Research of the issue

The Garbled Computer: Towards Computing without Seeing

By Qutaibah Malluhi

Our increased reliance on the cyber infrastructure has, without a doubt, made cyber security a top priority worldwide. Recent high-profile breaches, the blockade against Qatar, and the determination to protect Qatar's valuable physical infrastructure has made cyber security a national security issue, and a main grand challenge for the country.

This project offers a novel solution to common security and privacy problems such as:

· How can we build secure and privacy preserving clouds?
· How can computers work on encrypted data?
· How can I prevent Google from seeing my emails?
· How can I prevent Apple from seeing my iCloud pictures?
· How can a computer run my code without seeing my program or my data?

This project develops a new secure computer model called the Garbled Computer (GC). The project develops novel technologies that tackle challenging cyber security concerns through enabling a new model for secure storage and computation that considers the host machine untrusted. Traditional security models and approaches that are based on the assumption that the operating system and the application are trusted are no longer valid. The proliferation of cloud services is making that model less realistic. Moreover, the operating system and applications are vulnerable because they expose a large attack surface. Furthermore, in today's hostile cyber environment, the operating system and applications can themselves be the source of an attack. In this project, our model is quite different as we consider the host machine as well as the operating system untrusted.