



FOR IMMEDIATE RELEASE:

CONTACT: I. Vanessa Boyd
Itillious, Inc.
(770) 481-0092 or vboyd@itillious.com
www.itillious.com

Itillious Attack Modeling Reveals Application Security Holes

Atlanta, Georgia, August 6, 2002 —Web-based applications that allow online shopping and account access are increasing in popularity as sales and communication channels. Businesses who embrace them face new risks to the security of their vendor and customer information databases. A breach of application or database security can do serious damage to customer relations and the bottom line. Itillious Attack Modeling (*IAM*) enables companies to ensure the security of their applications and mission-critical databases by identifying both real and potential vulnerabilities and providing practical, cost-effective solutions to reduce and manage risks.

“CEOs lose sleep because their application could be responsible for betraying private customer information, or for decreasing the company’s revenue by allowing purchase information to be altered by hackers,” notes Dave Fentress, President and CEO of Itillious. “The presence of the “lock” at the bottom of the browser doesn’t necessarily mean the application or data is completely safe. Studies continue to show that web application security is the weakest link in enterprise IT security. An IAM application assessment helps a corporation understand its vulnerabilities and take appropriate steps to reduce application security risks. ”

And CEOs have a good reason to worry. According to a recent article in CNET News.com, “...such computer-related crimes are estimated to cost U.S. corporations and consumers as much as \$11 billion per year.” Web-based applications are easy to create and alter using simple scripting languages. Web developers strive for ease-of-use and convenience for the customer with security often being the last consideration for these mission-critical programs.

Itillious Attack Modeling (*IAM*) provides both automated and manual reviews of the application and the environment in which it is developed and deployed. The automated assessment provides breadth of coverage for potential security risks; the manual assessment complements automation by providing depth of coverage. The manual examination of the business use cases and processes that drive development is necessary to ensure that an assessment covers all aspects of the application.

The first step of the process is to create an Attack Path Map, which charts the course of how a user accesses information using the application. Step two is Attack Tree Modeling, which documents possible scenarios of application penetration based on the Attack Path Map. Finally, Vulnerability Verification is performed as a “sanity check” to predict the likelihood of a given application breach. This three-phase approach ensures that the recommendations resulting from the Itillious Attack Modeling process are realistic, practical, and thorough.

Founded in 2001 and headquartered in Atlanta, GA, Itillious provides practical information security solutions to clients in a wide range of industries from mid-size companies to the Fortune 500. Itillious provides an array of services from high-level policy development to technical network and application assessments. The Itillious *IAM* Application Assessment offers significant value to clients by identifying application risks and developing solutions to reduce application security risk and increase customer trust. The *IRIS*® web-based Security Portal provides an effective communication and training mechanism for clients' intranet environment. *IRIS*® provides a *one-stop shop* for an organization's policies, procedures, and security awareness needs. For more information about Itillious Attack Modeling or Itillious, Inc., please contact I. Vanessa Boyd at (770) 481-0092 or vboyd@itillious.com, or Karen Morrione at 770-609-2664 or karen@working-media.com www.itillious.com

###