Summary

A new technology has been developed for protecting the intellectual property of copyright holders. This technology allows for the simple detection of emulated or monitored environments, such that a computer program running the emulated environment can modify its operation in order to protect digital content. The technology is generic in nature and requires no prior knowledge of the emulated environment. Furthermore, the approach is not significantly weakened if an attacker knows the method of protection employed.

The Technology

Digital content is convenient and reliable. It suffers no degradation upon transmittal and can be shared worldwide with just a few “point and click” operations. As such, it is a medium of considerable power and flexibility. Unfortunately, this same technology can be used to pirate digital information and steal intellectual property.

One of the most powerful techniques available to an attacker is the ability to run a computer program in a synthetic environment. In such an environment, the program will reveal its secrets, allowing an attacker to understand its control and structure or to steal otherwise protected content. Furthermore, it is difficult for a program that is in such a synthetic environment to determine whether it is being monitored and should terminate or otherwise modify its operation, as all program inputs are directly controlled by the attacker.

Our technology provides a method of using timing information for detection of such simulated environments. In particular, we do not use changes in the magnitude of particular operations, but in the variation of these magnitudes. By studying a “real” system, a fingerprint of timing variations can be extracted. If this changes, the program can be terminated or otherwise vary in operation. Another possibility is to decrypt content using a decryption key derived from the statistical properties of the timing of the system. This approach allows for digital content to only be decrypted on a particular system with no requirement for an external keyserver.

The underlying idea is both simple and powerful. When a computer program executes a system call, the exact time taken for that call to complete will vary based upon many different factors. Hardware interrupts, process and thread scheduling, and context switches can all impact the absolute time for call completion. Furthermore, if a call is repeated many times on a particular operating system, a characteristic pattern of call timings can be built up. Certain features of this pattern are not greatly affected by changes to CPU load or memory utilization. These features can then be used either to derive a decryption key for continued program operation or to otherwise modify computer operation.

Corporate Research and Technology Transfer
Florida Institute of Technology
150 W. University Blvd.
Melbourne, FL 32901
Phone: (321) 674-8960 | Fax: (321) 674-8969

Inventor: Richard Ford
Contact: (321) 674-7473
E-mail: rford@fit.edu