Course Program

Wednesday, June 23:
• 09:30-10:30 Introduction, Claudia Diaz
• 11:00-12:30 Overview of Privacy Enhancing Technologies, Claudia Diaz
• 14:00-15:30 Exploring European data protection: From social networks to cookies, Eleni Kosta
• 16:00-17:30 Privacy and Web mining, Bettina Berendt

Thursday, June 24
• 09:00-10:30 To share or not to share - a user's perspective on privacy in social networks, David Geerts
• 11:00-12:30 Privacy Concerns and Information Disclosure: An Illusion of Control Hypothesis, Alessandro Acquisti
• 14:00-15:30 Privacy, Requirements Engineering and Online Social Network Services, Seda Gürses
• 16:00-17:30 Predicting Social Security Numbers From Public Data, Alessandro Acquisti
• 17:30 Discussion speakers and participants
Introduction

Claudia Diaz
K.U.Leuven ESAT/COSIC
Outline

- The Privacy debate
- Example applications with implications for privacy
- Defining privacy
- Privacy models
Caricature of the debate: Security or Privacy

- “Privacy” important but...
  - ...what about abuse and accountability?
  - ...difficulties for Law Enforcement?
  - ...copyright or libel
  - ...what does a good, honest person have to hide anyway?

- Established wisdom:
  - Need for a balance...
  - Control/limit “dangerous” technology (or research).
  - Result: Surveillance by design → no privacy (often).
“I have nothing to hide”

“I don’t care about surveillance because I have nothing to hide”

“If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.” – Eric Schmidt, Google’s CEO
Daniel Solove


“The problem with the ‘nothing to hide’ argument is its underlying assumption that privacy is about hiding bad things.”

“Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocation.”
Taking privacy to create security

Is there a tradeoff between privacy and security?

Source: http://www.myconfinedspace.com/
“Balancing” Privacy with Security

- “Surveillance is good and privacy is bad for national security. We need a tradeoff between privacy and security”
- Law enforcement keywords to justify more surveillance: terrorism, child pornography, money laundering, crime...
- Public opinion pressure on politicians fuelled by high-impact crimes
  - Making legislation as a response to concrete cases
- “We need more surveillance” is a powerful argument
  - If attacks increase, you can argue that you need even more
  - If attacks decrease, you take credit
Surveillance = Security?

- **Not effective**
  - Indiscriminate instead of targeted (old times)
  - Shift of resources to electronic surveillance
  - High rates of false positives (e.g., no-fly lists, wrong people sent to detention centers)
  - Smart adversaries evade surveillance
    - Knowing the position of cameras to hide your face (CCTV not deterring crime)
    - Adapting behavioral patterns to remain undetected (financial transactions, mobile phone usage, etc.)
  - Vicious circle: all we need is *more* surveillance!

- **Function creep**: where do we stop?
  - Once the capability is in place, why to use it to do *more*?
Surveillance = Security?

- Risk of **abuse**: lack of transparency and safeguards

- Information asymmetries $\rightarrow$ power asymmetries
  - Those with information resources even more at an advantage (checks and balances?)
  - Made worse by the fact that you do not know what they know about you

- Organizations are very keen on protecting their own secrets
  - How they create and use profiles

- Corruption of
  - Organizations themselves: Use against political opponents
  - Certain individuals within those organizations: Financial gain
Surveillance = Security?

- Risk of subversion for crime/terrorism
  - Example: Greek Vodafone scandal (2006): “someone” used the legal interception functionalities (backdoors) to monitor 106 key people: Greek PM, ministers, senior military, diplomats, journalists...
  - [Diffie and Landau] “Communication is fundamental to our species; private communication is fundamental to both our national security and our democracy.”
Privacy = Security Property

- Governments / Military
  - Protection of national secrets, confidentiality of law enforcement investigations, diplomatic activities, political negotiations

- Companies
  - Protection of trade secrets, business strategy, internal operations, access to patents

- Individuals
  - Freedom from intrusion, profiling and manipulation, protection against crime / identity theft, flexibility to access and use content and services, control over one’s information

- Shared infrastructure
  - Despite varying capabilities infrastructure is shared
  - Telecommunications, operating systems, search engines, on-line shops, software, . . .
  - Denying security to some, means denying it to all
Privacy no longer a social norm, says Facebook founder

Bobbie Johnson, Las Vegas
guardian.co.uk, Monday 11 January 2010 01.58 GMT
Article history

People have become more comfortable sharing private information online, says Facebook founder Mark Zuckerberg. Photograph: Eric Risberg/AP

The rise of social networking online means that people no longer have an expectation of privacy, according to Facebook founder Mark Zuckerberg.

Talking at the Crunchie awards in San Francisco this weekend, the 25-year-old chief executive of the world's most popular social network said that privacy was no longer a "social norm".

"People have really gotten comfortable not only sharing more information and different kinds, but more open for everyone to know people," he said. "That social norm is just something that has evolved over time."
People don’t care about privacy (?)

In the offline world, people want to control information
- What we tell to whom
- Impression management / self-presentation
- Concerns over information taken out of context: privacy as contextual integrity (Nissenbaum)
- Personal safety
Still adapting to the information era?

- The cost of gathering and analyzing information without advanced technologies has guaranteed that we had a rather high level of privacy protection.

- What will be the new equilibrium?
Some example applications with implications for privacy
How many ways have you been located today?

- cell phone (turned on?)
- laptop computer
- credit card at the gas station
- bank card in the ATM machine
- driving through a monitored intersection
- security camera at the supermarket
- scan badge to enter a building
- pass a Bluetooth-enabled printer
“Chattering” devices

- RFID
- Bluetooth/Zigbee
- WLAN
- WiMAX
- 2G/GSM
- 3GSM
- GPS/Glonass/Galileo
Location Based Services

- Location-based traffic monitoring and emergency services
  - e-Call, traffic congestion control
  - Pay-as-you-drive
- Location finder:
  - Where is the nearest restaurant, gas station,...
- Social applications
  - Geotagged Twitter
  - Google Latitude
- Ubiquitous environments

Gartner Revenue of LBS:
- 2008: 998.3 M$
- 2009: 2.2 B$
Why is this a problem?

- Do you want to be seen at certain locations?
  - Abortion clinic, AIDS clinic, business competitor, or political headquarters (Google Street View)

- What can be automatically inferred about a person based on location?
  - Child: at school location during school hours
  - Home and work address
  - Movement routines, changes in routine

- Personal safety (e.g., stalking, child abduction)

- Spionage (high government officials, journalists, CEOs, military...)
Social networks

- What information about you is currently available in social networks?
  - Do you *actually* know?
  - To whom is it available?
  - If you want to delete, can you be assured that it will no longer be available?

- How much of that information was published by other people other than you?
Identity theft

BBC NEWS

Personal data privacy 'at risk'

Millions of people are leaving themselves open to identity theft when using social networking websites, according to the consumer group Which?

Members of sites such as Facebook can join large networks which reveal personal information to thousands of others on the network.

Which? says people are at a greater risk of being targeted by fraudsters than they think.

On average, UK residents' details are held on about 700 databases.

Which? says that fraudsters can use the internet to gather personal information which could then be used to trick people into revealing PIN numbers and other security information.

These could then be used by conmen to apply for credit cards or loans in somebody else's name.

Burglars could also benefit from such information, it says.

CONSUMER RIGHTS

LATEST NEWS

• Christmas shoppers 'undeterred'
• Shoppers' nights 'under threat'
• Cheaper toys 'are Christmas hits'
• Personal data of 51,000 is lost
• Phone tariffs 'too bewildering'

ANALYSIS AND GUIDES

• Do legal messages make a difference?
• Five useful consumer laws
• Payment fraud: Your rights?
• 'It sounded convincing'
• Cybercrime threat rising sharply
• How safe are your Christmas presents?

IN PICTURES

Fake trade
Dangerous gifts found by UK trading standards officers.

RELATED INTERNET LINKS

• Which?
  The BBC is not responsible for the content of external internet sites

TOP BUSINESS STORIES

• Cadbury rejects hostile Kraft bid
• Gold hits highest level in 24 years

Claudia Diaz -- Interdisciplinary Privacy Course

June 23, 2010
Spear phishing

Spear-Phishing:
Social Networks open to harvesting

In a recent article, I outlined the problems with increased breaches of security on sites as huge as MySpace and Facebook, not to mention sites that are supposed to be geared specifically towards businesses. While there is still a digital DMZ around most enterprise, those who would compromise your users and security are going after these so-called soft targets with a new twist on the old social engineering methods to extract information and gain access to your resources. Here is what you should know about this latest ploy!

Social Engineering
Social engineering is nothing new. It has been around since before there were PCs. An individual talks their way into an office, claiming to be there to solve a problem from someone, working on the phones, picking up a file, etc. Social engineering is alive and well and remains the most effective hacking technique according to Aaron Higbee, a managing partner and co-founder of the Intrepidus Group. Its use assists in proliferation of malware, spam, mass phishing, botnets and even more advanced hacking techniques.

Today's social engineering threats have progressed beyond the scope of infamous hacker Kevin Mitnick, who earned his reputation and subsequent jail time by using his ability to find soft targets within an organization and schmoozing them into providing information that would allow him access to their systems and network. Now out, Kevin Mitnick runs Mitnick Security Consulting LLC, a computer security consultancy firm.

Spear-Phishing?
Ok, so you have heard of Phishing, the electronic equivalent of throwing a hook and bait into a lake. Instead of a fish, the target of Phishing is information. So what is spear-phishing.
Information taken out of context

4/24 NEW YORK

The Officer Who Posted Too Much on MySpace

By AMYWIR
Published March 10, 2009

In pictures, Vaughan Ettienne is a champion bodybuilder of surreal musculature. In conversation, he is polite and thoughtful.

And in the looking glass of his computer screen, he becomes a man of fierce, profane views on how to keep law and order. A few weeks ago, he posted a description of his mood on a MySpace account. “Devious,” he wrote.

The next day, a man accused of carrying a loaded gun would go on trial in State Supreme Court in Brooklyn — and in large part, the case rested on the credibility of Vaughan Ettienne, bodybuilder, Internet user and arresting officer.

What seemed like a simple gun possession case became an undeclared war over reality: Was Officer Ettienne a diligent cop who found a gun after chasing an ex-convict weaving through traffic on a stolen motorcycle? Or was his story a “devious” facade in keeping with the ruthless character he revealed on social network Web sites?

“You have your Internet persona, and you have what you actually do on the street,” Officer Ettienne said on Tuesday. “What you say on the Internet is all bravado talk, like what you say in a locker room.”

Except that trash talk in locker rooms almost never winds up exposed on a digital screen somewhere, available for download. The
Stalking

Social Networking Sites: A Bonanza for Stalkers?

"Vengeance will be mine....," declared a defiant message on MySpace.com. "I should have killed you all when I had a gun and some drugs." This violent monologue, one of several postings on the writer's site, threatened his ex-wife, who had fled the state to escape his abuse. In postings on other sites, he demanded photos of his family and warned that if he didn't get to see the kids, "It isn't going to be real good, because I'm gonna see them whether you let me or not."

The increasing use of MySpace to threaten and stalk victims raises many important questions. Do social networking sites enable stalking? What recourse do victims have when these sites are used to stalk? And what tools can help block the use of these sites to stalk?

What Are Social Networking Sites?
Social networking sites such as MySpace and Facebook are virtual communities where people with mutual interests meet online to share information and build relationships. Site visitors can chat, debate, network, and socialize. On many sites, members may post details about themselves—photos; educational backgrounds; favorite books, movies, and music; and relationship status. Others sites promote business, activism, networking, counseling, socializing, or many types of recreational interests. Sites such as MySpace, Facebook, Friendster, and Xanga have attracted millions of members, particularly among teenagers and young adults.
Predators on Social Networks

Sexual Predators and Child Molesters Find Easy Prey
From Tony Bradley, CISSP ISSAP, former About.com Guide

Social networking is all the rage. Various web sites have sprung up for the sole purpose of providing a place for users to express themselves, share with like-minded individuals, discover new things, and communicate with others. Even I have a Myspace profile and a LinkedIn profile.

The concept is so popular that even the 400-pound gorilles of the Web have jumped on the bandwagon. MySpace was snatched up by Rupert Murdoch's News Corp. Google has Orkut. Yahoo tried Yahoo 360, and is now beta-testing their new social network dubbed Mash. Microsoft just bought into a large stake of Facebook.

The concept of social networking has also been extended to other areas. For example, Youtube (also picked up by Google), provides users with the ability to express their creativity, network, rate their favorite video clips, etc. Some sites like Flickr, DropShots, or PhotoBucket provide users with the ability to post and share photos and family videos.
Profiling

Using social networks for persuasion profiling

Posted by Dean Eckles in Facebook, HCI, participatory media, persuasion profiling, persuasive technology, psychology, social software, sociology, statistics

BusinessWeek has an exuberant review of current industry research and product development related to understanding social networks using data from social network sites and other online communication such as email. It includes snippets from people doing very interesting social science research, like Duncan Watts, Cameron Marlow, and danah boyd. So it is worth checking out, even if you're already familiar with the Facebook Data Team's recent public reports ("Maintained Relationships", "Gesundheit").

But I actually want to comment not on their comments, but on this section:

In an industry where the majority of ads go unclicked, even a small boost can make a big difference. One San Francisco advertising company, Rapleaf, carried out a friend-based campaign for a credit-card company that wanted to sell bank products to existing customers. Tailoring offers based on friends' responses helped lift the average click rate from 0.9% to 2.7%. Although 97.5% of the people surfed past the ads, the click rate still tripled.

Rapleaf, which has harvested data from blogs, online forums, and social networks, says it follows the network behavior of 480 million people. It furnishes friendship data to help customers fine-tune their promotions. Its studies indicate borrowers are a better bet if their friends have higher credit ratings. This might mean a home buyer with a middling credit risk score of 550 should be treated as closer to 600 if most of his or her friends are in that range, says Rapleaf CEO Auren Hoffman.

The idea is that since you are more likely to behave like your friends, their behavior can be used to profile you and tailor some marketing to be more likely to result in compliance.

In the Persuasive Technology Lab at Stanford University, BJ Fogg has long emphasized how powerful and worrying personalization based on this kind of "persuasion profile" can be. Imagine that rather than just personalizing screens based on the books you are expected to like (a familiar idea), Amazon selects the kinds of influence strategies used based on a representation of what strategies work best against you: "Dean is a sucker for limited-time offers", "Foot-in-the-door works really well against Domenico, especially when he is buying a
Inferences

Gaydar Algorithm Outs Facebook Users
By Susannah F. Locke  Posted 09.21.2006 at 12:27 pm  7 Comments

What are your friends saying about you? Online social networks like this Facebook one might reveal more about you than you think. See here. (CC licensed)

A pair of MIT students claim that they have created an algorithm that outs gay members of Facebook by analyzing the sexual orientations of their networks of friends.
Main problems

- Indeterminate visibility of information
  - Transitive access control
- Information about ourselves revealed by others
  - Information related to many
- Hard to predict potential inferences (rich profiles)
- Lack of transparency/feedback
- Usability of privacy controls
- Removing information
- Interest of SNS Providers in more info being shared
  - Also with advertising companies
Wave imaging (Airport security)

- Advantages [TSA, May 2009]:
  - Effective, fast, convenient, safe

- How privacy is addressed:
  - The system uses a **pair of security officers**
  - A passenger's **face** is blurred
  - Cameras, cell phones or **recording devices not allowed** into the room
  - The computers have been programmed so they have “**zero storage capability**”
  - Images are “**automatically deleted**”
Wave imaging (Airport security)

- What is the problem then?
  - Image quality can improve
  - Storage capability could be reactivated
  - No cameras allowed?
    - Incentives: images of celebrities?
  - Policy could be changed down the road
  - As machines get cheaper, will we see them in supermarkets or schools?
  - General concerns over human rights, personal dignity, proportional?
Smart energy

- Smart meters
  - Better use of resources
  - Send information back to provider (wired/wireless)

- Privacy issues
  - Information that can be inferred
    - At home / away
    - Rutines (e.g., sleep/eat schedule, tv, washing machine...)
    - Changes in routines (e.g., visitors)
Defining Privacy
What is privacy?

- Abstract and subjective concept, hard to define
  - Dependent on cultural issues, study discipline, stakeholder, context

- Popular definitions:
  - “The right to be let alone”
    - Focus on freedom from intrusion
  - “Informational self-determination”
    - Focus on control
  - “The freedom from unreasonable constraints on the construction of one's own identity”
    - Focus on autonomy
Solove’s taxonomy of privacy

- **Information Collection**
  - Surveillance
  - Interrogation

- **Information Processing**
  - Aggregation
  - Identification
  - Insecurity
  - Secondary Use
  - Exclusion

- **Information Dissemination**
  - Breach of Confidentiality
  - Disclosure
  - Exposure
  - Increased Accessibility
  - Blackmail
  - Appropriation
  - Distortion

- **Invasion**
  - Intrusion
  - Decisional Interference
Data protection (EU)

- Data collected for specific and legitimate **purpose**
- **Proportional**: adequate, relevant and not excessive (data minimization)
- With the subject’s awareness and **consent**
  - Unless data is necessary for...
- Data subject’s right to access, correct, delete her data
- Data security: integrity, confidentiality of the data
Technical privacy properties

- Anonymity
- Pseudonymity
- Unlinkability
- Unobservability
- Plausible deniability
- Location privacy
- Censorship resistance
- ...
Can we “measure” privacy?

- Need to specify
  - Privacy properties we want to achieve (e.g., anonymity)
  - Details of the system (the Devil is in the details!)
  - Adversary model: goals and capabilities

- Typically, adversaries are able to obtain probabilistic information. Examples:
  - Probability of a person being the anonymous subject we want to identify (limited number of people in the world)
  - Probability of two information items being related to each other (e.g., two web page requests coming from the same user)

- Various proposals for privacy metrics (e.g., entropy)
Privacy models: soft and hard privacy
“Trust-based” or “Soft” privacy

- **System model**
  - Data subject provides her data
  - Data controller responsible for its protection

- **Threat model**
  - External parties, errors, malicious insider
Soft privacy

- Controller: main security “user”
- Policies, access control, trust, audits (liability)
- Goal (data protection): purpose, consent, data security
Soft privacy

- Data subject has already lost control of her data
- In practice, very difficult for data subject to verify how her data is collected and processed
Soft privacy

- Data subject has already lost control of her data
- In practice, very difficult for data subject to verify how her data is collected and processed
- Need to trust data controllers (honesty, competence) and hope for the best
- Weak enforcement, low penalties

TRUST ASSUMPTIONS?

INCENTIVES?

TECHNOLOGICALLY ENFORCED?
Darling admits Revenue loss of 25 million personal records
Lost: Two discs, 25 million accounts

By John Oates • Get more from this author

Posted in Government, 20th November 2007 16:22 GMT
Free whitepaper – The human factor in laptop encryption

UK Identity Crisis Alistair Darling told the House of Commons this afternoon that a police investigation has been launched into how Her Majesty’s Revenue and Customs has lost child benefit records relating to 25 million people.

Records for 25 million people, relating to child benefit payments for 7.25 million families, were sent using the HMRC’s own postal system, called grid, but never arrived.
Clarkson stung after bank prank

TV presenter Jeremy Clarkson has lost money after publishing his bank details in his newspaper column.

The Top Gear host revealed his account numbers after publishing the furore over the loss of 25 million people's personal details on two computer discs.

He wanted to prove the story was a fuss about nothing.

But Clarkson admitted he was "wrong" after he discovered a reader had used the details to create a £500 direct debit to the charity Diabetes UK.

Clarkson published details of his Barclays account in the Sun newspaper, including his account number and sort code. He even told people how to find out his address.

"All you'll be able to do with them is put money into my account. Not take it out. Honestly, I've never known such a palaver about nothing," he told readers.

"I was wrong and I have been punished"

Jeremy Clarkson

SEE ALSO
- Clarkson quizzed over gang ordeal
  06 Dec 07 | England
- More firms 'admit disc failings'
  04 Dec 07 | UK Politics
- Brown apologises for records loss
  21 Nov 07 | UK Politics

RELATED BBC LINKS
- Top Gear

RELATED INTERNET LINKS
- Diabetes UK
- Jeremy Clarkson

The BBC is not responsible for the content of external internet sites

TOP ENTERTAINMENT STORIES
- Rowling arrives for Potter case
- Star Wars' Baker 'a lot better'
- TV host Speight was found hanged

MOST POPULAR STORIES NOW
- TV host Speight was found hanged
- Day in pictures
- Lonely Planet rebuts 'fake' claim

Claudia Diaz -- Interdisciplinary Privacy Course
Facebook CEO Mark Zuckerberg and his company are suddenly facing a big new round of scrutiny and criticism about their cavalier attitude toward user privacy.

An early instant messenger exchange Mark had with a college friend won't help put these concerns to rest.

According to SAI sources, the following exchange is between a 19-year-old Mark Zuckerberg and a friend shortly after Mark launched The Facebook in his dorm room:

**Zuck:** Yeah so if you ever need info about anyone at Harvard

**Zuck:** Just ask.

**Zuck:** I have over 4,000 emails, pictures, addresses, SNS

[Redacted Friend's Name]: What? How'd you manage that one?

**Zuck:** People just submitted it.

**Zuck:** I don't know why.

**Zuck:** They "trust me"

**Zuck:** Dumb fucks.

Brutal.
Hard privacy

- System model
  - Subject provides as little data as possible

- Reduce as much as possible the need to “trust” other entities

- Threat model
  - Adversarial environment: communication provider, data holder
  - Strategic adversary with certain resources motivated to breach privacy (similar to security systems)
Hard privacy

- Subject is an active security “user”
- Goal (data protection): data minimization
- Goal (Solove): protect against surveillance, interrogation, aggregation, identification
- Next talk: overview of (hard) Privacy Enhancing Technologies
Conclusions

- Open debate, unclear how it will evolve
- Increasing number of applications with implications for privacy: which will be the long-term effects?
- Privacy is not “opposed” to security, but rather a security property
- You should care about privacy
- Soft and hard privacy: two privacy paradigms