Computer Communications 68 (2015) 1–3

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Editorial

Security and privacy in unified communications: Challenges and solutions

Unified Communications (UC) merge different communication technologies, types of products, and services, from various manufacturers, operators, and countries, following diverse policies and standards. Specifically, in the context of UC, a range of communication tools are integrated in a way that both corporations and individuals are able to manage all their communications in one entity instead of doing it disjointly. It is therefore said that UC bridges the opening between the various computer related communication technologies and Voice over IP (VoIP). However, this high level of heterogeneity expands the risks related to security and privacy that stakeholders should deal with.

One of the major issues in UC is privacy: as users interact with each other and with multimedia servers, the media traffic that passes through different network elements *e.g.,* proxies and trusted as well as untrusted IP networks, reveals private information about users' identity, behavior, location, etc. Taking the aforementioned heterogeneity into account, access control is another topic that requires special consideration in the context of UC. Also, security assessment in general needs special attention since signaling passes through different service operators, and security decisions are based on information gathering from diverse sources. Last but not least, the Bring-Your-Own-Device (BYOD) philosophy followed by many corporations introduces new entry points and leads to more threats in UC.

This special issue presents selected high-quality papers that cover the domain of security and privacy in UC from different perspectives presenting open issues, algorithms, protocols, policies, frameworks, standards, and UC tailored solutions. We received a total of 54 submissions, out of which eight were selected (acceptance rate 14%) considering their quality and relevance to the topic of the special issue.

1. Location privacy

While location-aware applications offer significant advantages to service providers and their customers, the privacy risks associated with them can withhold their adoption. Calderoni et al. from University of Bologna in Italy and Bournemouth University in UK, proposed the Spatial Bloom Filter in their paper entitled "Location Privacy without Mutual Trust: the Spatial Bloom Filter". This new data structure together with two proposed protocols preserves users' location privacy when they use location-aware services on mobile devices.

2. Privacy in multimedia recommendation systems

Recommendation systems help users of online multimedia delivery systems get meaningful recommendations for other products that might be of interest. The privacy issues behind such systems have been identified and a number of algorithms for privacy protection have been proposed which, however, decrease recommendation accuracy. Feng et al. from Beijing Jiaotong University in China in their paper "Can User Privacy and Recommendation Performance Be Preserved Simultaneously?" proposed a privacy preserving framework which can maintain the accuracy of recommendation systems used on online systems that deliver multimedia services.

3. Privacy on eVoting through VoIP

In online surveys where each new question is determined by the answer given in the previous question, participants' privacy is not protected from snoopers even when answers are encrypted. Vera del Campo et al. from Universitat Politècnica de Catalunya and Scytl in Catalonia proposed in their paper "Private Surveys on VoIP" an eVoting framework that preserves end users' privacy in surveys performed on mobile devices utilizing Voice-over-IP technologies.

4. Security and QoS in UC

Taking into account the heterogeneity observed in UC scenarios, the assessment of security and QoS is difficult and based on partial information. In their paper "Contextualising Heterogeneous Information in Unified Communications with Security Restrictions", Nieto and Lopez from University of Malaga in Spain provide the extension of a model for transforming heterogeneous information into context-based information and a tool for assessing the security and QoS trade-off in UC.

5. Security in CDNs

Content Distribution Networks (CDNs) are networks used for transmitting multimedia streams to end users; their federation into Federated CDNs (FCDNs) involves providers that belong to different domains, making security a challenging issue. Pimentel et al. from Universidade de São Paulo in Brasil, in their paper entitled "OCP: A Protocol for Secure Communication in Federated Content Networks",

http://dx.doi.org/10.1016/j.comcom.2015.08.004

propose a protocol for preventing misuse of FCDN resources. Actually, it is a security mechanism that allows secure signaling among FCDNs, addresses route forgery and conceals network architecture from third parties.

6. Dynamic access control in mobile cloud computing

Traditional access control mechanisms are not sufficient in an environment where UC enable seamless data sharing across heterogeneous networks and devices from anywhere and anytime. Li et al. from City University in UK and University of Padova in Italy, proposed an access control framework for mobile cloud computing in their paper entitled "Robust Access Control Framework for Mobile Cloud Computing Network". This solution is based on the inclusion of dynamic attributes in conventional access control schemes with comparable efficiency.

7. Identity management on cloud-based UC

While UC over the cloud are on the rise, delegating corporate identity information to cloud providers will be a major issue for enterprises. Beltran and Bertin from Orange labs in France, in "Unified Communications as a Service and WebRTC: An Identity-Centric Perspective", tackle the Identity Management (IdM) issues found in UC-as-a-Service (UCaaS). In their paper they review IdM models, identify the relevant requirements for UCaaS, and finally propose a modified version of WebRTC to meet these requirements.

8. Security in BYOD

As the BYOD concept is gaining acceptance in corporate environments, new entry points are created for attackers and security policies need to be adapted to meet the new challenges. In "Corporate Security Solutions for BYOD: A Novel User-Centric and Self-Adaptive System", De las Cuevas et al. from University of Granada in Spain propose an open source system called MUSES for securing BYOD environments. MUSES utilizes machine learning and computational intelligence to establish and improve security rules based on users' behavior.

The aforementioned articles cover a wide range of security and privacy topics in UC. However, the heterogeneity observed in such applications creates an environment where new security challenges will continuously need to be faced. As the convergence of different types of communication means will continue towards UC, we believe that the domains of security and privacy in UC will remain an interesting and important research field.

Georgios Karopoulos is a Scientific Officer at the Critical Infrastructure Protection unit of the European Commission's Joint Research Centre (JRC), in Ispra, Italy. Previously, he was a Postdoctoral Researcher at the Institute of Informatics and Telematics of the Italian National Research Council (IIT-CNR). He holds a Ph.D. in Computer Networks Security, an M.Sc. in Information and Communication Systems Security and a B.Sc. from the department of Information and Communication Systems Engineering, University of the Aegean, Greece. His research interests are focused on critical infrastructure protection, mobile and wireless networks security and privacy, and multimedia security, and he has published in conferences and scientific journals in the above areas. He has been involved in national and EU funded R&D projects in the areas of Information and Communication Systems Security. He is a reviewer of international journals like IEEE Transactions on Systems, Man, and Cybernetics, and Elsevier's Computer Networks (COMNET) and Journal of Network and Computer Applications (JNCA) and has served as a technical program committee member in international conferences in security and networking.

Georgios Portokalidis is an Assistant Professor in the Computer Science Department at Stevens Institute of Technology, in Hoboken, New Jersey. He obtained his doctorate degree in Computer Science from Vrije Universiteit in Amsterdam, while he also holds an M.Sc. from Leiden University and a B.Sc. from University of Crete. His research interests are mainly around the area of systems security, but extend to networking, operating systems, virtualization, and data privacy. His work focuses on improving the security of existing software on commodity systems, and using virtualization to retrofit software with protection mechanisms. More recently, he has been involved with improving software reliability and availability, mobile device security, and privacy issues in mobile devices and the cloud. He has authored numerous papers in high impact conferences, including ACM CCS, ACM EuroSys, Usenix Security, and ACSAC. He has also been involved in several projects funded by the EU, DARPA, IARPA and NSF, and he has received funding through IARPA. He has served in committees of various conferences, including ACSAC, SEC, and EuroSec, while he regularly reviews for journals, like ACM Transactions of Information and System Security, IEEE Transactions on Reliability, etc.

Josep Domingo-Ferrer is a Distinguished Professor of Computer Science and an ICREA-Acadèmia Researcher at Universitat Rovira i Virgili, Tarragona, Catalonia, where he holds the UNESCO Chair in Data Privacy. He received his M.Sc. and Ph.D. degrees in Computer Science from the Autonomous University of Barcelona in 1988 and 1991 (Outstanding Graduation Award). He also holds an M.Sc. in Mathematics. His research interests are in data privacy, data security, statistical disclosure control and cryptographic protocols, with a focus on the conciliation of privacy, security and functionality. He has coauthored five patents and over 350 publications (H-index 43). He has received a Google Faculty Research Award (2014), the ICREA Acadèmia Research Prize (2008 and 2013), and the "Narcís Monturiol" Medal for merit in Science and Technology (2012). He is a fellow of IEEE (2012), and an Elected Member of Academia Europaea (2012) and the International Statistical Institute (2012). He currently coordinates the EU H2020 project "CLARUS" and the "CO-UTILITY" project funded by Templeton World Charity Foundation. He has been the co-ordinator of EU FP5 project CO-ORTHOGONAL and of several Spanish funded and U.S. funded research projects. He has chaired 16 international conferences and has served in the program committee of over 220 conferences on privacy and security. He is a co-Editor-in-Chief of "Transactions on Data Privacy", and an Associate Editor of "IEEE Transactions on Dependable and Secure Computing", "KAIS-Knowledge and Information Systems", "Computer Communications", "Journal of Official Statistics".

Ying-Dar Lin is a Distinguished Professor of Computer Science at National Chiao Tung University (NCTU) in Taiwan. He received his Ph.D. in Computer Science from UCLA in 1993. He served as the CEO of Telecom Technology Center in Taipei during 2010–2011 and a visiting scholar at Cisco Systems in San Jose during 2007–2008. Since 2002, he has been the founder and director of Network Benchmarking Lab (NBL, www.nbl.org.tw), which reviews network products with real traffic. NBL recently became an approved test lab of the Open Networking Foundation (ONF). He also co-founded L7 Networks Inc. in 2002, which was later acquired by D-Link Corp. His research interests include design, analysis, implementation, and benchmarking of network protocols and algorithms, quality of services, network security, deep packet inspection, wireless communications, embedded hardware/software co-design, and recently software defined networking. His work on "multi-hop cellular" was the first along this line, and has been cited over 600 times and standardized into IEEE 802.11 s, IEEE 802.15.5, WiMAX IEEE 802.16j, and 3GPP LTE-Advanced. He is an IEEE Fellow (class of 2013), an IEEE Distinguished Lecturer (2014 & 2015), and a research associate of ONF. He is currently on the Editorial Boards of *IEEE Transactions on Computers, IEEE Computer, IEEE Network, IEEE Communications Magazine - Network Testing Series, IEEE Wireless Communications, IEEE Communications Surveys and Tutorials, IEEE Communications Letters, Computer Communications, Computer Networks, Journal of Network and Computer Applications, and IEICE Transactions on Information and Systems*. He has guest edited several Special Issues in IEEE journals and magazines, and co-chaired symposia at IEEE Globecom'13 and IEEE ICC'15. He published a textbook, *Computer Networks: An Open Source Approach* (www.mhhe.com/lin), with Ren-Hung Hwang and Fred Baker (McGraw-Hill, 2011). It is the first text that interleaves open source implementation examples with protocol design descriptions to bridge the gap between design and implementation.

Dimitris Geneiatakis received a five-year Diploma in Information and Communication Systems Engineering in 2003, and an M.Sc. in Security of Information and Communication Systems in 2005, and a Ph.D. in the field of Information and Communication Systems Security from the Department of Information and Communications Systems Engineering of the University of Aegean, Greece. He has participated in various research programs projects in the area of information systems security. His current research interests are in the areas of security mechanisms in internet telephony, intrusion detection systems, network, and lately in software security. He is an author of more that forty refereed papers in international scientific journals and conference proceedings. Furthermore, he has served as program committee member on several international conferences on Information Systems and I am a reviewer in various well-known scientific journals. Currently, he is a lecturer at the Department of Electrical and Computer Engineering of the Aristotle University of Thessaloniki. Previously, he was a postdoctoral researcher at Joint Research Center of European Commission and at Columbia University under the supervision of Prof. A. Keromytis. In the past he was also a visiting lecturer at the departments of Telecommunications Science and Technology and Digital Systems in the University of Peloponnese and Piraeus correspondingly.

Georgios Kambourakis received the Diploma in Applied Informatics from the Athens University of Economics and Business and the Ph.D. in Information and Communication Systems Engineering from the Department of Information and Communications Systems Engineering of the University of the Aegean. He also holds a Master of Education degree from the Hellenic Open University. Currently, Dr. Kambourakis is an Assistant Professor at the Department of Information and Communication Systems Engineering, University of the Aegean, Greece. His research interests are in the fields of mobile and wireless networks security and privacy, VoIP security, Public Key Infrastructure, DNS security, and mLearning and he has more than 100 publications in the above areas. He has been involved in several national and EU funded R&D projects in the areas of Information and Communication Systems Security. He is a reviewer for a plethora of IEEE and other international journals and has served as a technical program committee member for more than 150 international conferences in security and networking.

Georgios Karopoulos*
Georgios Portokalidis
Josep Domingo-Ferrer
Ying-Dar Lin
Dimitris Geneiatakis
Georgios Kambourakis
Anthony van Leeuwenhoeksweg 56a, 2408 AN, Alphen a/d Rijn, The Netherlands

* Corresponding author. Tel.: +31 172 466200; fax: +31 172 466222.