Aalto University

Securing Cloud-Assisted Services and IoT Systems

Professor. : N. Asokan (Aalto University & University of Helsinki)

Date & Time: February 21, 2017 11 am.

Venue: Faculty of Engineering and Technology Auditorium, JMI

Speaker Profile:

Professor Asokan is a researcher, specialising in systems security. He presently co-leads Secure Systems Group at Aalto University. He also directs the Helsinki-Aalto Center for Information Security (HAIC) and Intel Collaborative Research Institute for Secure Computing in Finland.

He is also a renowned professor at the Department of Computer Science at Aalto University and Department of Computer Science, University of Helsinki.

Previously he has spent his inestimable 17 years in industrial research at the IBM Zurich Research Laboratory (ZRL) and then at Nokia Research Center (NRC). His research interests chiefly focuses on understanding how to build systems that are simultaneously secure, easy to use and inexpensive to deploy. he has initiated and led several projects , co-designed 'simple pairing system' for bluetooth devices, 'generic authentication architecture'. At Zurich, he designed and implemented ' generic payment service framework' for 'Semper Project'.

He has received his former education at IIT Kharagpur , Syracause university and University of Waterloo.

Abstract:

Cloud services covers a wide range of resources that a service provider delivers to customers via the internet. Customers can provision services on an on-demand basis and shut them down when no longer necessary. On-demand computing services can save large enterprises and small businesses a lot of money, but security and regulatory compliance become difficult. He emphasised that these systems may present a variety of potential security risks that could

be exploited to harm consumers. He discussed the privacy concerns that arise and how we can address them effectively.

What is cloud service?

A cloud service is any service made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers. Cloud services are designed to provide easy, scalable access to applications, resources and services, and are fully managed by a cloud services provider.

What is the "Internet of Things"?

IoT can be described as the connection of physical objects to the Internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing. The IoT includes consumer-facing devices, as well as products and services that are not consumer-facing. The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices and everyday things that utilize embedded technology to communicate and interact with the external environment, all via the Internet.

IoT Examples

Examples of objects that can fall into the scope of Internet of Things include connected security systems, thermostats, cars, electronic appliances, lights in household and commercial environments, alarm clocks, speaker systems, vending machines and more. Businesses can leverage IoT applications to automate safety tasks (for example, notify authorities when a fire extinguisher in the building is blocked) to performing real-world A/B testing using networked cameras and sensors to detect how customers engage with products.

Risks

Despite numerous benefits these systems create a number of security and privacy risks.

1. Data Breaches

He cited that the largest breaches haven't involved any such advanced techniques, which remain for the most part lab experiments. But the possibility still acts as a brake on what is looking like broad enterprise adoption of cloud computing. Clouds represent concentrations of corporate applications and data, and if any intruder penetrated far enough, who knows how many sensitive pieces of information will be exposed.

Unfortunately, while data loss and data leakage are both serious threats to cloud computing, the measures you put in place to mitigate one of these threats can exacerbate the other. Encryption protects data at rest, but lose the encryption key and you've lost the data. The cloud routinely makes copies of data to prevent its loss due to an unexpected die off of a server. The more copies, the more exposure you have to breaches.

2. Data Loss

A data breach is the result of a malicious and probably intrusive action. Data loss may occur when a disk drive dies without its owner having created a backup. It occurs when the owner of encrypted data loses the key that unlocks it. And a data loss could occur intentionally in the event of a malicious attack.

3. Account Or Service Traffic Hijacking

Account hijacking sounds too elementary to be a concern in the cloud, but it is a problem. Phishing, exploitation of software vulnerabilities such as buffer overflow attacks, and loss of passwords and credentials can all lead to the loss of control over a user account. An intruder with control over a user account can eavesdrop on transactions, manipulate data, provide false and business-damaging responses to customers, and redirect customers to a competitor's site or inappropriate sites.

If your account in the cloud is hijacked, it can be used as a base by an attacker to use the power of your reputation to enhance himself at your expense.

If credentials are stolen, the wrong party has access to an individual's accounts and systems. A service hijacking lets an intruder into critical areas of a deployed service with the possibility of "compromising the confidentiality, integrity, and availability" of those services, the report said.

4.InsecureAPIs

The cloud era has brought about the contradiction of trying to make services available to millions while limiting any damage all these largely anonymous users might do to the service. The answer has been a public facing application programming interface, or API, that defines how a third party connects an application to the service and providing verification that the third party producing the application is who he says he is.

His recommendations for best practices

Data security

Participants discussed a number of specific security best practices. He encouraged companies to consider these practices:

First companies should implement security by design by buikding security into their devices at the outset , rather than as an afterthought.in addition. Companies should do a privacy or security risk assessment , consciously considering the risks presented by collection and retention of cosumer information.

Secondly , companies must ensure that their personnel practices should promote good security. Companies should also train their employees about good security practices recognizing that technical expertise does not necessarily equate to security expertise.

Data minimization

Companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. Data minimization can help guard against two privacy related risks. Companies should also consider if it could offer same features while collecting less information.

With these recommendations on data minimization, he is mindful of the need to balance future.

Data Sharing

Prof. offerered tips on how to practice defense in depth against hijackings, but the must-do points are to prohibit the sharing of account credentials between users, including trusted business partners; and to implement strong two-factor authentication techniques "where possible."

Conclusion

The cloud services and internet of things presents numerous benefits to consumers and has potential to change the ways that consumers interact with technology in fundamental ways. In future these systems are likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective these bodies pose particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely want privacy. The designated commission will continue to enforce laws, educate consumers and businesses, and engage with industry and academics to promote appropriate security and privacy protections. At the same time, he urged further self-regulatory efforts on IoT, along with enactment of data security and broad based privacy legislation.