World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:7, No:7, 2013

Authentic Learning for Computer Network with Mobile Device-Based Hands-On Labware

Kai Qian, Ming Yang, Minzhe Guo, Prabir Bhattacharya, and Lixin Tao

Abstract**—**Computer network courses are essential parts of college computer science curriculum and hands-on networking experience is well recognized as an effective approach to help students understand better about the network concepts, the layered architecture of network protocols, and the dynamics of the networks. However, existing networking labs are usually server-based and relatively cumbersome, which require a certain level of specialty and resource to set up and maintain the lab environment. Many universities/colleges lack the resources and build-ups in this field and have difficulty to provide students with hands-on practice labs. A new affordable and easily-adoptable approach to networking labs is desirable to enhance network teaching and learning. In addition, current network labs are short on providing hands-on practice for modern wireless and mobile network learning. With the prevalence of smart mobile devices, wireless and mobile network are permeating into various aspects of our information society. The emerging and modern mobile technology provides computer science students with more authentic learning experience opportunities especially in network learning. A mobile device based hands-on labware can provide an excellent 'real world' authentic learning environment for computer network especially for wireless network study. In this paper, we present our mobile device-based hands-on labware (series of lab module) for computer network learning which is guided by authentic learning principles to immerse students in a real world relevant learning environment. We have been using this labware in teaching computer network, mobile security, and wireless network classes. The student feedback shows that students can learn more when they have hands-on authentic learning experience.

Keywords**—**Mobile computing, android, network, labware.

I. Introduction

COMPUTER network courses are essential parts of college computer science curriculum. The ACM/IEEE Computer Science Curriculum 2008 lists Computer Networking as a required course under the "Net Centric Computing" body of knowledge. To improve computer network learning, hands-on networking lab is well recognized as an effective approach to help students understand the network concepts, the layered architecture of network protocols, and the dynamics of network. However, existing networking labs are usually server-based and relatively cumbersome, which require a certain level of specialty and resource to set up and maintain the lab environment. Major research universities have more resources for building their network-course-related lab facilities; but many other universities/colleges that lack the resources and build-ups in this field have difficulty to provide students with hands-on practice labs. A new affordable and easily-adoptable approach to networking labs is desirable for those universities/colleges to enhance their network education.

Another issue with current network labs is that they are short on providing hands-on practice for modern wireless and mobile network learning. Mobile computing has become an essential part of information technology into today's society. Smart mobile devices and their applications are making a fundamental shift in the way people conduct commerce, disseminate information, and perform daily activities. With the prevalence of smart mobile devices, wireless and mobile networks are permeating into various aspects of our information society. It is essential for computer science undergraduate students to be exposed to the cutting-edge wireless and mobile networking knowledge. More and more college and universities have realized the importance of these topics, and they either offer dedicated courses on wireless and mobile networking or integrate them into existing courses; but the focus of these courses are usually on theory of wireless local area networks and protocols, and the hands-on labs are sparse.

To overcome these problems, this paper presents our work on developing a lightweight, affordable, and easily-adoptable mobile device-based labware to enhance computer network teaching and learning through hands-on practice and immersive experience. We recognize the capability of smart mobile device as a unified platform to provide various authentic network environments for computer network learning, including IP network, wireless network, and mobile network. In addition, students will benefit from the instant gratification of mobile application development – they can quickly build a working graphical application and play the resulting application on their own mobile devices [1].

The labware in this paper is built upon the Android platform. The Android platform is open-source and Java-based, which enables students to leverage a wealth of Java API tools and benefits the incorporation of mobile computing into most of the core subjects in computer networks since it imposes fewer extra requirements on students and thereby shortens its learning curve. In addition, Android is the fastest growing mobile platform to date, and its popularity enables students to learn in a modern context with a great interest [2], [3].

Kai Qian and Ming Yang are with Southern Polytechnic State University, Marietta, GA 30060, USA (phone: 678-915-3717; fax: 678-915-5511; e-mail: kqian@spsu.edu).

Minzhe Guo and Prabir Bhattacharya are with University of Cincinnati, Cincinnati, OH 45221, USA (e-mail: bhattapr@ucmail.uc.edu).

Lixin Tao is with Pace University, Pleasantville, NY 10570, USA (e-mail: ltao@pace.edu).

In the development of the labware, an authentic learning strategy is employed to provide students with authentic networking problems and case studies, to encourage students discover authentic problems, and to leverage the authentic learning environment.

The rest of this paper is organized as follows. Section II presents the authentic learning for computer networks and the design of the labware. Section III demonstrates several example modules of the labware. Section IV discusses our experience in integrating the labware in network courses. Section V concludes the paper and describes our future work.

II. Labware

This section presents our authentic learning strategies for computer network and the design of our mobile device based labware that employs the authentic learning strategy.

A. Authentic Learning for Computer Networks

More and more colleges and universities across the country are turning to authentic learning practices and are putting the focus back on the learner in an effort to improve the way students absorb, retain, and transfer knowledge [4].

Authentic learning situates students in learning contexts where they encounter activities that involve problems and investigations reflective of those they are likely to face in their real world professional contexts [5], [6]. Researchers [4], [7], [8] have identified several characteristics of authentic learning, including: (1) authentic contexts that reflect the way the knowledge will be used in real-life; (2) authentic activities that are complex, ill-defined problems and investigations; (3) collaboration allowing for the social construction of knowledge; (4) opportunities for reflection involving meta-cognition; (5) opportunities for articulation to enable tacit knowledge to be made explicit; and (6) authentic assessment that reflect the way knowledge is assessed in real life.

Mobile computing can be a perfect fit to construct hands-on authentic learning environment for study of computer networks, in particular for the study of wireless and mobile networking. With mobile devices, students can work either individually or in a group setting for networking communication practice anywhere and anytime, without time and space constraints.

To implement the authentic learning for computer networks, we employ the following strategies in the development of the labware, including: 1) tie to the abstract concepts to real-world wireless and mobile network practices so that students can better understand the concepts and work more actively and effectively with facts and realistic problems; 2) encouraging students to identify for themselves the real-world mobile related tasks; 3) providing students with opportunity of reflection in action so that they can learn how and when to use particular strategies for problem solving; and 4) promoting the development of new perspectives and strategies for future applications.

Following the above strategies, all the lab activities in the labware are designed from real world mobile network scenarios, and they can be implemented and tested individually, either in peer-to-peer, or in a group setting. Students not only gain real-world experience with designed hands-on lab activities but also actively participate in developing their own mobile networking add-on labs on a given topic based on their own mobile device to be shared by other students. For example, some students developed lab for turning an Android phone to a hotspot router, which provides Wi-Fi service to other devices nearby. In the authentic learning environment, students will be encouraged to develop their own add-on lab activity in the same module.

We believe that the strong connection between academic subjects, real world applications, and digital-native students' everyday lives will promote students' learning interest and efficacy, and better prepare students for the high industrial demands.

B. Labware Design

The main objective of the proposed labware is three-fold: (1) using mobile labs to help students better understand network core concepts, the layered architecture of network protocols, and the dynamics of the networks; (2) facilitating students learning of network knowledge and skills; and (3) encouraging a community of faculty and students to share material and ideas for teaching and exploring mobile communication and network.

With the above objectives in mind and employing the authentic learning strategy, our mobile device based hands-on labware is designed as follows. The labware adopts a modular structure that organizes the learning materials into a sequence of reusable and self-contained learning laboratory modules. Each lab module is designed as a building block so that labs can be combined together into a single course of mobile development, or be integrated into the related courses. Each module covers a specific fundamental or emerging networking concept subject, such as the knowledge in the application layer of TCP/IP and mobile security. Each individual lab in a module is closely tied to a specific aspect in the module such as Bluetooth application and Wi-Fi application with mobile devices. Each lab consists of pre-activities (concept introduction), hands-on activities (hands-on step-by-step laboratory practices), and post-activities (student add-on labs that encourage student groups to create and share new add-on lab practice on the topic). These activities will also promote faculty's professional development and lifelong learning. Fig. 1 shows an example structure for application layer module of the labware.

Module: Application Layer

Learning Objectives:

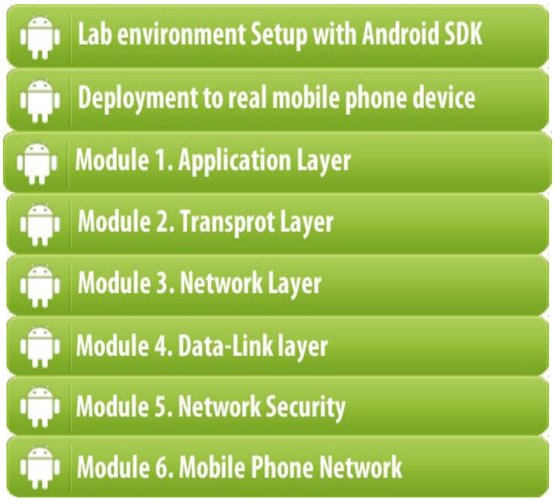
- Students understand the main concept of Application Layer.
- Students understand the best practice to the Application Layer on Android mobile device.

Activities:

- **Pre-Lab Activities**
- **Hands-on Lab Activities**
  1. HTTP request and respond
  2. Domain Name Service
  3. Email (POP3 and SMTP)
- **Post-Lab Activities** (*Student Add-on lab)

Fig. 1 Application Layer Module

The labs are designed in such a way that students can get started with mobile program development quickly, helping them build learning confidence through the lab practice. Lab modules will be designed to make student learning more relevant to their daily lives. In addition, all labs will facilitate the CS theory and concept learning to overcome the lack of hands-on lab practices in traditional teaching and learning environment. All learning modules are deployed on a Google repository site with mobile friendly interface shown below for easy mobile access anywhere and anytime (Fig. 2). The labware is expandable and evolvable so that faculty can easily add new lab modules into the repository.



Lab environment Setup with Android SDK
Deployment to real mobile phone device
Module 1. Application Layer
Module 2. Transprot Layer
Module 3. Network Layer
Module 4. Data-Link layer
Module 5. Network Security
Module 6. Mobile Phone Network

Fig. 2 Mobile Friendly Labware Page on Google Site

III. Lab Demonstration

To better illustrate the labware, this section demonstrates some of the labs that have been developed in the labware.

A. Network Layer

This lab uses mobile phones to introduce to students the routing services in the network layer of TCP/IP protocol stack. After finishing the lab, students should be able to understand the basic idea of how the routing works. The lab involves at least three Android devices: one works as a router and maintains a routing table, and the other two devices communicate through the router. The underlying communication protocol is Wi-Fi protocols. Fig. 3 depicts the working flow of the three devices in this lab.

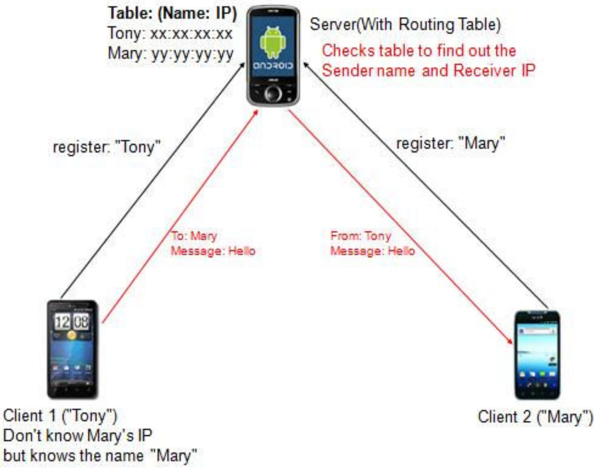
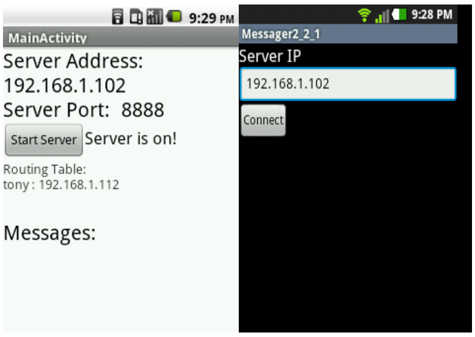


Fig. 3 The work flow of the routing lab

The phone router (the *Server* in Fig. 3) maintains a routing table that stores the information (e.g., identity and IP address) of clients (the *Client 1* and *Client 2* in Fig. 3) in local area. For a single network, client users may only know the name of the other clients rather than other clients' IP addresses. In this case, the router will help clients communicate with each other without knowing the exact IP address of the destination. In a more general case (i.e., clients can form multiple local area networks), phone routers will also find the correct network to forward the message. Before the clients can communicate through the routers, they need to register their information to the routers. For example, in Fig. 3, *Client 1* and *Client 2* register themselves to the *Server*, and then *Client 1* can communicate with *Client 2* by its registered name. In the following, we demonstrate the registration and communication processes.



9:29 PM
MainActivity
Server Address:
192.168.1.102
Server Port: 8888
Start Server Server is on!
Routing Table:
tony : 192.168.1.112
Messages:

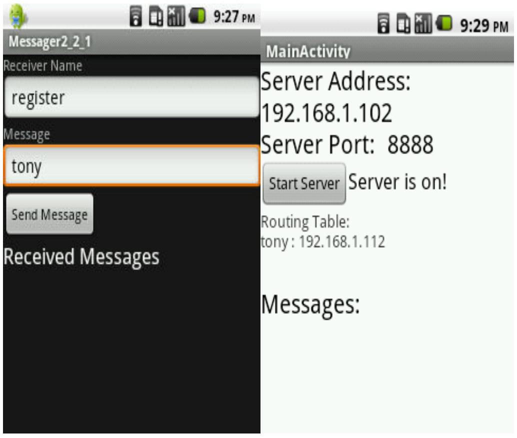
9:28 PM
Messager2_2_1
Server IP
192.168.1.102
Connect

Fig. 4 Server Startup

(1) Startup: the sub-graph on the left of Fig. 4 shows that the router app is started in the *Server* and its IP address is 192.168.1.102 (a private IP address for laboratory

purpose), and the sub-graph on the right of Fig. 4 shows that a client app is started in the client phone and is to establish a connection with the router app.

(2) Registration: after establishing the connection, clients need register to the *Server*'s routing table. For example, the left sub-graph of Fig. 5 shows that *Client 1* registers itself to the routing table by typing "register" command in the receiver name box and the name "tony" in the message box to register "tony" and send the request to the *Server*. The *Server* receives the registration request and adds *Client 1*'s information to the routing table, which is shown in the next screen shot on the right of Fig. 6.



Messager2_2_1

Receiver Name

register

Message

tony

Send Message

Received Messages

MainActivity

Server Address:
192.168.1.102
Server Port: 8888

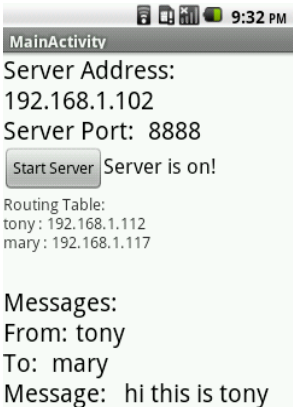
Start Server Server is on!

Routing Table:
tony : 192.168.1.112

Messages:

Fig. 5 Registration

(3) After the registration, clients can communicate by specifying the name of recipient and sending the message to the *Server*. The *Server* checks the routing table and finds the recipient's IP address, and then it forwards the message to the recipient. Fig. 6 shows the message sent from *Client 1* "tony" to *Client 2* "mary" through the *Server*.



MainActivity

Server Address:
192.168.1.102
Server Port: 8888

Start Server Server is on!

Routing Table:
tony : 192.168.1.112
mary : 192.168.1.117

Messages:
From: tony
To: mary
Message: hi this is tony

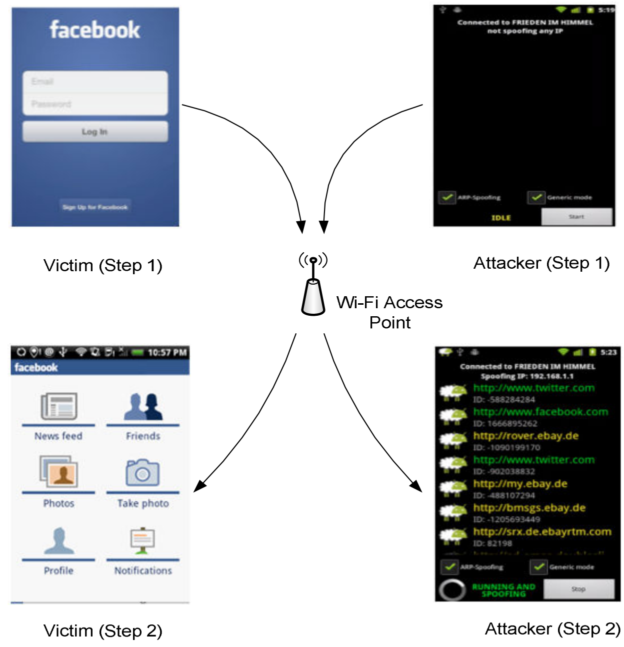
Fig. 6 Communication

B. Network Security

The network security module provides students with network security threat analysis and protection experience. In traditional computer security education, the protection principles and practices are the central topics. However, some academics have identified that, by experiencing actual attacks, the students will gain more insight, and that will enable them to design and implement better protections [9]. This attack/defend approach has been recognized as a highly effective approach to learning information security [10]. Therefore, in order to make the learning more effective, for each specific network threat, such as session hijacking and phishing, our labware develops a pair of hands-on labs: one for threat analysis and one for protection practice. Students will first experience an actual attack instance, and then they will be instructed on how to implement a protection solution using step-by-step tutorials. A protection solution practice can be to develop a mobile app (e.g., implementing a filter to block malicious text messages), applying an open-source security tool (e.g., using reverse engineering tools apktool and dex2jar), or a configuration (e.g., configuration of Android app permission).

For the attack analysis labs, we adopt the following design strategies: (1) we develop multimedia or mobile apps to demonstrate instances of network security attacks for the purpose of facilitating students in network security threats analysis; (2) students will not design attacks and will not perform real attacks to harm servers or peers' mobile devices; (3) the developed attack apps will be hard-coded and will not be effective in practice; and (4) the complete source code is hidden from students and is not distributed.

As an example, Fig. 7 illustrates the attack flow of an instance of session hijacking attack in the Wi-Fi networks, which is introduced in the attack analysis lab for session hijacking threat.



Connected to FRIEDEN IM HIMMEL
not spoofing any IP

IDLE

Connected to FRIEDEN IM HIMMEL
Spoofing IP: 192.168.1.1

http://www.twitter.com
ID: -588284284
http://www.facebook.com
ID: 1666895262
http://rover.ebay.de
ID: -1090199170
http://www.twitter.com
ID: -902038832
http://my.ebay.de
ID: -488107294
http://bmsgs.ebay.de
ID: -1205693449
http://srx.de.ebayrtm.com
ID: 82198

RUNNING AND SPOOFING

Fig. 7 Attack Flow of the Attack Analysis Lab for Network Session Hijacking Threat

As shown in Fig. 7, the lab involves at least two Android devices (one serves as the victim's device and the other one serves as the attacker's device) that connect to Internet via a same Wi-Fi access point. An Android device can be an Android emulator on desktop computers or a real Android smartphone/tablet. We develop a Wi-Fi session hijacking attack app, which is based on the open-source project DroidSheep [11], and install the attack app in the attacker's device. A prerequisite for the attack is that the attacker knows the IP addresses of the Wi-Fi access point and the victim, which can be achieved via network scanning or probing techniques. In the lab demonstration, an attack starts with activating the attack app and starts to spoof of the victim via ARP Spoofing ("Attacker (Step 1)" in Fig. 7). Then we let the victim request to access to her Facebook account ("Victim (Step 1)" in Fig. 7). This request with the victim's encoded Facebook account name and password will be sent through the access point to Facebook.com; and if authenticated, a response that contains the session information will be sent back through the access point to the victim. The victim can start to operate on her Facebook account ("Victim (Step 2)" in Fig. 7). Since the attacker has spoofed the victim's address, the response from the Facebook to the victim will also be sent to the attacker by the access point; and thus the session information is captured. If the Victim does not use HTTPs protocol for the request and response, the session information will appeared in clear text ("Attacker (Step 2)" in Fig. 7). The attacker can hijack the victim's session and operate on the victim's Facebook account.

In the protection practice part, the lab instructs students on using a protection app for protecting against the session hijacking attack. The protection app adapts DroidWall [12], an open-source Android Firewall, to allow students to conFig. the network activities of applications, such as not allowing the Facebook app to use Wi-Fi for communication. In addition, it helps students check whether the HTTPS protocol is actually used in the communication with a user-defined list of websites. Students can install the app in Android devices so that they can obtain an instant gratification from the hands-on practice and they are encouraged to create their own apps to detect new types of attacks and develop corresponding protection solutions.

IV. Student Feedback

Several lab modules in the labware have been presented to a network course and 26 undergraduate students completed a preliminary evaluation of the modules. Table I presents the questionnaire in the survey and the student feedback. Most of the students felt the labs were interesting and helpful, and obtained immerse experience in learning. The assignments were challenging in the development of an application for their own mobile devices. Most students felt that the experiences with our labware gave them confidence and motivation to learn more about wireless networking concepts and to try projects that are more ambitious in the future. Some of the student's comments are presented in the following:

- *I think the mobile project is interesting and useful. Current job regards mobile development skill as a plus to your programming experience. As a result, I think it is good to practice what we have learned in class to a real Android project.*
- *I think those labware were so effective and taught me a lot. I want to thank my professor.*
- *These labs were very interesting to complete. I especially enjoyed the ones where we were to use WireShark for packet capturing.*
- *I thought that the labware was a great idea and I enjoyed being able to learn something different.*
- *I liked the material where I learned how to create android project*
- *I liked being able to gain some hands on experience.*

V. Conclusion

In this paper, we presented a mobile device based labware that builds upon the state-of-the-art Android platform to provide good authentic learning environment and practice for learning computer networks concepts in a practical way. The labware engages students in active learning so that they can conFig. and program networking apps using smart mobile devices. It will foster students' innovation ability in the reflection of today's reality and prepare our undergraduate students for entrance into the industrial workforce. In the future, we will continue the development of the labware, and integrate and evaluate the labware in more courses.

TABLE I
Student Survey

#	**Survey Questions**	**Strongly Agree or Agree**
1	The mobile labware helps me understand better about the networking concepts in the project.	73.9%
2	The mobile labware provides me with more hands-on experience on learning networking concepts.	69.5%
3	The mobile labware is easy to follow and practice.	56.5%
4	The mobile labware promotes my interest and engagement in computer networks.	72.7%
5	The mobile labware promotes my interest and engagement in mobile app development.	69.6%
6	I gained real world networking experience from the real world relevant hands-on mobile labs.	56.5%
7	The hands-on lab will help me understand better about the network concepts.	73.9%
8	I prefer the anywhere and anytime on-go hands-on lab with open source based smartphones.	56.5%
9	The mobile labware will promote my interest and engagement in networking study.	77.2%
10	I prefer to get real world experience with the hands-on mobile labs.	65.2%

Acknowledgments

The work is partially supported by the National Science Foundation under award: NSF SFS grant award #1241651, Capacity Building in Mobile Security through Curriculum and

Faculty Development. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] M. Zyda, D. Thukral, J. Ferrans, "Incorporating Mobile Games into a Computer Science Game Degree Program," Microsoft Academic Days Conference on Game Development in Computer Science (GDCSE), 2008.

[2] D. Metcalf, S. Raasch, M. Milrad, A. Hamilton, D. Cheek, "My Sports Pulse: Increasing Student Interest in STEM Disciplines through Sports Themes," In Proceedings of Fifth IEEE International Conference on Wireless, Mobile, and Ubiquitous Technology in Education, March 23-26, 2008.

[3] Q. Mahmoud, A. Dyer, "Mobile Devices in an Introductory Programming Course," Computer, vol. 41, no. 6, pp. 105, 106-107, June 2008.

[4] M. Lombardi, "Authentic Learning for the 21st Century: An Overview," ELI White Papers, EDUCAUSE Learning Initiative (ELI), 2007, available at http://www.educause.edu/library/resources/authentic-learning-21st-century-overview, retrieved on Dec. 1, 2012.

[5] J. Brown, A. Collins, and P. Duguid, "Situated Cognition and the Culture of Learning, Educational Researcher, 18, n1, pp.32-42, 1989.

[6] J. Lave and E. Wenger, Situated Learning: Legitimate Peripheral Participation (Learning in Doing: Social, Cognitive and Computational Perspectives), Cambridge University Press, 1991.

[7] J. Herrington and R. Oliver, "An instructional design framework for authentic learning environments," Educational Technology Research and Development, 48(3), pp. 23-48. 2000.

[8] J. Herrington, J. Mantei, A. Herrington, I. Olney, and B. Ferry, New technologies, new pedagogies: Mobile technologies and new ways of teaching and learning, (eds.), University of Wollongong, 2009, 138p, ISBN: 978-1-74128-169-9.

[9] S. Caltagirone, P. Ortman, S. Melton, D. Manz, K. King, and P.W. Oman, "RADICL: A Reconfigurable Attack-Defend Instructional Computing Laboratory," Security and Management, Jun. 20-23, 2005, Las Vegas, Nevada, USA.

[10] W. Yurcik and D. Doss, "Different Approaches in the Teaching of Information Systems Security," in Proceedings of the 2001 Information Systems Education Conference (ISECON'01), Nov. 2001, Cincinnati, OH, USA.

[11] A. Koch, "DroidSheep," http://droidsheep.de, accessed on Oct. 29, 2012.

[12] R. Rosauro, "DroidWall - Android Firewall," http://code.google.com/p/droidwall, accessed on Oct. 29, 2012.