User Behavior Anomaly Detection in Online Banking

The Need
According to the Federal Financial Institutions Examination Council, the "Authentication in an Internet Banking Environment" regulation requires all U.S financial institutions to deploy web user behavior anomaly detection systems for online banking applications starting January 2012. The FFIEC describes these systems as:

"fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response"

The need for such systems is further explained:

"Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer’s established patterns of behavior."

Crimeware
Authentication is futile when dealing with modern menaces such as Man-In-The-Browser Trojans. Crimeware now bypasses existing authentication solutions by piggybacking legitimate, unsuspecting web users. The Trojan allows the end client to use whatever method of authentication his bank has provided. Then, when the user has entered his online banking account, the Trojan and the user go their separate ways. While the legitimate user checks his balance, for instance, the Trojan is busy transferring money into a different bank account, trading stocks and retrieving confidential information out of the victim's account. Monitoring the device's origin and reputation also fails in this case. The victim's PC has never been reported as part of any crime ring or bot-net. In fact, this criminal act might only occur once, so the window of opportunity to catch the crime is very short.

The Hybrid Advantage
Hybrid Telepath uses 3rd generation Web fraud detection technology. Based on advanced artificial intelligence algorithms combined with behavioral rules, Telepath keeps up with 0-day threats regardless of the technology used on client side. Telepath requires no software updates. In fact, the more unknown the threat is, the faster Telepath detects it and reacts. It is an auto-deductive solution, able to profile end user behavior rapidly. It detects users by name and behavior, session and origin. Telepath studies the normal business logic of each online work-flow process along with its user population action trends. Telepath automatically creates normal behavior models for different user groups as well as individual user names. This enables Telepath to provide a protection umbrella against various threats including, but not limited to:

1. Trojan horses
2. Business logic manipulation
3. Bot-nets
4. Identity theft & account takeover
5. Fraudulent user behavior

Telepath is a non-intrusive network appliance acting as a sniffer. It provides real-time intelligence and risk score regarding all Web-bound transactions. It complements existing systems such as: Web Application Firewalls, Authentication systems, SSL extenders, Log-based data-mining and Business Intelligence. Telepath assists in fraud investigations and provides unmatched visibility into suspicious web sessions at the business logic layer.