



Blackboard Statement on Client System Security

On April 12, 2003, Blackboard pursued legal action against two individuals in order to protect the privacy and security rights of our clients as well as Blackboard's own intellectual property rights. Blackboard took this action in response to individuals who are promoting methods to dismantle secure hardware installations by vandalizing and gaining access to wiring of Blackboard Transaction Systems™. Blackboard's action was not taken to repress the free discussion of any perceived hardware or software security flaws within Blackboard products.

By taking legal action, Blackboard is making a very public statement about the facts related to illegal activities to be promoted by these two individuals and how those activities are detrimental to the entire Higher Education community utilizing these systems. Our action was taken over the weekend prior to presentation at the InterzOne II conference in Atlanta, GA. It is important to note that the Court orders pertain only to the illegal activities and information that these individuals intended to present and did not pertain to InterzOne II or its conference organizers.

As part of our legal actions, Blackboard secured a Temporary Restraining Order issued by the Superior Court of DeKalb County, Georgia prohibiting these individuals from publicly disseminating certain information at the InterzOne II conference in Atlanta, GA. A preliminary hearing was originally set for April 16, 2003, but these individuals, through their lawyer, agreed to an extension of the Temporary Restraining Order's restrictions, without modification of any kind, and asked the Court to postpone that hearing for at least 45 days.

Blackboard recognizes that the hacker community plays an integral role in assisting technology companies in improving their offerings, most notably around security. Blackboard values this and in fact counts on it as a symbiotic relationship. For example, last year Blackboard worked closely with the hacker community to successfully address a security opening in one of the supported Operating Systems on which Blackboard software products operate. Blackboard expects that this type of collaboration and partnership will continue on an ongoing basis.

The events which prompted Blackboard's action constitute a very different situation. One of these individuals, who has worked as a consultant for one of our competitors, physically dismantled hardware components owned by a higher education institution without the institution's knowledge or permission, and detailed the process and information gathered. It was this activity and experience that these individuals intended to relate at the InterzOne II event for the sole purpose of enabling a select group of individuals to falsify security events and financial transactions, putting the general public and approximately 275 academic institutions in potential jeopardy. It is this harm, coupled with the safety of these academic institutions and their constituents (primarily, students and faculty) that mandated Blackboard take a very careful and measured stance and a difficult but required position to protect its clients.

Background on Transaction Systems & Current Security Practices

On college campuses, Blackboard (as well as other vendors) sells and install hardware and software to enable financial transactions at point of sale devices – vending machines, copiers, laundry machines – so that students can use debit cards to purchase products and services. The physical devices are secured in various vending and public areas. Historically, Blackboard's solution and other industry solutions utilized proprietary wiring on campuses. The routing of transactions was secured through the physical security of these networks. The transactions themselves are secured unless the hardware systems involved are physically compromised (i.e. breaking into a school's control box on campus).

April 16, 2003



Blackboard Statement on Client System Security

The Blackboard Transaction System is a secure and stable system and has been for more than 15 years. Any perceived reader security issues appear to arise only in the context of physical vandalism and/or physical damage to hardware and/or communication connections. This is not hacking; this is vandalism.

In recent years, Blackboard has taken the initiative to design, develop, and manufacture new devices which ensure that transactions travel over public and private IP-based networks. In this environment, Blackboard embraces even more stringent encryption technologies for each individual transaction. We are taking these developments even further with the release of point of sale devices that ensure a transaction is encrypted from the point of the card's swipe through the reader device.

The industry as a whole has utilized proprietary networks (such as RS-485) for many years. Blackboard has, we believe, a leadership position in developing new-generation, IP-based, and encrypted communications. Our client base as a whole has welcomed these developments and has been leading the deployment of these newer generations of technologies.

Background on Blackboard Learning System & Portal System Security Practices

Blackboard conducts internal security audits as part of the comprehensive Quality Assurance process rolled into each release of the Blackboard Learning System and the Blackboard Community Portal System. In addition, Blackboard supports industry-standard protocols such as 128-bit SSL (Secure Sockets Layer), ensuring that sensitive data is safe, secure, and available only to the proper users within the Blackboard Learning and Community Portal Systems. With the recent proliferation of worms and viruses affecting businesses and corporations alike, Blackboard now aggressively tests all security-related patches and updates issued by third-party vendors (such as Microsoft, Sun, Redhat, Oracle) as soon as they are released for compatibility with the Blackboard Learning and Community Portal Systems.

Lastly, Blackboard routinely works with members of the client community in assessing security concerns and actively participating in the diagnosis as well as resolution of any security-related matters. As a preventative measure, Blackboard has established formal relationships with security centers such as the CERT[®] Coordination Center, positioning Blackboard to react quickly and efficiently to any security incidents that may surface.

Further Questions

If you have additional questions please contact:

Michael J. Stanton
Senior Director, Corporate Communications
Blackboard Inc.
Phone: +1-202-463-4860
Email: mstanton@blackboard.com

April 16, 2003