Journal of Information Technology Education: Innovations in Practice Volume 15, 2016

Cite as: Peltsverger, S., & Zheng, G. (2016). Enhancing privacy education with a technical emphasis in IT curriculum. *Journal of Information Technology Education: Innovations in Practice, 15,* 1-17. Retrieved from http://www.jite.org/documents/Vol15/JITEv15IIPp001-017Peltsverger1873.pdf

Enhancing Privacy Education with a Technical Emphasis in IT Curriculum

Svetlana Peltsverger and Guangzhi Zheng
Kennesaw State University, Marietta, GA, USA

speltsve@kennesaw.edu; gzheng@kennesaw.edu

Abstract

The paper describes the development of four learning modules that focus on technical details of how a person's privacy might be compromised in real-world scenarios. The paper shows how students benefited from the addition of hands-on learning experiences of privacy and data protection to the existing information technology courses. These learning modules raised students' awareness of potential breaches of privacy as a user as well as a developer. The demonstration of a privacy breach in action helped students to design, configure, and implement technical solutions to prevent privacy violations. The assessment results demonstrate the strength of the technical approach.

Keywords: Privacy, Education, Curriculum, Information Security, Information Assurance

Introduction

Computing curriculum in many universities include courses that teach students how to develop secure software and use the best practices for system configuration. In many of these programs, the focus of the education is on confidentiality. However, confidentiality does not guarantee privacy. Protecting privacy has become a widely recognized priority for both businesses and government agencies ("Consumer data privacy in a networked world," 2012). In the European Union, the PRIPARE project (PReparing Industry to Privacy-by-design by supporting its Application in Research) was started in 2013 to identify gaps and provide recommendations on privacy and security-by-design practices (Roda et al., 2014). Computing professionals must consider privacy issues as they design and manage information systems that protect information from misuse.

To help students have better understanding of privacy issues, the authors proposed a conceptual framework (Peltsverger & Zheng, 2012) to enhance privacy education and curriculum. The framework particularly addresses the technical aspects of privacy education. Guided by the framework, this paper describes the design of four sample learning modules that all include hands-on labs to teach the technical details of privacy. The purpose of these technical labs is to demonstrate what happens "behind the scene" when users interact with information systems. They not only demonstrate how to protect customers' privacy and write privacy policies, but also how to develop technical/automatic procedures for their enforcement. These modules have been incorporated into current courses and tested by students.

Editor: Lynn Jeffrey
Submitted: March 30, 2015; Revised: July 21, September 11, November 16 & 18;
Accepted: December 13, 2015

The next section provides a general view on issues of privacy, followed by the brief summary of the privacy curriculum framework. After describing the module design and four developed modules, student feedback from surveys is presented and discussed.

Privacy in IT Curriculum

The attack surface on privacy started to expand in mid-1990s when the Internet introduced a nearly instantaneous way to access data via web browsers, emails and later instant messages, forums, blogs, social networks, e-commerce sites, global positioning systems, etc. People expose their personal information when they use computers, smart phones, and other devices in everyday business and personal life. Every time digital content is retrieved, a digital footprint that can be used to trace the action to a particular individual or device is created. The explosion of online content and the growth of online services such as online banking and electronic health records expanded the surface of attacks on personal privacy. According to Cisco (2014), by 2018 global IP traffic is expected to reach 1.6 zettabytes per year, and over half of all IP traffic will originate with non-PC devices. Contributing factors for growing concerns about privacy are:

- Decreasing storage cost.
- Decreasing cost of computing power.
- Decreasing cost of transmitting data.
- Increasing popularity of business intelligence
- Business digitalization

In 2001 due to the USA Patriot Act banks started performing due diligence on customers, such as verifying identity and indefinitely storing account activity. It triggered the collection of personal data such as credit card records, phone records, health care records, e-mails, and mobile devices location. “Digitalization - The Third Era of Enterprise IT” has begun, according to Gartner (2014).

Computing professionals are the ones who must design and implement information systems to prevent private information disclosure. Privacy violations are not always the result of poor security, so students must learn about privacy as an essential principle in information systems, instead of learning it as consequences of poor information system security. The disclosure of personal information will eventually compromise security, as it happened with Sarah Palin’s account when a published answer to a security question allowed a password change (Zetter, 2008).

Despite the importance of privacy, many educational programs do not cover the subject systematically and comprehensively. Many universities base their computing curriculum on the Association for Computing Machinery’s (ACM) curriculum model. The authors found that both ACM Information Technology Curricula IT 2008 (ACM, 2008) and ACM Computer Science Curricula 2013 (ACM, 2013) have a minimal coverage of privacy topics. Moreover, the majority of the learning objectives only call for understanding rather than application and analysis. Students must learn how to incorporate privacy protection in the software designs and the systems configuration if they are to be effective in countering security breaches. They must be able not only to describe, but also to design and implement privacy protection in information systems. In addition, both curriculum models do not provide details for the learning objective and topics. Therefore, the interpretation and implementation of learning outcomes largely depends on individual instructors.

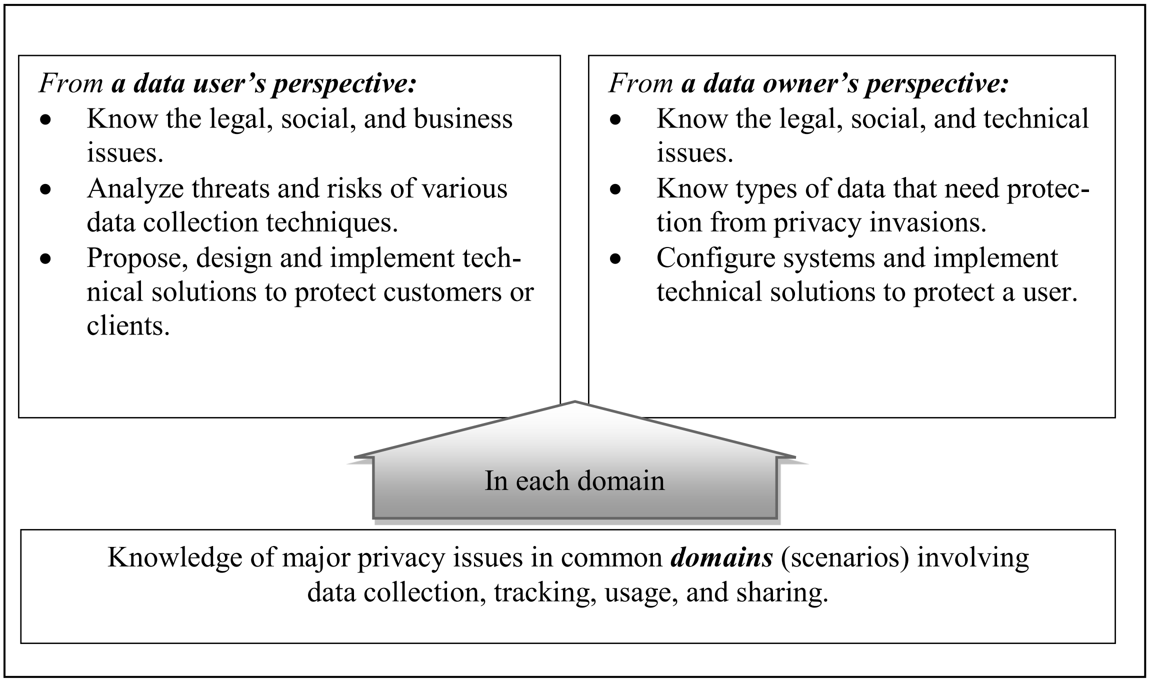
Several authors have shown that there is a gap between students knowing that there is a possible privacy issue and their behaviors as end-users (Ackerman, 2000; Brandimarte, Acquisti, & Loewenstein, 2010; Rowan & Dehlinger, 2014). Students need to see how a privacy breach happens and to start behaving accordingly.

The following incidents and research motivated development of the labs presented in this paper:

- In 2010 Google launched a social service called Buzz and exposed the personal contacts of its email users. Internet privacy groups received $8.5M when Google settled the lawsuit (Krazit, 2010). Another example is the location tracking as a result of wide use of mobile devices.
- eBay users' public profiles were cross-referenced with social network profiles on Facebook to reveal sensitive information about eBay users (Minkus & Ross, 2014).
- Facebook was forced to implement a more secure authentication method to protect users from widely publicized FireSheep wireless networking attack. Google now uses https as a default protocol to deliver query results (McMillan, 2011).
- Researchers in the paper "I Know Where You are and What You are Sharing" (Blond, Zhang, Legout, Ross, & Dabbous, 2011) used Skype API and Maxmind to track user mobility even when they were behind NAT.
- The newest threat is the Internet of Things which can compromise privacy by combining the characteristics of ubiquitous sensor networks and other identifiable things (Abomhara & Koien, 2014).

A Privacy Education Framework

To address the current education and training deficiencies on privacy, the privacy education framework was developed to guide the curriculum development. The learning framework proposed by the authors (Peltsverger & Zheng, 2012) is based on the competencies illustrated in Figure 1. The framework emphasizes the knowledge and skills built upon domains, and it features a complete educational focus on both perspectives of data collector and data providers.



From ***a data user's perspective:***

- Know the legal, social, and business issues.
- Analyze threats and risks of various data collection techniques.
- Propose, design and implement technical solutions to protect customers or clients.

From ***a data owner's perspective:***

- Know the legal, social, and technical issues.
- Know types of data that need protection from privacy invasions.
- Configure systems and implement technical solutions to protect a user.

In each domain

Knowledge of major privacy issues in common ***domains*** (scenarios) involving data collection, tracking, usage, and sharing.

Figure 1: Privacy Curriculum Development Framework

A domain is an application or behavior area where privacy issues are likely to rise. Each domain may have its own unique issues and involve specific technologies and regulations. For example, Privacy Rights Clearinghouse has provided a list of these areas ("Privacy Today," 2015), and the list is growing as new technologies and behaviors emerge. This trend is illustrated when the wide usage of smartphones with geo location technology introduced the location privacy issues. At different stages of processing data, these issues and domains can be categorized as data collection (including explicit and implicit data collection), data storage and management, and data use.

The skills and competencies are broadly categorized into two areas based on the entity's relationship to data: data owner and data user. Data owners are often the service consumers who are the owners of the information, and their information may be captured and used by service providers (data users) when consumers are using or have used the service. Data users can also include those who collect and use secondary data that is not directly collected from data owners.

These two areas are complementary to each other and together depict the complete education blueprint. Education on both areas is equally important as students can be involved in both areas. As data owners, students should be able to understand the privacy issues involved and know how to use tools to protect their own privacy, either from an individual perspective or from an organization's perspective. This aspect of privacy is most often covered in existing IA curriculum. Education on the data user side is equally important as students are designing and developing systems and applications to collect and analyze data, and any negligence may lead to potential troubles and damages.

From either perspective, both technical and non-technical knowledge should be addressed. Non-technical parts are commonly about the laws and regulations that govern the data collection and sharing process, such as Family Educational Rights and Privacy Act (FERPA), the Gramm Leach Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA). The technical part, such as system administration and configuration (e.g., user permissions, domain policies), data sharing and application development, is a particular focus for information technology students.

A data-sharing example: In the online advertising industry, DoubleClick can be protected from legal actions if all data they sell is protected from deanonymization. The company tracks the individual Internet users. As soon as the first advert is displayed on a computer, a unique number is generated and saved in a cookie file on the user's computer. When the user visits another website with DoubleClick adverts, DoubleClick reads the cookie and can customize what advert will be displayed. Participating businesses need to fully understand the threats and risks involved in DoubleClick's technologies.

Students should be introduced to best practices, technologies, and systems for privacy preservation. Not only should they know and evaluate these technologies, but also know how to develop and configure systems to prevent privacy violations. Students must understand common data collection and tracking technologies, so they can configure systems to protect their own privacy. Google's CEO Eric Schmidt in his interview with the Wall Street Journal (Jenkins, 2010) said: "every young person one day will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends' social media sites."

The framework provides a conceptual guideline for privacy education assessment. It can also be used to identify current course deficiencies and course development opportunities.

Learning Module Design

Many instructors would like to cover privacy topics from a more technical aspect, but a lack of teaching resources and environment limits their ability to do so. It is necessary to develop teaching materials that include hands-on exercises to address major technical competencies defined in the framework. The development of appropriate courseware will benefit not only existing courses to add hands-on learning experience in technical aspects of privacy and data protection, but will also open up new opportunities to a more specialized and strengthened track.

To illustrate the design of technical aspects of privacy education, we have developed the first four modules that focused on the technical competencies. All learning modules include technical labs. Each learning module consists of readings, demonstrations, hands-on assignments, discussions, and assessments. As a prerequisite, students should have a fundamental knowledge of networking concepts (ports, protocols, HTTP, DNS) and basic web technologies and be able to use client-side technologies (forms, JavaScript) to implement web pages.

A study guide is provided to assist the completion of each module. The study guide consists of overview, learning outcomes, lecture notes, a list of reading materials, and tasks with estimated time to complete for each assignment (see Figure 2).

1) Overview: this section gives a high level overview of the module and describes the basic purpose and objectives.
2) Learning outcome: this section specifies the key learning outcomes in terms of concepts and practices.
3) Learning materials:
    a) Reading materials and references (2 to 3 hours).
    b) Lecture notes, tutorials, labs, etc.
    c) Additional reading materials and resources.
4) Task list: lab, assessment instruments (quizzes, review questions, assignments) to measure interest, knowledge and skills of students before and after the labs).
    a) Lab or guided exercise (1 hour).
    b) Discussion: 3 to 5 review questions focusing on the most important concepts (1 hour).
    c) Research and discuss (optional): required students to conduct light research work and share findings with the class. This may be used for senior level or graduate courses.
    d) Assignments: 2 to 3 tasks focusing on hands-on solutions (2-3 hours).
    e) Assessment: 10 to 15 multiple-choice quiz (1 hour).

Figure 2. Basic learning module structure (organization).

The following two sections briefly describe each module to illustrate the module content and the structure.

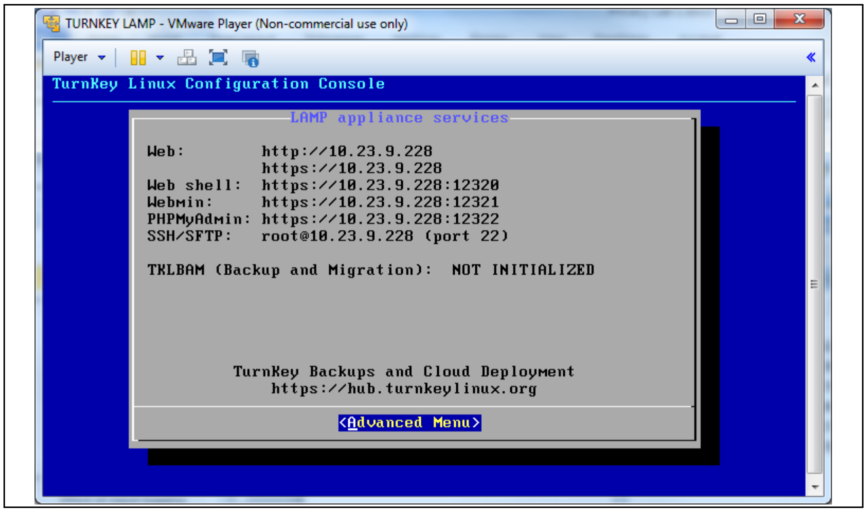
Module 1: Keyboard and Mouse Action Tracking

Every time a user presses any key on a keyboard to enter, modify, or delete characters, or uses a key combination to copy (ctrl+c) and paste (ctrl+v) text, these events can be captured by the web application and trigger other events. It is also possible to track mouse movement such as screen position, clicking, hovering, and scrolling. This lab demonstrates how user keyboard and mouse actions can be tracked using client scripts and commonly available tools. Prerequisites for this module are a knowledge of HTML, CSS, and JavaScript.

Upon completion of the module, students will be able to:

- Examine client scripts that can track keyboard actions.
- Examine client scripts that can track mouse actions.
- Evaluate potential privacy risks arising from user tracking.

To deliver this lab, a TurnKey LAMP VM is used (http://www.turnkeylinux.org/lampstack). The LAMP stack is a popular open source web platform commonly used to run dynamic web sites and servers. It includes Linux, Apache, MySQL, and PHP/Python/Perl. All lab applications are deployed inside the VM. Figure 3 shows booted VM that displays server information.



```
TurnKey Linux Configuration Console

                    LAMP appliance services

      Web:         http://10.23.9.228
                   https://10.23.9.228
      Web shell:   https://10.23.9.228:12320
      Webmin:      https://10.23.9.228:12321
      PHPMyAdmin:  https://10.23.9.228:12322
      SSH/SFTP:    root@10.23.9.228 (port 22)

      TKLBAM (Backup and Migration):  NOT INITIALIZED



               TurnKey Backups and Cloud Deployment
                   https://hub.turnkeylinux.org

                         <Advanced Menu>
```

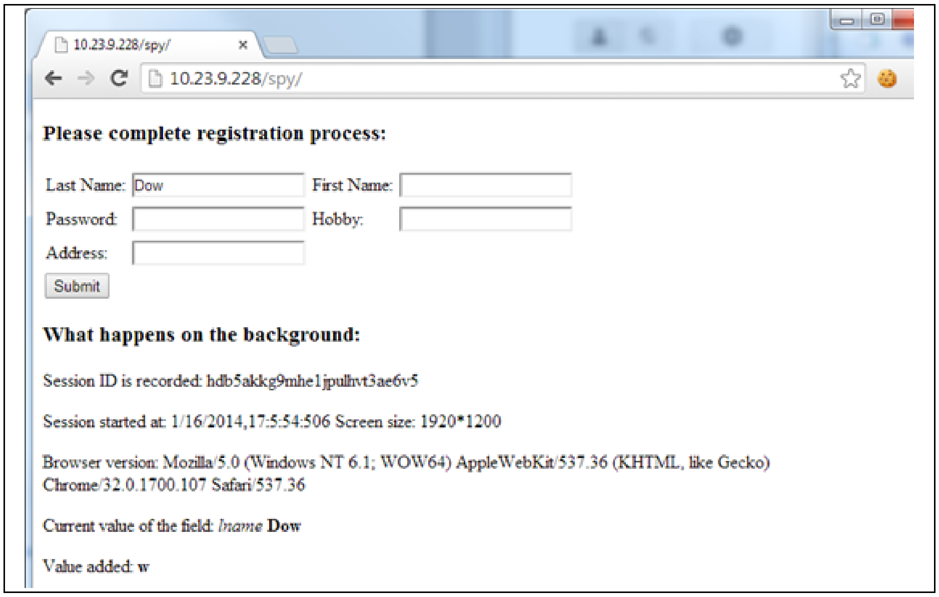
Figure 3. TurnKey LAMP VM.

The pre-lab section consists of assigned reading, theory overview, and five guided exercises.

1) Studying DOM properties. Students use Firefox's Developer Toolbar to learn the structure of the Google Search home page http://google.com
2) Manipulating DOM using JavaScript. Students use Firefox's Developer Toolbar to alter the structure of the Google Search home page http://google.com
3) Analyzing details of three main keyboard events (onkeydown, onkeypress, and onkeyup) in different web browsers. Students use the keyboard to produce keyboard events and analyze generated alerts.
4) Mouse position tracking. Student use the mouse to produce keyboard events and analyze generated alerts.
5) Analyzing components of dragging event. Students learn four components of the drag (ondragenter, ondragover, ondragleave, ondrop) by producing events and analyzing generated alerts

To reinforce understanding of the theory, two guided exercises are included in the main lab section.

The first exercise is dedicated to keyboard tracking and walks students through a registration form that uses Ajax to collect user's input without form submission. Figure 4 shows the form that is used to collect information from a user. During this exercise, students also use a Firefox add-on proxy Tamperdata to track actions of a web application. Later students are presented with a log file that has a record of every keystroke they made.



Please complete registration process:

Last Name: Dow First Name:

Password: Hobby:

Address:

Submit

What happens on the background:

Session ID is recorded: hdb5akkg9mhe1jpulhvt3ae6v5

Session started at: 1/16/2014,17:5:54:506 Screen size: 1920*1200

Browser version: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36

Current value of the field: *lname* **Dow**

Value added: w

Figure 4. Keyboard tracking.

The second exercise for the mouse tracking includes playing Ping-Pong (Figure 5) and observation of tracking results using smt2 tracking (see http://code.google.com/p/smt2/wiki/readme).

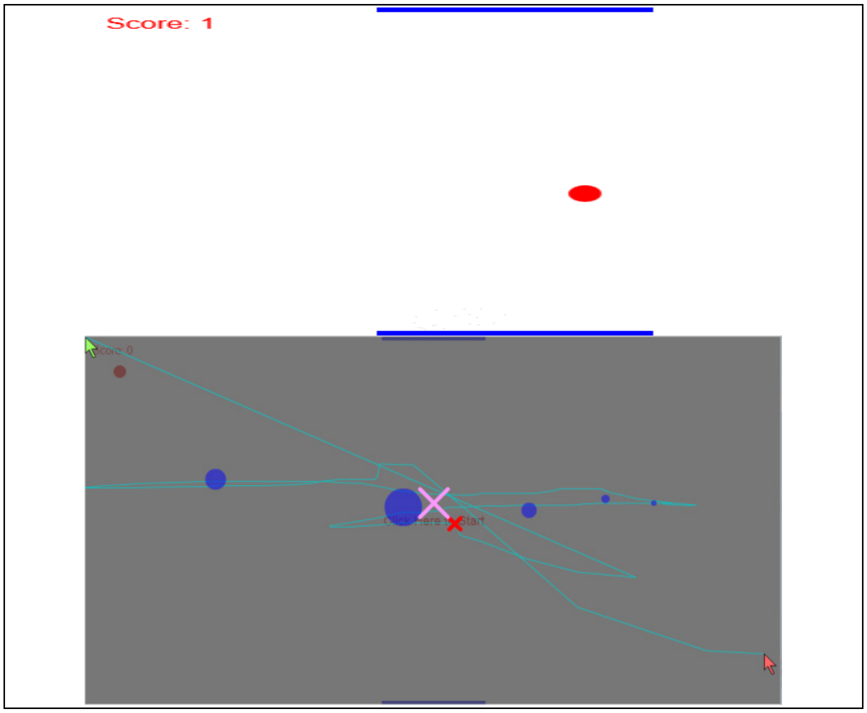


Figure 5. Ping Pong Game and the results of mouse tracking

The guided exercises include discussion of browser settings to show that disabling right and/or middle mouse button or disabling JavaScript altogether will limit or even make impossible tracking of user actions. Besides guided exercises, all source code is provided to students so they understand the programming side of keyboard and mouse tracking.

The discussion section reflects on what students have learned about user tracking during guided exercises. Throughout this activity, students create a list of protective measures that include browser settings modification and browser add-ons. The application contains tracking code and students have to find exactly which user activity is being tracked, how it is done and how it can be prevented.

Module 2: Cookies and Privacy Concerns

A cookie is a small piece of data stored by a web browser on a client computer. It can be read by the server side programs to retrieve its value. Cookies are commonly used for session management, user preference and/or history setting, and tracking. Because of their use in user tracking techniques, cookies have raised many privacy concerns. This module examines cookies in depth and demonstrates how cookies can be used to store and track various user data what may lead to privacy violations (Toubiana, Verdot, & Christophe, 2012).

Upon completion of the module, students will be able to:

- Explain how cookies can be used to store user information and what types of data can be stored.
- Explain cookie attributes, restrictions, and their impact.
- Explain the use of cookie to track users within and across websites (domains).
- Configure privacy settings related to cookie usage in browsers.
- Discuss how cookies can potentially compromise the privacy.

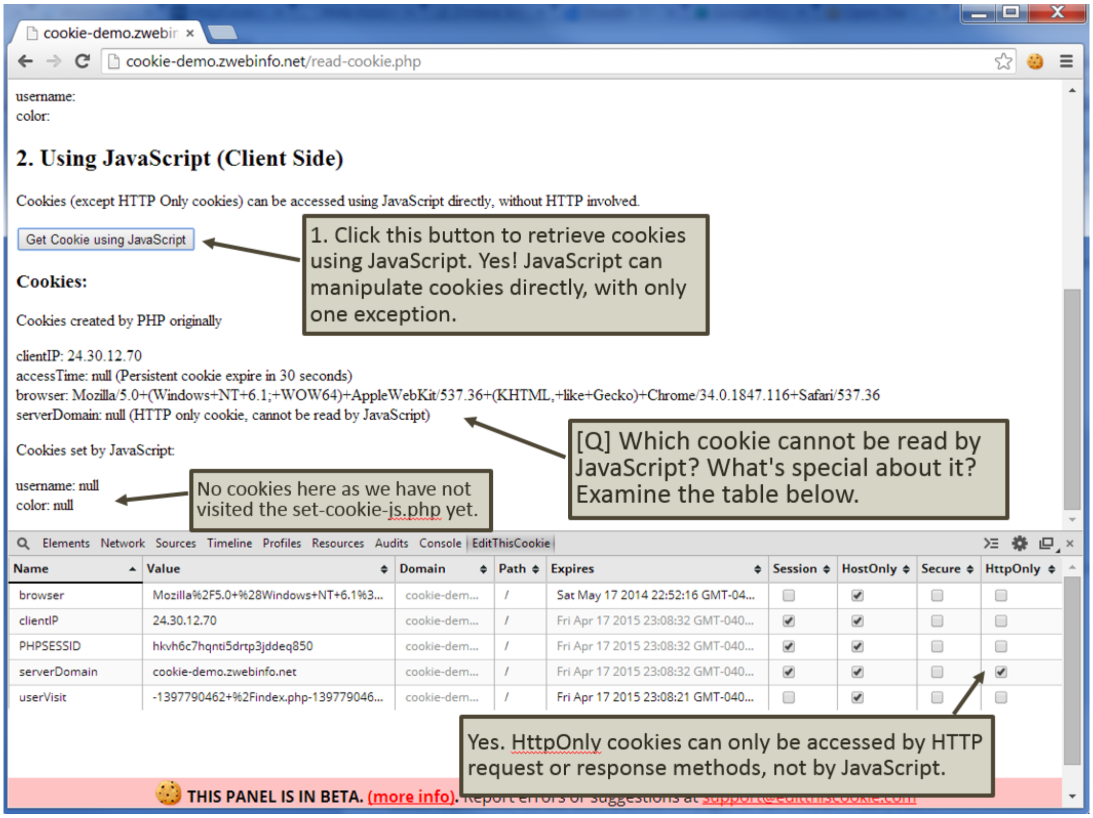
The lab section consists of five guided exercises. A lab environment includes three domains (one with two sub domains) and a number of web pages that creates and reads cookies.

1) View cookie data using browser tools (Chrome Developer Tools) and third party tools (like EditThisCookie) (Figure 6). Students will have firsthand experience of seeing how cookies are set and read with HTTP protocol, and properties of cookies like name, value, domain, path, expiration, size, etc.
2) Examine major cookies' attributes and their impacts. In this exercise, students will have in depth experience with the effects of major cookies attributes expires, HTTPOnly, and see the effects of server-side set cookies and client-side set cookies. Students will learn the difference between session and persistent cookie.
3) Examine how cookies are used for user tracking. The example shows how JavaScript is used for user action tracking. The captured information stored in cookies and will be sent to the server the next time this page is requested.
4) The exercise demonstrates cross-domain user tracking and the technique of webbug.
5) Configure browser setting to allow/block third party and all cookies.

Besides guided exercises, all source code is provided to students so that they understand the programming side of cookie manipulation. Two programming methods are used: PHP on the server side and JavaScript on the client side. The module demonstrates the difference between server and client side processing of cookies. They are asked to change the code to modify cookie attributes.

1. Students are guided to set and read cookies in the same domain and different domains. They will practice a number of ways on cross-domain cookie use, including iframe, image, and JavaScript.

2. Students are shown one particular scenario demonstrating how an advertising service works using cookies.



cookie-demo.zwebir ×
cookie-demo.zwebinfo.net/read-cookie.php

username:
color:

2. Using JavaScript (Client Side)

Cookies (except HTTP Only cookies) can be accessed using JavaScript directly, without HTTP involved.

Get Cookie using JavaScript

1. Click this button to retrieve cookies using JavaScript. Yes! JavaScript can manipulate cookies directly, with only one exception.

Cookies:

Cookies created by PHP originally

clientIP: 24.30.12.70
accessTime: null (Persistent cookie expire in 30 seconds)
browser: Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/34.0.1847.116+Safari/537.36
serverDomain: null (HTTP only cookie, cannot be read by JavaScript)

[Q] Which cookie cannot be read by JavaScript? What's special about it? Examine the table below.

Cookies set by JavaScript:

username: null
color: null

No cookies here as we have not visited the set-cookie-js.php yet.

Name	Value	Domain	Path	Expires	Session	HostOnly	Secure	HttpOnly
browser	Mozilla%2F5.0+%28Windows+NT+6.1%3...	cookie-dem...	/	Sat May 17 2014 22:52:16 GMT-04...	☐	☑	☐	☐
clientIP	24.30.12.70	cookie-dem...	/	Fri Apr 17 2015 23:08:32 GMT-040...	☑	☑	☐	☐
PHPSESSID	hkvh6c7hqnti5drtp3jddeq850	cookie-dem...	/	Fri Apr 17 2015 23:08:32 GMT-040...	☑	☑	☐	☐
serverDomain	cookie-demo.zwebinfo.net	cookie-dem...	/	Fri Apr 17 2015 23:08:32 GMT-040...	☑	☑	☐	☑
userVisit	-1397790462+%2Findex.php-139779046...	cookie-dem...	/	Fri Apr 17 2015 23:08:21 GMT-040...	☐	☑	☐	☐

Yes. HttpOnly cookies can only be accessed by HTTP request or response methods, not by JavaScript.

THIS PANEL IS IN BETA. (more info). Report errors or suggestions at support@editthiscookie.com

Figure 6. Using JavaScript to Read a Cookie

After the lab, a number of tasks are presented to students to see if they have learned from the readings and guided exercises.

Finally, an assignment is provided for additional hands-on work. The assignment asks students to design and implement a solution (using cookies) to track user input in a form and automatically load the user input the next time the form is requested.

1. Develop a prototype solution, using cookies, to demonstrate that a website can log its user search terms and the date/time of each search. You may need a web server for this assignment. Submit your source code for the webpage.
2. [Bonus] Is that possible to log user search terms and the date/time of each search from a third party cookie? Please test your design and demonstrate.

Module 3: How Websites Use Your Data to Display Targeted Ads

This lab demonstrates how visiting a single page can result in information about your visit being shared with dozens of other businesses, how web information sharing is implemented, and what service providers do not tell their customers. It is a follow-up of the previous module on cookies to apply the basic techniques in a more realistic ecommerce scenario. It demonstrates how a third party company or an advertising network (e.g., DoubleClick) can collect user-tracking data from several sites and then display targeted ads.

Upon completion of the module, students will be able to:

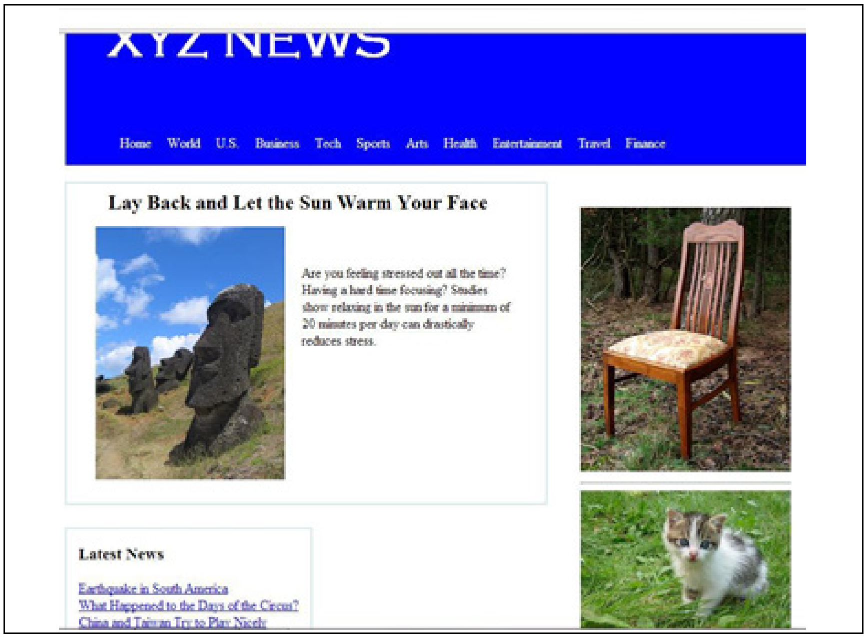
- Detect web bugs.
- Recognize web traffic that is generated by third parties.
- Evaluate potential privacy risks arising from user tracking.

The majority of big tracking sites are connected through third-party sites, e.g., tmz.com connects Facebook and DoubleClick (Cross & Geary, 2012). The students use Firefox/Chrome add-on Collusion to see real time interaction between Internet sites. The lab is developed inside the TurnKey LAMP VM (Figure 3) and contains four ecommerce websites *kittenshop.org*, *chairworld.com*, *xyznews.com* and *twoclicks.com*.

Pre-Lab activities include assigned reading and discussion on browser vulnerabilities and overview of lawsuits filed against companies that collect users' browsing history without users' knowledge.

The guided exercise walks student through two e-commerce websites *kittenshop.org*, *chairworld.com* and then brings students to visit a news portal *xyznews.com* (see Figure 7) where they find ads showing chairs and kittens they were interested in at *kittenshop.org* and *chairworld.com*. Besides guided exercises, all source code is provided to students so they understand the programming side of user tracking using cookies.

Students study how the information about browsing was collected by a third party website *twoclicks.com*. Then students are directed to *twoclicks.com* to check what browsing information *twoclicks.com* has collected. Every time students visited a product page, *twoclicks.com* collected the URL, details about the browser, requester's IP, and time of the request.


XYZ NEWS
Home World U.S. Business Tech Sports Arts Health Entertainment Travel Finance

Lay Back and Let the Sun Warm Your Face

Are you feeling stressed out all the time? Having a hard time focusing? Studies show relaxing in the sun for a minimum of 20 minutes per day can drastically reduces stress.

Latest News

Earthquake in South America
What Happened to the Days of the Circus?
China and Taiwan Try to Play Nicely

Figure 7. The results of user tracking

The image included in both ecommerce websites *kittenshop.org* and *chairworld.com* is generated by *handle.php* file called from TwoClicks site. The file sets a cookie if the cookie is not set for this browser. Information about the cookie is stored in the TwoClicks database. The database also stores:

- user's IP address,
- referer information (the URL of a web page that contains the link that called the current page),
- time and date, and
- the browser information.

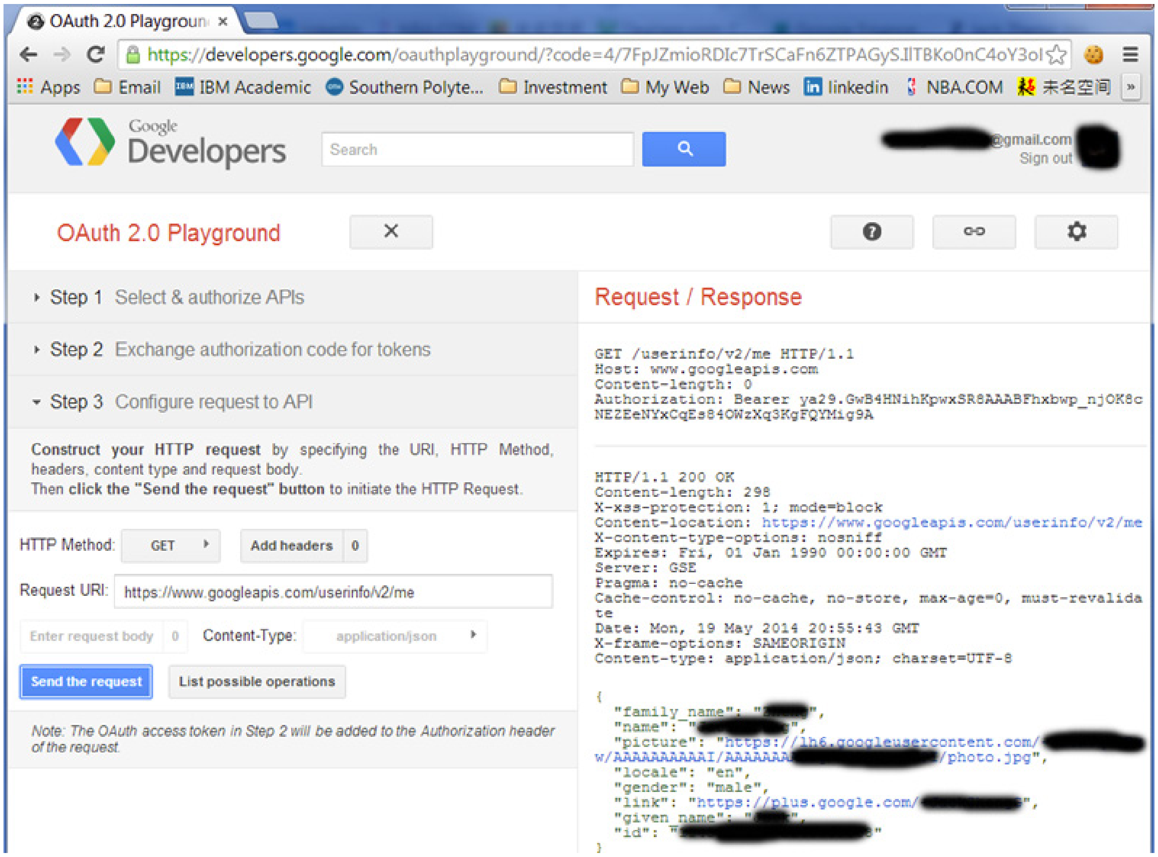
The exercise is followed by discussion on tracking detection and prevention, a quiz, and a module assessment assignment. The students are asked to rewrite TwoClicks site to use a persistent cookie or HTML5 application cache.

Module 4: Public Identity Service and Privacy Concerns

Many small and social oriented websites and mobile apps allow users to be authenticated by certain co-operating sites (known as Relying Parties or RP) using a third party service, eliminating the need for webmasters to provide their own ad hoc systems and allowing users to consolidate their digital identities. Some of these services not only provided authentication but also share user information with consumer websites. In this module, students will perform a detailed inspection of what kind of data can be shared by these services. The goal of this module is to raise the awareness of user data sharing behind the scene.

Upon completion of the module, students will be able to:

- Explain and contrast authentication and authorization.
- Survey major public third party authentication/identity services.
- Discuss the advantages and privacy issues related to these services.
- Examine Google Authentication and Authorization Service and its technical details.
- Develop programs utilizing Google's service to get user information.
- Understand user information sharing associated with Google login.
- Manage user app permission configurations in Google.



OAuth 2.0 Playground

Step 1 Select & authorize APIs

Step 2 Exchange authorization code for tokens

Step 3 Configure request to API

Construct your HTTP request by specifying the URI, HTTP Method, headers, content type and request body.
Then **click the "Send the request" button** to initiate the HTTP Request.

HTTP Method: GET

Add headers 0

Request URI: https://www.googleapis.com/userinfo/v2/me

Enter request body 0 Content-Type: application/json

Send the request

List possible operations

Note: The OAuth access token in Step 2 will be added to the Authorization header of the request.

Request / Response

```
GET /userinfo/v2/me HTTP/1.1
Host: www.googleapis.com
Content-length: 0
Authorization: Bearer ya29.GwB4HNihKpwxSR8AAABFhxbwp_njOK8c
NEZEeNYxCqEs84OWzXq3KgFQYMig9A

HTTP/1.1 200 OK
Content-length: 298
X-xss-protection: 1; mode=block
Content-location: https://www.googleapis.com/userinfo/v2/me
X-content-type-options: nosniff
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Server: GSE
Pragma: no-cache
Cache-control: no-cache, no-store, max-age=0, must-revalida
te
Date: Mon, 19 May 2014 20:55:43 GMT
X-frame-options: SAMEORIGIN
Content-type: application/json; charset=UTF-8

{
  "family_name": "[redacted]",
  "name": "[redacted]",
  "picture": "https://lh6.googleusercontent.com/[redacted]
w/AAAAAAAAAAI/AAAAAAA[redacted]/photo.jpg",
  "locale": "en",
  "gender": "male",
  "link": "https://plus.google.com/[redacted]",
  "given_name": "[redacted]",
  "id": "[redacted]"
}
```

Figure 8. Google Authentication Playground

In the lab, students will complete a hands-on exercise to experiment with Google Authentication and Authorization Services. Students will login to a sample website using Google credentials and access the user's information.

The lab consists of four exercises:

1) Experience the basic login process with an example site that accepts Google login and learn what information is requested.
2) Visit the Google OAuth Playground https://developers.google.com/oauthplayground/ to see what information can be shared (see Figure 8).
3) Write code that uses Google login https://developers.google.com/+/quickstart/javascript
4) Managing permissions: granting and revoking access to a token or app in three ways.

The assignment is to develop a website that uses Google login and retrieves user's activities and information from YouTube.

Students Survey and Feedback

At the end of each module, students complete a survey that collects feedback in the following four areas:

- Learning material organization, instruction and logic flow.
- Achievement of learning outcomes.
- Satisfaction with learning process.
- Effectiveness of assessments that cover technical details.

The survey consists of 14 questions or statements. The first group consists of twelve statements that measure students' perceptions and learning effectiveness. Students evaluate these statements using a 5-point Likert scale. The next group consists of two open-ended questions designed to collect qualitative comments and feedback. Students' qualitative feedback provided valuable insights that were used to improve the current modules and will help in the development of future modules on technical aspects of privacy. The survey questions are included in the Appendix.

The first two modules were used in two graduate courses. The first module was used in a graduate course that focused on multi-tier application development, and the second module was used in a graduate course that focused on advanced web concepts and applications. A total of 27 students completed the modules and provided feedback. Quantitative responses are summarized in Table 1.

Overall, more than 96% of all students agreed that modules have a clear objectives/learning outcomes and assigned reading helped them to successfully achieve module outcomes. 100% of students agreed that tasks in the modules were helpful in applying knowledge with 93% indicating that hands-on exercises and examples provided in the modules are crucial in understanding technical aspects of privacy and that the assessments tested what they have learned through the module.

Sixty-four percent of students did not fully understand the concepts covered in modules before starting the module. Eighty-nine percent of students agreed that after the completion of the module they are more aware of the issues and will act accordingly. Seeing examples in the module motivated 95% of the students to learn more about technical aspects of privacy.

Table 1: Student Feedback Summary

#	Survey Item	Strongly disagree %	Disagree %	Neutral %	Agree %	Strongly agree %
1	This module has clear objectives and learning outcomes	0	0	4	59	37
2	The readings in this module are adequate to achieve learning outcomes.	0	0	4	52	44
3	The tasks are helpful in applying knowledge.	0	0	0	41	59
4	These laboratory exercises are crucial in understanding technical aspects of privacy.	0	4	4	33	59
5	The assessment indeed tests what I have learned through the module.	0	0	7	48	44
6	Seeing these examples motivated me to learn more about technical aspects privacy.	0	0	5	53	42
7	I've already learned these concepts in other classes	0	22	26	37	15
8-10 *	I fully understood concepts covered in the module before starting the module	0	37	27	23	12
11	Examples and guided exercises from this module gave me better grasp of the concepts.	0	0	7	41	52
12	Now I will be more aware of the issues and act accordingly	0	0	11	37	52

* Some questions are combined for analysis and reporting

Students reported the following strengths of the developed modules:

- Informative content that includes guided exercises and videos;
- Credibility of used materials;
- Thorough coverage of the content starting from the basics.
- Guided exercises that contributed to the achievement of the learning outcomes.

Students suggested the following improvements:

- Include more examples;
- Include more exercises;
- Include instructions in alternative formats;
- Include more details for each step of the guided exercises.

The feedback from students is encouraging. It shows that in spite of being exposed to web applications every day, the majority of the students did not understand the concepts covered in the modules. This shows the need for these types of learning exercises and the importance of coverage of the technical details. The students had a clear understanding of what they will learn and were provided adequate reading and enough hands-on exercises to understand the concepts and apply them in future.

Discussion and Conclusion

Our research shows that learning privacy from a technical perspective is much needed. A knowledge of privacy topics is expected by students' future employers and society. The curriculum framework that inspired the labware development anticipates attention to technical aspects to complement the coverage of privacy topics. The four sample modules introduced in this paper helped students to experience and, as a result, better understand the main privacy concerns with keyboard and mouse tracking, cookies, user tracking, and public identity. Throughout lab activities, students not only experimented with privacy breaches, but also created a list of protective measures that includes browser settings modification and browser add-ons. The learning modules assessments show that students after completing assigned reading and guided exercises are able to detect implicit and explicit data collection and design, configure, and implement technical solutions to prevent privacy violations.

The resulting framework and courseware can serve as a model for developing additional privacy learning modules under the framework and teach students about potential privacy risks. The collected feedback shows that hands-on laboratory exercises are helpful in understanding the technical aspects of privacy.

For future work, we plan to continue the development of new modules and encourage other relevant work to fill the gap. A more complete curriculum will help IT and IS departments design well-structured privacy courses and programs, and produce graduates that satisfy requirements of the industry, government, and society.

References

Abomhara, M., & Koien, G. M. (2014). Security and privacy in the Internet of Things: Current status and open issues. *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*. IEEE, 2014.

ACM. (2008). *Information technology curricula (IT 2008)*. Retrieved on January 17, 2014 from http://www.acm.org//education/curricula/IT2008%20Curriculum.pdf

ACM. (2013). *Computer science curricula 2013 (CS 2013)*. Retrieved on January 17, 2014 from http://www.acm.org/education/CS2013-final-report.pdf

Ackerman, M. S. (2000). The intellectual challenge of CSCW: The gap between social requirements and technical feasibility. *Human-Computer Interaction , 15*(2-3), 179-204.

Blond, S., Zhang, C., Legout, A., Ross, K., & Dabbous, W. (2011). I know where you are and what you are sharing. In *Proceedings of ACM SIGCOMM Internet Measurement Conference*, November 2-4, 2011

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2010). *Misplaced confidences: Privacy and the control paradox*. Workshop on the Economics of Information Security (WEIS), Boston, MA, June 2010. Retrieved July 2015 from http://www.futureofprivacy.org/wp-content/uploads/2010/07/Misplaced-Confidences-acquisti-FPF.pdf

Cisco. (2014). *The zettabyte era—Trends and analysis*. Retrieved on January 17, 2014 from http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html

Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. (2012). The White House. Retrieved on December 21, 2015 from https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Cross, C., & Geary, J. (2012, April 23). Tracking the trackers: Who are the companies monitoring us online? - interactive. *The Guardian*. Retrieved on January 17, 2014 from http://www.theguardian.com/technology/interactive/2012/apr/23/tracking-trackers-companies-following-online

Gartner. (2014). *Gartner's annual global CIO survey*, Retrieved on January 17, 2014 from https://www.gartner.com/imagesrv/cio/pdf/cio_agenda_insights2014.pdf

Jenkins, H. (2010, August 14). Google and the search for the future. *The World Street Journal.* Retrieved on January 17, 2014 from http://www.wsj.com/articles/SB10001424052748704901104575423294099527212

Krazit, T. (2010). *Google settles Buzz lawsuit for $8.5M*. Retrieved on January 17, 2014 from http://www.cnet.com/news/google-settles-buzz-lawsuit-for-8-5m/

Minkus T., & Ross, K. W. (2014). I know what you're buying: Privacy breaches on eBay. In *Proceedings of PETS'14*.

McMillan, R. (2011, January 26). Facebook offers protection against wireless Firesheep attack, *Computerworld*. Retrieved on January 17, 2014 from http://www.computerworld.com/article/2512602/security0/facebook-offers-protection-against-wireless-firesheep-attack.html

Peltsverger, S., & Zheng, G. (2012). Defining a Framework for Teaching Privacy in Information Assurance Curriculum. In *Proceedings of the 16th Colloquium for Information Systems Security Education (CISSE),* Orlando, FL June (pp. 89-94).

Privacy Today: A Review of Current Issues. (2015). Privacy Rights Clearing House. Retrieved on July 19, 2015 from https://www.privacyrights.org/ar/privacy-issueslist.htm

Roda, C., Kennedy, B., Perry, S., del Álamo, J. M., Tsormpatzoudi, P., Coudert, F. … Koop, H. (2014). *PReparing Industry to Privacy-by-design by supporting its Application in Research.* AUP

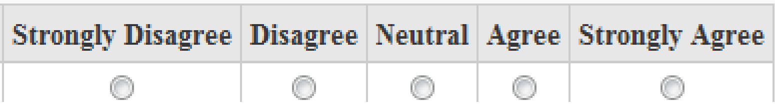
Rowan, M., & Dehlinger, J. (2014). Privacy incongruity: An analysis of a survey of mobile end-users. In *Proceedings of the 13th International Conference on Security and Management.*

Toubiana, V., Verdot, V., & Christophe, B. (2012). Cookie-based privacy issues on Google services. In *Proceedings of the second ACM conference on Data and Application Security and Privacy* (pp. 141-148). ACM Press. doi:10.1145/2133601.2133619

Zetter, K. (2008, September 18). Palin e-mail hacker says it was easy. *Wired*. Retrieved from http://www.wired.com/2008/09/palin-e-mail-ha/

Appendix. Post Survey for Lab 1 and 2: How Websites Use Your Data to Display Targeted Ads

Part I. For each statement below, check the appropriate column, as it applies to you.



Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
○	○	○	○	○

Common survey questions for all modules

1. This module has clear objectives and learning outcomes.
2. The readings in this module are adequate to achieve learning outcomes.
3. The tasks are helpful in applying knowledge.
4. These laboratory exercises are crucial in understanding technical aspects of privacy.
5. The assessment indeed tests what I have learned through the module.
6. Seeing these examples motivated me to learn more about technical aspects privacy.

Module specific survey questions

Module 1	Module 2
7. I learned in other classes how web apps could undermine privacy. 8. I fully understood before starting this module how a. user web tracking works. b. targeted ads and web behavioral marketing works. 9. Seeing examples from this module gave me better grasp of how a. web tracking works. b. targeted ads and web behavioral marketing works. 10. Analysis of logs generated by my interaction with a browser gave me better understanding of how user tracking is done.	7. I learned in other classes how cookies can be of a privacy concern from a technical perspective. 8. Before starting this module, I fully understood how a. Cookies work technically. b. Cookies are used for user tracking technically. c. to use PHP and JavaScript to set and read cookies. 9. Examples and guided exercises from this module gave me better grasp of how cookies work and are used for tracking. 10. I will be more aware of the tracking posed through a website and act accordingly (e.g. configure cookie or privacy settings).

Open-ended questions (same for all modules)

11. What are the strengths of this module?
12. What can be improved?

Biographies

Dr. Svetlana Peltsverger obtained her Ph.D. in Computer Science from the Institute of Systems Analysis, Russian Academy of Sciences, Moscow, Russia. Her primary research and teaching interests include networking, distributed computing, security, and databases. She is an Associate Professor of Information Technology at Kennesaw State University. She created various curricular materials for information security and privacy courses both at undergraduate and graduate levels. She serves as a curriculum coordinator for the Security/Policy group and holds a CISSP (Certified Information Systems Security Professional) certification. Dr. Peltsverger is a member of ACM Education Board IT2017 Task Group that is charged with updating the ACM/IEEE 2008 Curriculum in Information Technology. She has been the PI or co-PI in several research grants in the information security and privacy.

Dr. Guangzhi Zheng is an Assistant Professor of Information Technology in the College of Computing and Software Engineering at Kennesaw State University. He received his Ph.D. in Computer Information Systems from Georgia State University. His primary research and teaching interests include web application security, business intelligence, user interface, data visualization, and IT education. His research has appeared in the AIS Transactions on HCI, Journal of Systems and Software, Journal of Information Technology, and Journal of Information System Education.