



Arcot Virtual Private Session

Protection Against “Man-in-the-Browser”

DATA SHEET

Overview

Patented ArcotVPS protects users from man-in-the-browser attacks.

Uses familiar CAPTCHA technology to present complete transaction to the user for verification using the same channel as the primary transaction.

Can be deployed along with other fraud detection and strong authentication solutions.

THE INTERNET THREAT CHALLENGE: Online web-based transactions are vulnerable to a number of attacks including phishing, pharming, man-in-the-middle and man-in-the-browser(MITB). The MITB is particularly insidious because most strong authentication solutions do not protect against this attack.

THE ARCOT VIRTUAL PRIVATE SESSION SOLUTION: Arcot Virtual Private Session (VPS) protects a user’s Web transactions from man-in-the-browser attacks. ArcotVPS uses CAPTCHA technology in an innovative way to foil a malicious attempt to change transaction data during the online transaction process. Arcot’s patented technology protects online users from internet threats reducing fraud and improving the online experience. Our solutions protect people while shopping, banking, and conducting business online.

What is a Man-in-the-Browser (MITB) Attack?

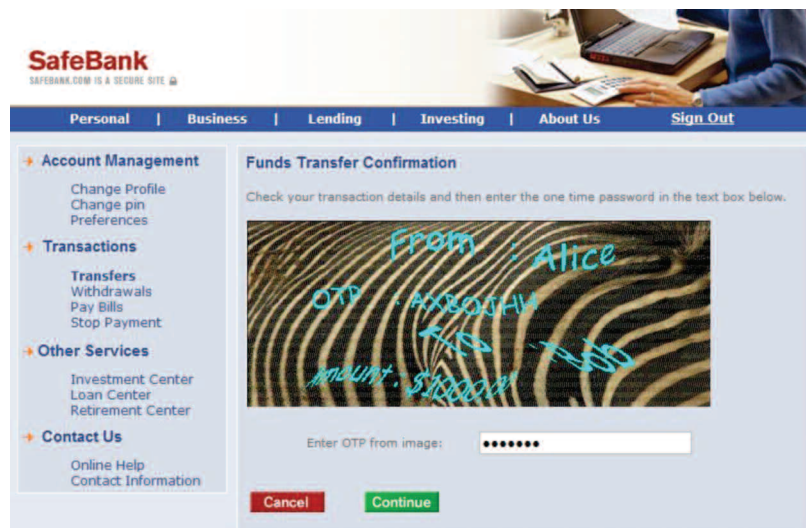
A typical MITB attack involves a specific Trojan that gets downloaded into the browser. Once downloaded, the MITB stays dormant until the user starts a transaction – a wire transfer, for example. The MITB waits until the user enters the details of the wire transfer. Before the transaction can be submitted to the server, the MITB substitutes the wire transfer details with bogus information as shown.

Common strong authentication solutions like hardware tokens or device ID checks authenticate the user at login time or at the start of the specific transaction. None of these approaches stop the MITB because the MITB strikes after the authentication is complete.

Alternate fraud detection methods like backend trend analysis and alternate channel confirmation work part of the time but may inconvenience users. Backend trend analysis may flag an alert because the amount in the fraudulent transaction is high but sophisticated fraudsters are careful to adjust the amount to stay under the fraud radar.

What the user requested		MITB	What the bank receives	
To	Alice		To	Marauder
A/C Number	0532-547821	A/C Number	0871-234567	
Amount	\$150.00	Amount	\$2,500.00	
Type	Same day wire	Type	Same day wire	

ARCOTVPS THWARTS MITB



Arcot patented Virtual Private Session (VPS) protects customers from man-in-the-browser (MITB) attacks. Transactions are verified by the user using CAPTCHA technology and cannot be parsed by an intruder before the transaction is completed.



Once the transaction is flagged, the typical response is to step up the authentication with a one time password (OTP) sent to the user's mobile phone over SMS. The user successfully completes the stronger authentication request without realizing that the transaction details have been modified. Some solutions attempt to send the transaction details to the user's phone for confirmation. These approaches fail because typical cell phones have a small screen and the details are difficult to read. The fraudster can easily adjust the changes to appear similar causing minimal concern. These solutions also depend on successful SMS delivery for the alternate channel confirmation.

Arcot Solution – Virtual Private Session (VPS)

Arcot patented Virtual Private Session uniquely uses CAPTCHA technology to foil an MITB attack. Arcot VPS presents details of the transaction along with a Transaction Confirmation Code back to the user in a CAPTCHA format in the same web channel. This approach does not

depend on alternate channels or backend analysis. The Confirmation Code must be entered in the web page within a configurable time to complete the transaction. The user reads the CAPTCHA, verifies the transaction details, and enters the confirmation code to confirm the transaction. The MITB Trojan is unable to parse the CAPTCHA and read the Transaction Confirmation Code within the time available. If the MITB has modified the transaction, the CAPTCHA image will show the modified transaction in its entirety. The user sees the transaction and can easily detect the change from what was originally entered. If the transaction has been modified the user can stop the transaction and prevent the MITB attack.

Arcot Protects Online Users from MITB Attacks

- Supports all transaction types
- Works with all primary authentication solutions
- Is platform independent – Windows, Mac, Linux
- Uses the same channel as the primary transaction
- Can be deployed along with other fraud detection solutions

About Arcot

Arcot is the cloud authentication leader. Our fraud prevention, strong authentication, and e-Document security solutions make Web transactions and online access safe for millions of consumer, enterprise, and e-Commerce users.

Organizations can transparently deploy stronger authentication and allow users to conveniently authenticate from any computer or mobile device. Arcot solutions deliver the right balance of cost, convenience and strength.

For more information, please visit www.Arcot.com, email sales@arcot.com, or contact your nearest sales office:

Corporate Headquarters, U.S.

Arcot Systems, Inc.
Ph: +1 408 969 6100

United Kingdom

Arcot International
Ph: +44 118 965 7998

Germany

Arcot Deutschland GmbH
Ph: +49 8157 997793

India

Arcot R&D Software Private Ltd
Ph: +91 80 6660 2745



www.arcot.com

Copyright © 2009 Arcot Systems, Inc. All rights reserved. Arcot, Arcot WebFort and ArcotID are registered trademarks of Arcot Systems, Inc. All other trademarks are the property of Arcot Systems, Inc. or their respective owners.

09-205