Detecting malicious files uploaded to cloud services

August 12 2015

Credit: Wikipedia

A powerful new computer security tool, called XDet, can detect malicious files being uploaded to a cloud computing service is reported this month in the International Journal of Space-Based and Situated Computing by researchers from Manchester Metropolitan University and Nottingham Trent University, UK.

Rob Hegarty (MMU) and John Haggerty (NTU) explain how cloud computing has become the predominant paradigm for organisational infrastructure development because of its great flexibility and scalability. As with any computer system, however, there are concerns regarding security and privacy. Firewalls and intrusion detection systems can do only so much to block hackers and malicious software but do not address the problem of malware being uploaded to the servers by legitimate users whose computers have been compromised or hackers, for instance. Moreover, they cannot detect and block undesirable downloads by such users either.

"The XDet approach has been developed to identify data leakage from cloud networks...and complements existing approaches, such as firewalls and IDS," the team says. The system works by generating a signature from private files and storing it for subsequent comparison with signatures derived from files being transferred across the network. "In this way, unauthorised uploads or downloads of potentially confidential data may be detected and prevented," the team explains.

The XDet software is placed between the cloud server and distributed file storage rather than on the perimeter of the cloud network as might be the case with other security measures, the team points out. This has three main advantages. First, it is itself thus protected by perimeter-based security devices, such as firewalls and IDS. Secondly, it is scalable and utilises the collaborative nature of cloud-based system to share security information. Thirdly, the cloud provider can employ network-based encryption to protect data in transit.

The researchers have carried out successful tests on live data on a cloud server demonstrate the potential of XDet to detect the illicit extraction of information.

More information: "Extrusion detection of illegal files in cloud-based systems." *International Journal of Space-Based and Situated Computing*. Volume 5, Issue 3. DOI: 10.1504/IJSSC.2015.070954

Provided by Inderscience