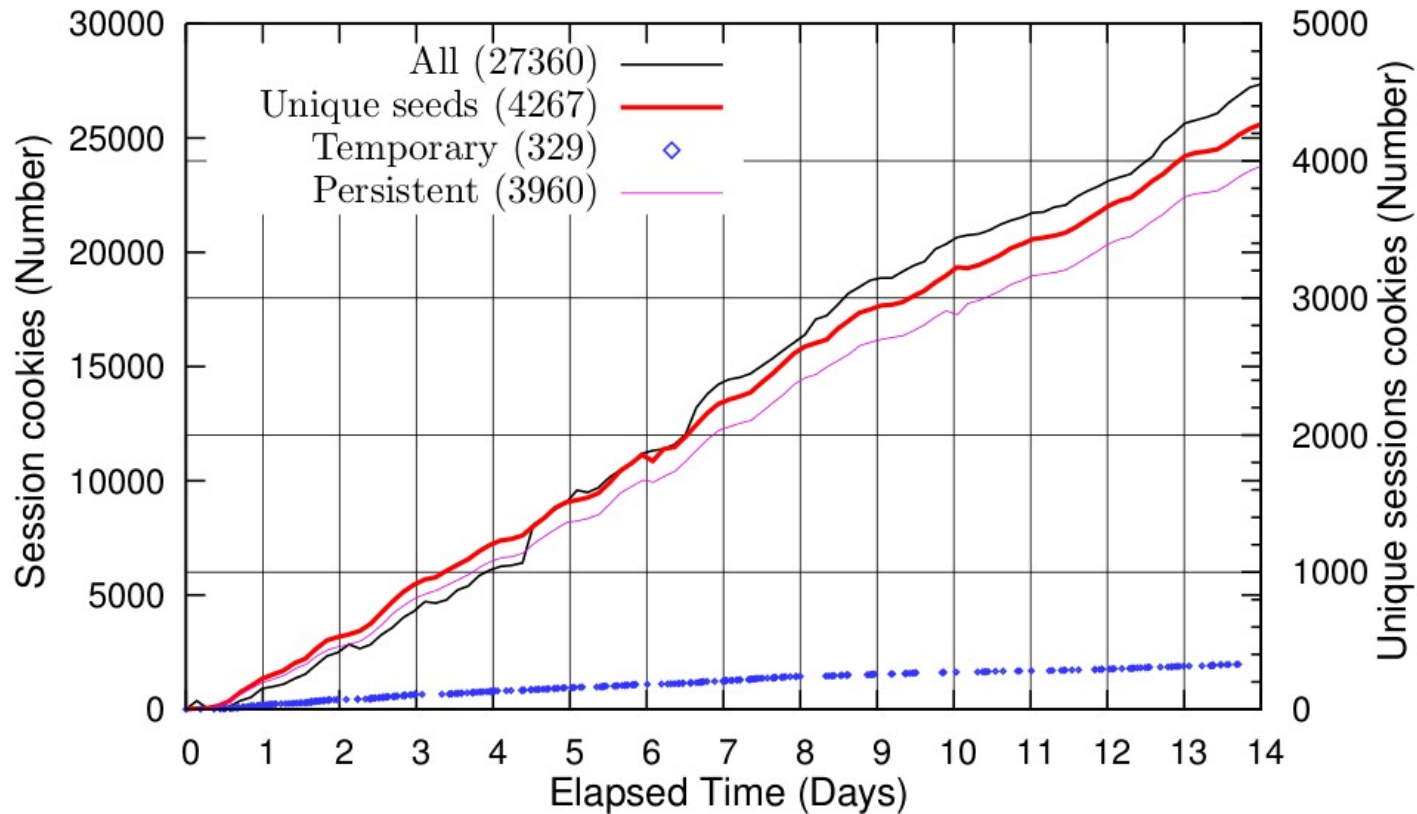


Figure: Number of sessions found through Tor exit node (14 days)

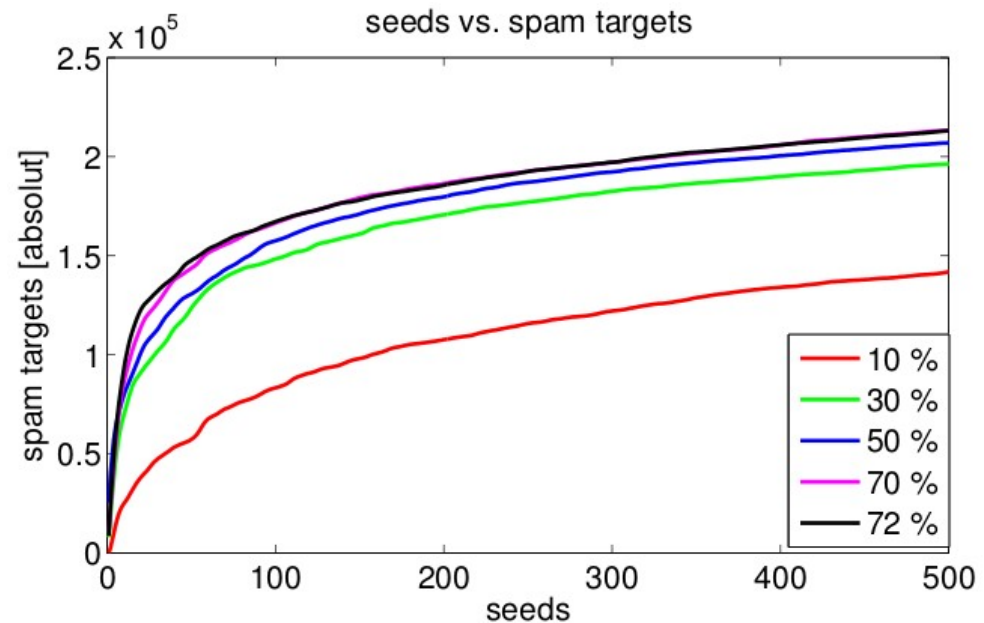
FiTM attacks: simulation

seeds	seeds [%]	targets	targets [%]
250	0.01	$1.94 \cdot 10^5$	6.28
450	0.01	$2.12 \cdot 10^5$	6.86
750	0.02	$2.27 \cdot 10^5$	7.35
1000	0.03	$2.40 \cdot 10^5$	7.77
1500	0.05	$2.58 \cdot 10^5$	8.35
2000	0.06	$2.70 \cdot 10^5$	8.74
3000	0.10	$2.90 \cdot 10^5$	9.39
4000	0.13	$3.03 \cdot 10^5$	9.80

- Simulation with two iterations and phishing success probability of 72%.
- 4000 attack seeds result in over 300.000 spammed users.

FiTM attacks: phishing success

- Phishing success rate's influence on overall spammed users.



Counter Session Hijacking Attacks

*Int. Secure Systems Lab
Vienna University of Technology*

- On the user-side
 - Usage of VPN tunnel, secure WiFi (WPA2 Radius), etc.
 - Browser extensions like EFF HTTPS everywhere
- On the provider-side
 - Full SSL/TLS support (e.g. XING)
 - Enable HTTPS per default

De-anonymization attacks

Int. Secure Systems Lab
Vienna University of Technology



"On the Internet, nobody knows you're a dog."

- A Practical Attack to De-Anonymize Social Network Users
- Faces of Facebook

Exploiting browser history

*Int. Secure Systems Lab
Vienna University of Technology*

Gilbert Wondracek, Thorsten Holz, Engin Kirda, Christopher Kruegel, A Practical Attack to De-Anonymize Social Network Users, IEEE Security and Privacy, Oakland, May 2010

- Based on well-known web browser history stealing attacks
- Malicious web sites can identify visitors
- Based on group memberships of social networking users

Browser history stealing

- Websites can query web browser if specific URLs have been visited
 - <http://ha.ckers.org/blog/>
 - <http://login.yahoo.com/>
 - <http://mail.google.com/>
 - <http://mail.yahoo.com/>
 - <http://my.yahoo.com/>
 - <http://sla.ckers.org/forum/>
 - <http://slashdot.org/>
 - <http://www.amazon.com/>
 - <http://www.aol.com/>

Query browser for social network profile URLs

*Int. Secure Systems Lab
Vienna University of Technology*

- If a website gets a positive result for a given social network profile URL query → user is identified

e.g. <http://www.facebook.com/profile.php?id=123456789>

- Facebook has currently over 600 Million members
 - It is unfeasible to query the browser for the complete set of profile URLs
 - Their experiments showed that around 90.000 queries can be performed in less than one minute
 - How to identify users?

Limiting query set via social networking groups

*Int. Secure Systems Lab
Vienna University of Technology*

- All major social networking services offer groups
- Twofold approach
 - Crawl profile IDs that exist in public groups
 - Use group memberships to limit set of profile URLs to query
 - Query group URLs first
 - Compile set of users that are in specific groups
 - Query user URLs for correct one

Social networking groups example

- Search for social networking groups results in:
 - Game Boy, Hidden Kitchen, Already Architecture., Kann dieser seelenlose Ziegelstein mehr Freunde haben als H.C. Strache?, I don't sleep enough because I stay up late for no reason, TEMPO!, Die peinlichsten und lustigsten FB Status Einträge & Fotos, Gin Tonic, Armin Wolf, Wooster Collective, Mc Gyver, Woody Allen, Louis de Funès
 - A search in the crawled data shows that 120 Facebook users have exactly these 13 groups
 - A query for the 120 Facebook users results in a single profile URL → user identified

Practical evaluation of history stealing de-anonymization

*Int. Secure Systems Lab
Vienna University of Technology*

- isecLAB online demo web-site for XING
 - Worked pretty well
 - Featured on heise.de
 - <http://www.heise.de/security/meldung/Plaudertasche-Web-Browser-erleichtert-Deanonymisierung-919076.html>
- XING fixed the issue by introducing random characters into profile URLs

Faces of Facebook

*Int. Secure Systems Lab
Vienna University of Technology*

Black Hat USA 2011 //briefings

Caesars Palace Las Vegas, NV • August 3 - August 4

Alessandro Acquisti, Faces Of Facebook - Or, How The Largest Real ID Database In The World Came To Be

- Crawled public available information from university students including photos
- Can state-of-the-art face recognition technology be used to identify people?
- Take a snapshot of a random person on campus, can you get the Facebook information to the person?
- Can users be re-identified across multiple web sites?
 - People give real name on Facebook and pseudonyms on dating sites, but pictures show the same person

Primarily results

*Int. Secure Systems Lab
Vienna University of Technology*

- User identification with 106 subjects
 - Unclustered matches:
 - Correctly recognized: 32 **(30%)**
 - Clustered matches
 - Correctly recognized: 45 **(42%)**
- Facebook.com and match.com
 - A number of users have been re-identified

A scene from minority report

*Int. Secure Systems Lab
Vienna University of Technology*

As of June 7th 2011 (yesterday), Facebook introduced face recognition.

- Opt-out of this feature!

Did the movie “minority report” see it coming? :-)

Facebook as an ID provider for face recognition?

Scene from minority report

*Int. Secure Systems Lab
Vienna University of Technology*



<http://www.youtube.com/watch?v=oBaiKsYUdvg>

Recent examples involving (automated) social engineering

Int. Secure Systems Lab
Vienna University of Technology

- Getting in bed with Robin Sage
 - Fake profiles on Facebook, LinkedIn, Twitter ...
 - “25-year-old cyber threat analyst at the Naval Network Warfare Command in Norfolk, Virginia.”
 - Befriended personal of US military/government
 - Collected personal and confidential information
- RSA SecureID hack
 - RSA SecureID authentication token compromised **“Robin Sage”**
 - Small group of employees targeted via Email
 - ‘2011 Recruitment plan.xls’ attachment
 - 40 million SecureID tokens have to be replaced



Conclusion

- Socio-technical attacks pose serious threat
 - Social engineering is an effective attack ...
 - in combination with technology also cheap
 - Social networking sites are attractive targets
 - Provider need to protect personal data
- The end of privacy
 - On the Internet everyone knows you are a dog
 - Holistic approaches needed to protect privacy
 - Legal, educational, technical ...

Questions?

*Int. Secure Systems Lab
Vienna University of Technology*

You can contact me at:
mhuber@sba-research.org

Get in touch for possible master and bachelor theses in security and privacy :-)