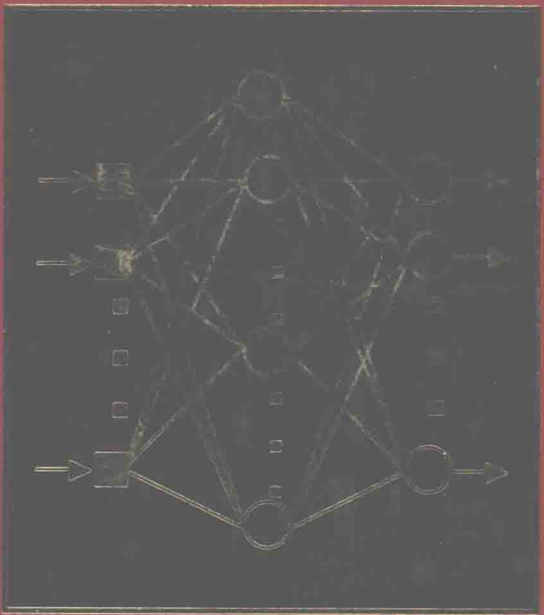
# Advances in COMPUTERS

## Volume 81

The Internet and Mobile Technology



Edited by

MARVIN V. ZELKOWITZ

# Advances in
# COMPUTERS

*EDITED BY*

MARVIN V. ZELKOWITZ

Department of Computer Science
University of Maryland
College Park, Maryland
USA

VOLUME 81

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK • OXFORD
PARIS • SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Academic Press is an imprint of Elsevier

ACADEMIC
PRESS

Academic Press is an imprint of Elsevier

32 Jamestown Road, London, NW1 7BY, UK
Radarweg 29, PO Box 211, 1000 AE Amsterdam, The Netherlands
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
525 B Street, Suite 1900, San Diego, CA 92101-4495, USA

First edition 2011

**Notice**
No responsibility is assumed by the publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein

**Library of Congress Cataloging-in-Publication Data**
A catalog record for this book is available from the Library of Congress

**British Library Cataloguing-in-Publication Data**
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-385514-5

ISSN: 0065-2458

For information on all Academic Press publications
visit our web site at elsevierdirect.com

Printed and bound in USA

11 12 13 10 9 8 7 6 5 4 3 2 1

*Advances in*

# COMPUTERS

## VOLUME 81

# Contributors

**Paul Braeckel** possesses over 11 years of software and product development experience, specifically within Computer Networking and Security, and using a wide variety of programming languages, platforms, and technologies. Currently, he leads the development of Ephemeral Credentialing Products as Project Manager at the Identity Theft and Financial Fraud Research and Operations Center in Las Vegas, Nevada, directed by Dr. Hal Berghel. He specializes in object-oriented development of cyber-security applications using .NET languages and his software development experience is broad, ranging from desktop business applications to complex web applications. Paul holds an M.S. in Computer Science from the UNLV and a B.S. in Mechanical Engineering from Washington University in St. Louis and is working on his Ph.D. in Informatics at the University of Nevada, Las Vegas. He may be contacted through the following e-mail address: paulb314@gmail.com.

**Carl Fischer** is a researcher and Ph.D. candidate in the School of Computing and Communications at Lancaster University, UK. He holds an engineering degree (2006) from Supélec and a Masters (2006) from the University of Rennes, both in France. He is interested in infrastructure-less tracking and navigation systems. Carl can be contacted at fischer@comp.lancs.ac.uk.

**Avi Goldfarb** is associate professor of marketing in the Rotman School of Management at the University of Toronto. He received his Ph.D. in economics from Northwestern University. His research has explored brand value, behavioral modeling in industrial organization, and the impact of information technology on marketing, on universities, and on the economy. Professor Goldfarb has published more than 30 articles in a variety of outlets. He is coeditor at *Journal of Economics and Management Strategy* and an associate editor of *Quantitative Marketing and Economics, Information Economics and Policy, International Journal of Industrial Organization*, and *Management Science*.

**Mike Hazas** is an academic fellow and lecturer in the School of Computing and Communications at Lancaster University. Mike received his Ph.D. degree from the

University of Cambridge (2003) for his work on broadband ultrasonic location systems. Since then, Mike has worked on position and context sensing hardware and signal processing, with a focus on evaluation using real deployments. Mike has served on the programme committees for a number of leading conferences on pervasive computing, including the International Conference on Ubiquitous Computing (UbiComp) and the European Conference on Wireless Sensor Networks (EWSN). Mike can be contacted at hazas@comp.lancs.ac.uk.

**Yiu-Wing Leung** received his B.Sc. and Ph.D. degrees from the Chinese University of Hong Kong in 1989 and 1992, respectively. His Ph.D. advisor was Prof. Peter T. S. Yum. He has been working in the Department of Computer Science of the Hong Kong Baptist University, and now he is a full professor. His research interests include two major areas: (1) networking and multimedia which include the design and optimization of wireless networks, optical networks, and multimedia systems, and (2) cybernetics and systems engineering which include evolutionary computing and multiobjective programming. He has published over 70 journal papers in these areas. Email address: ywleung@comp.hkbu.edu.hk.

**James W. Losey** is a program associate with the Open Technology Initiative at the New America Foundation. He focuses on connectivity and technology at the community, national, and international level. Most recently he has published in *Slate* and *IEEE Spectrum*, as well as resources on federal broadband stimulus opportunities and analyses of the National Broadband Plan. He can be reached at lesey@newamerica.net.

**Sascha D. Meinrath** is the director of the New America Foundation's Open Technology Initiative and is a well-known expert on community wireless networks, municipal broadband, and telecommunications policy. Sascha is a cofounder of Measurement Lab, a distributed server platform for the deployment of Internet measurement tools, and coordinates the Open Source Wireless Coalition, a global partnership of open source wireless integrators, researchers, implementors, and companies. Sascha has worked with Free Press, the Cooperative Association for Internet Data Analysis (CAIDA), the Acorn Active Media Foundation, the Ethos Group, and the CUWiN Foundation. He can be reached at meinrath@newamerica.net.

**Kavitha Muthukrishnan** is currently a postdoctoral researcher at the Embedded Software Group, Delft University of Technology, The Netherlands. She obtained her Ph.D. degree in Computer Science in 2009 from the University of Twente. Her Ph.D. thesis was entitled "Multimodal localisation: Analysis, Algorithms and Experimental Evaluation." She was associated with the Embedded Interactive Systems group at

Lancaster University as a visiting researcher in 2008. Prior to that, she obtained her Master's degree in Electrical Engineering from the University of Twente, the Netherlands in 2004 and her Bachelor's degree in Engineering (specializing in Electronics and Communication) from the University of Madras, India in 2000. Her research interests include location sensing systems, localization algorithms, ubiquitous computing, sensor networks, SLAM methods, sensor fusion, and evaluation of location sensing technologies and algorithms. Kavitha can be contacted at k.muthukrishnan@tudelft.nl.

**Victor W. Pickard** is an assistant professor in the Department of Media, Culture, and Communication at the Steinhardt School of New York University. He received his doctorate from the Institute of Communications Research at the University of Illinois. His research explores the intersections of U.S. and global media activism and politics, media history, democratic theory, and communications policy and has been published in over two dozen scholarly journal articles, essays, and book chapters. He is currently finishing a book on the history and future of news media. His e-mail address is vwp201@nyu.edu.

**Catherine Tucker** is the Douglas Drane Career Development Professor in IT and management and assistant professor of marketing at MIT Sloan School of Management. She is interested in understanding how networks, privacy concerns, and regulation affect marketing outcomes. She received an undergraduate degree in politics, philosophy, and economics from Oxford University and a Ph.D. in economics from Stanford University.

**Xinyuan Wang** is an associate professor in the Computer Science Department at George Mason University. He received his Ph.D. in Computer Science from North Carolina State University in 2004. His main research interests are around computer network and system security including malware analysis and defense, attack attribution, anonymity and privacy, VoIP security, digital forensics. He has developed the first interpacket timing based packet flow watermarking scheme that is provably robust against timing perturbation. He has first demonstrated that it is feasible to track encrypted, anonymous peer-to-peer VoIP calls on the Internet. In his later work, he has demonstrated the fundamental limitations of existing low-latency anonymous communication systems in the presence of timing attack and developed the first practical attack that has "penetrated" the Total Net Shield—the "ultimate solution in online identity protection" of www.anonymizer.com with less than 11 min worth of Internet traffic. He is a recipient of the 2009 NSF Faculty Early Career Development (CAREER) Award. He may be contacted through the following e-mail address: xwangc@gmu.edu.

**Ruishan Zhang** received his Ph.D. in Computer Science and Engineering from Shanghai Jiaotong University for his dissertation on "Security in Mobile *Ad Hoc* Networks" in 2006. He spent 1½ years as a postdoctoral researcher at George Mason University, investigating the security of the SIP protocol and deployed SIP-based VoIP systems. Then he worked at Helsinki Institute for Information Technology until December 2009, focusing on VoIP spam prevention and P2P SIP security. Currently, his research interests include VoIP security, fuzz testing, reverse engineering, 3G network security, and peer-to-peer network security. He may be contacted through the following e-mail address: zhangruishan@gmail.com.

# Preface

Welcome to Volume 81 of the *Advances in Computers*. This series, continuously published since 1960, is entering its sixth decade of publication, and it is the oldest series covering the development of the computer industry. Today there is no doubt that the dominant force in computing is the Internet; therefore, the theme of this volume is "the Internet and mobile technology." Whereas the design goal for the original ARPANET in the 1960s was to be able to reliably link together computers at various locations, this concept has evolved to where the computer-to-computer connection is taken for granted, and the current goals are to free the user from being tied down to a specific location. Therefore, mobility is a current research topic that has led to an explosion of mobile computing devices. We no longer have cellular telephones, but instead have small mobile computers that are able to communicate via telephony. This leads to numerous security and related issues to provide the reliability and integrity needed in today's world. In this volume, we present six chapters that address various aspects of these issues.

In the first chapter, "VoIP Security: Vulnerabilities, Exploits, and Defenses" by XinyuanWang and Ruishan Zhang, the authors discuss telephony via Voice over IP (VOIP). Rather than having a fixed wire connecting a telephone to the central switching office, VOIP works by using the Internet to send voice packets on the Internet along with assorted other Internet traffic such as e-mail, video, or Web pages. But if voice is carried along as digital packets, what level of security must there be to avoid the issues that plague other Internet traffic, such as spamming, phishing, hijacking, eavesdropping, etc.? In this chapter, the authors explain the general workings of VOIP transmission and then discuss the various strategies for dealing with security problems with this technology.

Yiu-Wing Leung in chapter, "Phone-to-Phone Configuration for Internet Telephony," addresses Internet telephony, the topic of the first chapter, with a different perspective. In the first chapter, the focus is on a communication line from one computer through the Internet to a receiving computer. But people are very mobile. How does one use a mobile telephone to provide VOIP services? One approach is for a service provider (e.g., local telephone company) to provide a local telephone number (a telephone gateway) a mobile phone user can call. At this local telephone number, the service provider connects to the Internet to send the call to a distant location, where it again is sent to a local mobile phone at the distant location. This allows users to use both computer-to-computer communications and mobile phone-to-mobile phone communications (e.g., Skype). The issues of optimizing traffic and minimal costs are the focus of this chapter.

In the third chapter, "SLAM for Pedestrians and Ultrasonic Landmarks in Emergency Response Scenarios," Carl Fischer, Kavitha Muthukrishnan, and Mike Hazas look at the issues in determining location from a mobile device. In particular, they are looking at the needs in emergency situations of determining location where visual clues are missing (such as inside a burning building). While most cellular telephones now contain GPS receivers, "darkness, smoke, fire, power cuts, water, and noise can all prevent a location system from working, and heavy protective clothing, gloves, and facemasks make using a standard mobile computer impossible." In this chapter, they discuss several existing systems for solving this problem, focusing on their simultaneous localization and mapping or SLAM method.

By now everyone is familiar with Bluetooth, that ubiquitous technology that allows one to connect one device to another device over short distances (e.g., microphone and earpiece to cellular phone without need to hold telephone). But what is Bluetooth, how does it work, and more importantly, what security exploits does it permit? In "Feeling Bluetooth—From a Security Perspective" by Paul Braeckel in the fourth chapter, the author discusses Bluetooth and provides insights into the kinds of security risks one has in using this technology.

The fifth chapter is titled "Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide" and is written by Sascha D. Meinrath, James W. Losey, and Victor W. Pickard. One of the side effects of the Internet is that an increasing number of aspects of our daily lives are becoming digital and communicated over the Internet. From telephony (e.g., first two chapters in this volume), GPS (third chapter), wi-fi, radio, picture and video transmission to numerous other technologies, all are vying for space on the network bandwidth. This leads to a congestion problem—who has access to this bandwidth? Do all share equally (e.g., "net neutrality"), or do some applications take precedence over other technologies (e.g., real-time video over e-mail)? Can or should one pay more for better access? These are the questions that this chapter addresses.

In the last chapter, "Online Advertising" by Avi Goldfarb and Catherine Tucker, the authors discuss an important feature of the Internet, one without which the Internet would not have existed, and that is advertising. Running the Internet, supporting ISPs (Internet Service Providers), and paying for the various Web sites and search engines that exist all take money. While some organizations use membership fees to support their activities, advertising has become the dominant method for paying for Internet access. But how does Internet advertising work? Who pays what and why? The general model of how Internet advertising works is the focus of this chapter.

I hope that you find these chapters of use to you. I also want to say that I have enjoyed producing these volumes. I have been series editor of the *Advances in Computers* since 1993, and Volume 81 is the 41st volume I have worked on in 19 years. The 2011 volumes will be my last; however, the series will continue under new competent leadership. I hope that you will continue to find this series of use to you in your work.

Marvin Zelkowitz
College Park, Maryland

# Contents

## VoIP Security: Vulnerabilities, Exploits, and Defenses

**Xinyuan Wang and Ruishan Zhang**

## Phone-to-Phone Configuration for Internet Telephony

**Yiu-Wing Leung**

## SLAM for Pedestrians and Ultrasonic Landmarks in Emergency Response Scenarios

**Carl Fischer, Kavitha Muthukrishnan, and Mike Hazas**

## Feeling Bluetooth: From a Security Perspective

**Paul Braeckel**

## Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide

**Sascha D. Meinrath, James W. Losey, and Victor W. Pickard**

## Online Advertising

### Avi Goldfarb and Catherine Tucker

# VoIP Security: Vulnerabilities, Exploits, and Defenses

XINYUAN WANG

*Department of Computer Science, George Mason University, Fairfax, Virginia, USA*

RUISHAN ZHANG

*Department of Computer Science, George Mason University, Fairfax, Virginia, USA*

**Abstract**

Telephone network is an important part of the critical information infrastructure. Traditional Public Switched Telephony Network (PSTN) has been shown to be reliable and hard to be tampered with by normal people. The general public has put a lot of trust on landline telephone, and they are relying on voice communication for many critical and sensitive information (e.g., emergency 911 calls, calls to financial institutions) exchange.

Voice over IP (VoIP) is an emerging technology that allows voice calls to be carried over the public Internet instead of traditional PSTN. While more and more voice calls are shifting from PSTN to VoIP, most people are not aware of the security vulnerabilities introduced by VoIP and they keep trusting VoIP the same as traditional PSTN.

In this chapter, we systematically study the security issues of VoIP and present the state of the art of VoIP security. Specifically, we discuss the security requirements of VoIP, people's expectations of VoIP, and existing VoIP security mechanisms. We present the identified vulnerabilities of existing VoIP, known and potential exploits of those VoIP vulnerabilities. We discuss not only the impact on the VoIP infrastructure itself but also the implications to the VoIP users. We discuss the inherent technical challenges and open problems in securing VoIP.

ADVANCES IN COMPUTERS, VOL. 81
ISSN: 0065-2458/DOI: 10.1016/B978-0-12-385514-5.00001-X

# 1. Introduction

Voice over IP (VoIP) is a technology that allows people to make voice phone calls across the public Internet instead of traditional Public Switched Telephony Network (PSTN). VoIP not only makes voice communication cheaper but also enables many functionalities (e.g., free choice of area code, e-mail notification of voice mail) that were not possible in traditional PSTN. In the past 10 years, VoIP has experienced phenomenal growth and more and more voice calls are carried at least partially over the Internet using VoIP technologies. A study by ABI [1] predicted that the number of residential VoIP subscribers worldwide will increase from 38 million in 2006 to more than 267 million by 2012.

One of the most basic and fundamental requirements of any VoIP services is that they must be reliable and trustworthy. When people subscribe or use any VoIP service, they have actually put a lot of implicit trust on it. For example, when people make phone calls, they intuitively trust that their calls will reach the intended callee once they dial the correct phone number and no one but the intended callee will receive their calls. When people talk over the established phone session, they trust that their conversation and any PIN number pressed will reach the intended receiver unaltered. In addition, people would expect that their calls will not be wiretapped without proper legal authorization. Based on this trust, voice communication has been used for exchanging much critical and sensitive information (e.g., emergency 911 calls, calls to customer service of financial institutions). The general public are used to giving out their SSN, credit card number, and PIN when they interact with the interactive voice response (IVR) system before they are connected to a service representative of their financial institution. Furthermore, people are comfortable to give out their credentials (e.g., SSN, account number, authentication code) to the service representative of their financial institution over the phone even if they do not personally know the service representative.

Now suppose a VoIP user Alice is planning to buy a house, and she wants to cash out some of her Google stock options for that. Because of the large amount of money involved, Alice prefers talking to a broker over the phone than using the Web. So she dials the 1-800 number shown in her TD AMERITRADE statement, and left a message asking for a call back since no one is available at the time. A few minutes later, a call with TD AMERITRADE callerID comes in, and a representative named Bob says he is returning the call to Alice. Alice is quite technical savvy, and she insists on getting Bob's extension number and calling him back. After hanging up the incoming call, Alice calls the official number of TD AMRITRADE with Bob's extension. Once Alice reaches Bob again, she feels at ease and requests to exercise 5000 shares of her Google stock options and wire the expected $500,000 profit to her