Because it’s increasingly difficult if not impossible to define the perimeter that separates the trusted inside from the untrusted outside, many security and privacy mechanisms no longer work in an online world.

Due to the amazing advances in information and communications technologies, we’re heading for an online world in which convenience goods have unprecedented computing power and are permanently connected to the Internet or stored in the cloud.

The Internet is everywhere, and now people are talking about the Internet of Things (IoT). Look at your own belongings; it’s likely that you carry around at least one or possibly several handheld devices such as smartphones that are permanently connected to the Internet. Each device has computing power that was sufficient for navigating a rocket to the moon 40 years ago. Now we use that power to download and play songs and movies, access social media such as Facebook or Twitter, run e-mail or messenger software, or access any of the other myriad apps people have created recently.

A NEW APPROACH TO SECURITY AND PRIVACY

The online world not only changes our way of living, but also the way we approach security and privacy. In particular, most security mechanisms we rely on in our daily lives are perimeter-oriented, meaning that they basically protect the edges of a particular domain. However, many of these mechanisms no longer work in an online world, mainly because it’s increasingly difficult if not impossible to define the perimeter and separate the trusted inside from the untrusted outside.

A mobile user typically requires remote access from a handheld device even if it’s located outside the corporate network. In some cases, the user employs a device to access the network, a situation the community refers to as BYOD (bring your own device). BYOD provides some unique challenges for a company’s chief information security officer. The bottom line is that perimeters need to be permeable to some extent, and many entities must exist on either side of a perimeter. Deperimeterization occurs naturally, and this not only poses new security challenges but also raises privacy concerns.

IN THIS ISSUE

There’s a large gap between the general knowledge and wisdom pertaining to computer and information security, which focuses on perimeter protection, and what’s really needed in practice. That is where the content in this special issue comes into play. Comprising six contributions, the content addresses some of the security and privacy challenges that apply to the online world.

In “Malicious and Spam Posts in Online Social Networks,” Saeed Abu-Nimeh, Thomas M. Chen, and Omar Alzubi report on an empirical analysis of Facebook posts that leads to the conclusions that an overwhelmingly large fraction of posts is spam, and only a much smaller fraction is malicious. This is good news, and it contradicts the publications that elaborate on the intrinsic dangerousness of social media in general, and social media posts in particular.
In “Security Vulnerabilities in the Same-Origin Policy: Implications and Alternatives,” Hossein Saiedian and Dan S. Broyles assess the effectiveness of the same-origin policy (SOP) that is at the core of many Internet and Web security technologies in use today. Their assessment is not particularly encouraging, but they also propose ways for the SOP to evolve in the future.

“Secure Collaborative Supply-Chain Management” by Florian Kerschbaum and coauthors demonstrates the practical applicability of secure multiparty computation to business collaboration. In particular, the authors report the key findings of the European research project SecureSCM, which applies secure computation protocols in the supply-chain management realm.

In “The Final Frontier: Confidentiality and Privacy in the Cloud,” Francisco Rocha, Salvador Abreu, and Miguel Correia focus on the confidentiality and privacy challenges of cloud computing, assuming, for example, that the cloud operator might have malicious employees operating as insiders. They also offer proposals to address these issues.

“Securing the Internet of Things” by Rodrigo Roman, Pablo Najera, and Javier Lopez provides an overview of the security challenges and protection mechanisms related to the IoT. As our world is heading in this direction, properly understanding and addressing the challenges and coming up with appropriate protection mechanisms is key for the IoT’s future deployment.

In their article titled “Sticky Policies: An Approach for Managing Privacy across Multiple Parties,” Siani Pearson and Marco Casassa Mont not only address the practically relevant question of how to handle privacy management across multiple parties, they also propose a solution.

The contributions selected for inclusion in this special issue are intended to provide a comprehensive picture of some of the most important topics related to security and privacy in the online world. We hope that some readers will become interested in directing their research activities to resolving the problems concerning these topics. Computer is strongly committed to providing additional coverage related to ongoing developments in the area of online security and privacy in future issues.

Rolf Oppliger, the founder and owner of eSECURITY Technologies, is an adjunct professor of computer science at the University of Zurich. Contact him at rolf.oppliger@esecurity.ch.

Selected CS articles and columns are available for free at http://ComputingNow.computer.org.