

ACI's risk management software protects more than 150 financial institutions worldwide.

**Faisal Azam**  
Vice President Architecture, Boston, U.S.A.



# Securing online banking

Fraud mitigation strategies to protect customers from man-in-the-browser attacks

Online banking grew by 50 percent in 2009. As impressive as this stat is, it is dwarfed by the growth rate of banking Trojans and password-stealing malware, which was estimated to grow by over 180 percent in the same time period. In fact, intelligence agencies report that the speed and sophistication of such malware is outpacing most anti-virus and firewall updates.<sup>1</sup>

## —> Malware such as banking Trojans, password stealing viruses and downloader applications has infected over 50 percent of corporate and consumer PCs in more than 100 countries as of June 2009<sup>2</sup>.

This will not be news to anti-fraud professionals at financial institutions, but it definitely is a significant challenge if they have solely relied on user authentication measures to secure the “front door” of an online banking website. These Trojans can infect a user’s PC, and then launch man-in-the-browser attacks that can completely circumvent even the strongest user authentication measures.

Once inside, fraudsters can do significant damage to both consumer and corporate online banking accounts – for example by wiring money externally or transferring funds via automated clearing house (ACH) or bill payment systems.

### **So, what can be done to address this issue?**

Just as door locks and chains are the front-line defense in keeping some crooks from breaking in to a house, they won’t keep the most sophisticated criminals away. Similarly, as motion detectors and alarms can more effectively secure a house, financial institutions can utilize “motion detectors” to more effectively secure consumer and corporate online banking systems to minimize the impact of man-in-the-browser attacks.

### **Anatomy of a man-in-the-browser attack**

What exactly are man-in-the-browser attacks? As the name suggests, a Trojan embeds itself in an internet browser application on a user’s PC. When a user logs onto specific online banking sites the Trojan is activated and intercepts and manipulates data as it is being communicated from the legitimate user’s PC to an online banking system. These attacks are designed to circumvent even the strongest user authentication techniques.

### **Limitations to traditional online banking fraud management strategies**

In the past, many banks have invested in multifactor authentication to try to ensure that only legitimate users access online banking systems. Although costly and somewhat inconvenient to a customer, user authentication techniques did effectively secure the door of most online banking sites – until now.

Likewise, many banks invested in systems that provide IP address intelligence for online banking transactions. Although IP address intelligence does effectively detect account takeover fraud scenarios where fraudsters have utilized phishing techniques and malware to obtain login credentials of legitimate users, it falls short at detecting man-in-the-browser attacks – which take place without affecting the legitimate device and IP address data sent through with the transaction.

### **Not an isolated problem**

The increase in quantity and complexity of malware is a growing trend for the industry. Malware such as banking Trojans, password stealing viruses and downloader applications has infected over 50 percent of corporate and consumer PCs in more than 100 countries as of June 2009.<sup>2</sup>

Email-born malware continues to slip past traditional anti-virus and anti-spam protections. According to the Q3 2009 CommTouch Internet Threats Trends Report, the amount of malware that slipped past normal defenses peaked every 11 to 13 days. Malware writers are beginning to distribute short, massive outbreaks of different variants of a single piece of malicious code, and these variants are not immediately blocked by most anti-virus programs. When a single malware appears with multiple variants, many traditional anti-virus solutions may have difficulty identifying and blocking them quickly.<sup>3</sup>

Additionally, the increasing use of social networking websites has contributed to the proliferation of man-in-the-browser attacks. When an avid social networker’s computer becomes infected with a virus, it can wait until the user logs into the social networking site, where it will raid the user’s “friends” list. It then sends an email to each of them to click on a link to view a photo or video. In this case those “friends” recognize the name of the sender and click on the link, and in doing so their computer can become infected with a man-in-the-browser Trojan.

### Threat for both retail and corporate banking sites

Man-in-the-browser attacks aren't exclusive to retail banking operations. Both retail and wholesale banking customers are at risk. In recent months the FBI issued warnings to small and medium businesses, municipal governments and school districts about an increase in fraud involving the exploitation of valid online banking credentials.<sup>4</sup>

Since man-in-the-browser Trojans neutralize the tighter user authentication measures that wholesale banking sites typically have in place – the larger account balances, payment size and wire activity associated with corporate online banking sites have made them a huge target of fraudsters.

### Mitigation strategies: event monitoring and customer behavioral profiling

So, what can banks and financial institutions do to protect their customers from the impact of man-in-the-browser attacks?

Customer authentication measures fall short in this scenario, so instead financial institutions can mitigate their risk by gaining a better understanding of the activity occurring within the online banking session to determine if it fits the established profile of the genuine customer.

A layered approach to online banking fraud monitoring – one that analyzes the login event, the outgoing transaction and risky sequences of events – best positions a financial institution to minimize online banking fraud. All customer interactions can be categorized into event classes that incorporate both monetary and non-monetary actions. These are as follows:

- **Payment events** – Financial transactions such as funds transfers and bill payments
- **Login events** – IP address and session ID profiling
- **Password events** – Changes in logon passwords
- **Profile events** – Changes to customer demographic information (e.g., addresses)
- **Payee events** – Changes to external payee account details
- **Navigation events** – Changes to how a customer navigates an online internet portal

## The basic flow of a man-in-the-browser attack

**Step 1:** Fraudster writes malicious code (often hidden in email spam scams, such as fake news stories, popular videos, links to greeting cards, etc.), which infects account holders' computers with a Trojan capable of executing man-in-the-browser attacks.

**Step 2:** Legitimate users log into their online banking site – usually by entering single or two-factor authentication requirements.

**Step 3:** Upon a successful log-in, the Trojan activates.

**Step 4:** The Trojan intercepts data as it is passed from the user's PC to the online banking application. The Trojan manipulates the destination account information so the funds end up in mule accounts. Often amounts are also changed so more funds are moved than the PC user requested.

**Step 5:** In some cases another level of authentication is required to confirm a transaction – especially with commercial online banking systems. In this case the Trojan alters the page being displayed to the legitimate user, showing the details they originally entered – where the legitimate user will provide the additional authentication necessary to complete the transaction.

In isolation, one of these events may not indicate fraudulent activity. When combined, however, they predict strong patterns of criminal intent.

Genuine customers tend to make transfers and bill payments to the same accounts and of fairly consistent amounts. Alternatively, fraudsters will transfer money to an account or biller that the genuine customer has never used, often for a much greater value than normal. Account profiling is a technique that enables institutions to cross-reference all external accounts with which a customer has transacted in the last 12 months against each new transfer. When a transfer occurs to an account the customer has never used before, the institution should analyze that transaction in greater detail.



When high-risk activity is detected, action can be taken in real time or near-real time to stop the transfer of funds from the customer's account, or to contact the customer to confirm that the transaction is genuine. For example, a major bank in the U.K. contacts the customer by phone when a new payee is created, and provides a verification code that must be entered onto the website before the transaction can continue. Whatever method the bank chooses, they need to place funds on hold until fraud analysts are able to verify the legitimacy of the transaction.

### **Internet banking fraud prevention as part of an enterprise fraud management strategy**

Enterprise fraud management takes a holistic view of a financial institution's relationship with a customer by collectively viewing every product or service the customer uses. This enterprise-wide approach protects financial institutions from fraud at every level, from identity theft to deposit fraud - essentially any type of fraud that could cause an institution or its customer's monetary loss or potentially damage the institution's reputation.

By capturing a broader view of customer activity, financial institutions gain a complete understanding of a particular customer's profile. This expanded view allows institutions to better detect and prevent fraud by monitoring transactions and events across the entire range of customer activity.

Online banking, mobile banking, IVR banking, ATMs and branches are all susceptible to fraudsters, and can all be tied to one deposit account. Today's successful transactional fraud teams view all debit, check, ACH, billpay, internet and telephone banking transactions side by side from a single customer perspective. Fraud teams can leverage advanced analytics and write rules that cut across these disparate channels, which is a substantial benefit over the silo approach and enables fraud to be stopped at the first possible opportunity.

## **Mobile banking**

Mobile banking transactions are predicted to grow to nearly 300 billion by 2012 according to Informa Telecoms & Media.<sup>5</sup>

Although not originated from a user's PC, mobile banking transactions are at similar risk of fraud as online banking transactions. Financial institutions who have adopted mobile banking technology have already been susceptible to fraud by compromising mobile browsers and through the use of call forwarding. Similar to online banking fraud management, determining if the activity occurring within the mobile banking session fits the established profile of the legitimate customer is pivotal in mitigating fraud risk.

## **Sharing intelligence**

Banks are working together to solve internet banking fraud, but policies and practices vary by country, and banks must find a delicate balance between protecting customer privacy while still preventing fraud.

Fraudsters are not limited by geography or time zone, which is why banks must continue to communicate their best practices and fraud lists in order to keep up with rapid changes.



Protecting consumer confidence requires an intelligent, multi-layered approach to online security. In the current banking climate, using the right mix of fraud detection systems and intelligence means that suspicious transactions can be crosschecked with a wealth of data. Combining real-time fraud detection tools with customer information across various channels gives banks a complete, enterprise-wide view of customer behavior to reduce fraud and increasing the detection speed of fraud patterns to stay ahead of rapidly-changing threats on the horizon.

### **An enterprise fraud management solution**

ACI Proactive Risk Manager for Enterprise Risk™ is a complete fraud detection solution to manage risk across a financial institution's business lines and customer accounts. Proactive Risk Manager combines the power of expertly defined rules with a custom-trained neural network model for fast, accurate and flexible response to the evolving and growing nature of fraud - including online banking fraud.

Proactive Risk Manager provides an end-to-end, enterprise-wide fraud detection and risk management solution. It monitors transactions from any channel within a retail or wholesale banking environment. By capturing a broader view of customer activity with Proactive Risk Manager, financial institutions gain a complete understanding of a particular customer's risk profile. This expanded view allows institutions to better detect and prevent fraud by monitoring transactions and events across the entire range of customer activity.

<sup>1</sup> Market for Financial Crime Risk Management Technology, 2009, Chartis Research Ltd., 2009

<sup>2</sup> Phishing Activity Trends Report, September 2009, Anti-Phishing Work Group, [http://www.apwg.org/reports/apwg\\_report\\_Q3\\_2009.pdf](http://www.apwg.org/reports/apwg_report_Q3_2009.pdf)

<sup>3</sup> Q3 2009 Internet Threats Trend Report, CommTouch, October 13, 2009, <http://www.commtouch.com/download/1548>

<sup>4</sup> [http://www.fbi.gov/pressrel/pressrel09/ach\\_110309.htm](http://www.fbi.gov/pressrel/pressrel09/ach_110309.htm)

<sup>5</sup> <http://www.tmcnet.com/submit/2009/02/26/4016595.htm>, June 5, 2009



## ACI Worldwide

Offices in principal cities throughout the world  
[www.aciworldwide.com](http://www.aciworldwide.com)

Americas +1 402 390 7600

Asia Pacific +65 6334 4843

Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide, Inc. 2011

ACI, ACI Payment Systems, the ACI logo and all ACI product names are trademarks or registered trademarks of ACI Worldwide, Inc., or one of its subsidiaries, in the United States, other countries or both. Other parties' trademarks referenced are the property of their respective owners.

ATL4623 03-11

## About ACI Worldwide

ACI Worldwide powers electronic payments for financial institutions, retailers and processors around the world with the broadest, most integrated suite of electronic payment software in the market. More than 90 billion times each year, ACI's solutions process consumer payments. On an average day, ACI software manages more than US\$12 trillion in wholesale payments. And for more than 150 payments organizations worldwide, ACI software ensures people and businesses don't fall victim to financial crime. We are trusted globally based on our unrivaled understanding of payments and related processes. We have a definitive vision of how electronic payment systems will look in the future and we have the knowledge, scale and resources to deliver it. Since 1975, ACI has provided software solutions to the world's innovators. We welcome the opportunity to do the same for you.