



How Arcot Solutions Protect Against Internet Threats

July 2006

Threat	Protected
Phishing	✓
Pharming	✓
Man-in-the-Middle	✓
Trojans and Key Loggers	✓
Replay Attack	✓
Fraudulent Administrator	✓
Brute Force	✓
Chosen Plaintext	✓
Challenge/Response Intercept	✓



Introduction

Arcot Systems, Inc. provides a complete suite of products that address the strong authentication and digital signing requirements for corporations of any size. The Arcot solutions consist of the authentication and application servers WebFort, RiskFort, and SignFort for two-factor authentication, risk-analysis and digital signing. The ArcotID is the fundamental technology which stores and protects digital identities. The Arcot solutions are uniquely able to protect digital identities assuring that businesses and their customers are conducting transactions safely over the internet.

ArcotID Security

The Arcot ArcotID is a “software smart card” that combines protection for Digital IDs approaching that of a hardware smart card with the ease of use, ease of distribution and the attendant lower costs of a software solution. The ArcotID can be held on the local desktop or carried in any persistent memory device, such as a USB memory stick. The ArcotID resists brute-force attacks using patented “*Cryptographic Camouflage*”¹ technology to protect the Digital ID from would-be attackers. The technology has been in use since 1997 and has been vetted academically by security experts and in practice by Fortune 500 companies.

The ArcotID can be used for two-factor authentication, challenge/response based authentication, and storing secure application keys and other user data. For example, when authenticating using an ArcotID, the Authentication Server first sends down a “challenge” – a random string. When the user provides the correct PIN or, the private key in the ArcotID is used to sign this “challenge” – creating a “response”. Only this “response” is sent back to the Authentication Server for verification. The PIN is never stored anywhere or transmitted to the Server. **By providing the challenge/response sequence in addition to two factors, Arcot can uniquely protect businesses and customers from Man-in-the-Middle attacks.**

While highly secure, the ArcotID features an easy-to-use and familiar username-password or PIN-pad entry user interface and integrates quickly with existing infrastructures with support for standards such as RADIUS-based OTP, SAML, MS CSP and PKCS#11. This makes deployments fast and painless for the corporation to implement and its customers to use.

Arcot Systems has also developed a patented technology to protect PIN (or password) entry from keyboard capture attacks. Arcot’s unique Scrambled Pin-Pad defeats keyboard “sniffers”. The Arcot solution can require the user to use their mouse to “click” the digits of their personal PIN on a virtual keyboard whose keys randomly shift during password entry. The virtual keyboard can be configured to re-scramble the keys after each mouse click or each password entry thus preventing the attacker from reading any keystrokes or making pattern guesses based on mouse click locations.

In addition to strong two-factor authentication, the ArcotID can securely store application keys for PKI-based applications such as electronic document signing, secure email and secure e-commerce. As a software-based solution, the ArcotID enables organizations to leverage the advantages of Public-Key Infrastructures without the expense and management issues inherent with hardware-based secure key storage.

The ArcotID provides protection against the common internet attacks and several futuristic attacks that are becoming popular among fraudsters. Other solutions, including one-time-password (OTP) generator tokens, do not offer the same level of protection against attacks such as the man-in-the-middle attack. The following table contains a list of known threats and shows how Arcot defeats those attacks.

¹ See “Software Smart Cards via Cryptographic Camouflage”, D.N. Hoover and B. N. Kausik, Proceedings of the 1999 IEEE Symposium on Security and Privacy, IEEE Computer Society.



ArcotID – Protection Against Internet Attacks

Threat	Attack Description	How Arcot Defeats the Attack
Phishing	Phishing relies on fooling users into entering their information into fake web sites. This is usually done by sending an email impersonating a bank, for instance, and asking them to click on a URL which takes them to the fraudulent site. They are then asked for their valid credentials. The user trusting his “bank” enters his pin or password.	<p>The Arcot solution protects users from phishing attacks with multiple layers of authentication.</p> <ol style="list-style-type: none"> 1. Arcot provides a Personal Assurance Message (PAM) for the site to display and the user to verify before entering his password. The PAM is a shared secret that the user establishes with the application server (for example, his online banking portal). The site prompts the user for his username or account ID only. After the user enters his username, the site displays the secret assurance message. This provides a cue that verifies to the user that he is at the real site and not a phishing site. The user should not enter his password if the wrong PAM or no PAM is present. 2. Arcot’s Risk Engine is another layer of defense assuming the user <i>did</i> enter his password. When the attacker tries to use the password, the Risk Engine will detect that the user is coming from an unregistered device, geographical location, reach a transaction limit or other predetermined checks. The risk engine can force an out-of-band check which will prevent the attacker from using the password. 3. Arcot employs strong two-factor authentication using the ArcotID combined with a PIN or password. Again, assuming a phisher convinces a user to disclose their password, they are still unable to impersonate the user as they don’t have the ArcotID file. The phisher needs both what the user has (the ArcotID file) and what the user knows (PIN/Password). This is a key advantage of the Arcot two-factor security solution.
Pharming	The attacker poisons the DNS server and redirects users to the fake web site. Users do not suspect anything because the redirect happens even when the user selects the web site from a saved favorite or actually types in the correct URL.	As mentioned above, each ArcotID contains information on the domain that issued that ArcotID. The ArcotID client checks to confirm that it is connected, via SSL, to the right domain before signing the challenge string. If the domains do not match, the ArcotID client will not sign the challenge and the attacker will not be able to complete the authentication.
Man-in-the-Middle	In a man-in-the-middle attack, the attacker intercepts the credentials and data while they are in transit. In this case, the attacker appears as the target server to the user and as the user to the target server.	The most insidious phishing attack is the Man-in-the-Middle. <u>Protection from this type of attack is unique to the Arcot solution.</u> Each ArcotID contains information on the domain that issued that ArcotID. The ArcotID client checks the Arcot certificate to confirm that it is connected to the same domain before signing the challenge response. If the domains do not match, the ArcotID client will not sign the challenge and the attacker will not be able to complete the authentication.



ArcotID – Protection Against Internet Attacks

Threat	Attack Description	How Arcot Defeats the Attack
Trojans and key-loggers	Logging crimeware captures every keystroke and mouse click on the computer and periodically sends that information over the internet to the criminal or hacker who created it.	<p>Arcot’s patented scrambled PIN Pad thwarts logging malware. (US Patent 6,209,102) The PIN Pad is a virtual keyboard that shows up on the screen; users enter their PIN by clicking with a mouse on a screen-based PIN Pad.</p> <p>The user will not use the keyboard to enter the ArcotID PIN and is hence protected completely from keyboard loggers.</p> <p>The scrambled PIN pad ensures that mouse click loggers are unable to determine what keys are actually pressed because of the change in the positions of the keys on the PIN pad.</p>
Replay attacks	The attacker stores a copy of the signed challenge and replays it to the site.	<p>The Arcot authentication involves a PKI based challenge/response model where the challenge sent to the client for signing is always a random challenge.</p> <p>When the signed challenge is sent to the server for verification, the server verifies the challenge and marks the particular signed challenge as having been verified.</p> <p>Since the challenge is a random one, each signed challenge will also be different. If the attacker replays the signed challenge, the server will detect that the particular signed challenge has already been verified earlier and will reject the signed challenge thereby preventing the replay attack.</p>
Non-Repudiation or Fraudulent Administrator	A fraudulent administrator gets access to the ArcotID on the server	<p>A fraudulent administrator may get access to the ArcotID, but the administrator cannot use it without the PIN. The PIN is not stored anywhere, nor does it travel to the server during authentication. It is used only to de-camouflage the private key at the client when the challenge is signed. Only the user knows the PIN – this ensures that the ArcotID offers non-repudiation.</p>
Brute Force Attack	Attacker copies the key container to his own equipment and exhaustively attempts millions of passwords, which eventually leads to the disclosure of the private key.	<p>Using Arcot’s patented “<i>cryptographic camouflage</i>” technology (US Patent 6,170,058), the key is encrypted based on the user’s PIN with standard encryption algorithms, but using the patented Arcot process. The effect of this process is that decryption, even using an incorrect PIN, will always produce a result that meets the specific, particular and well-documented characteristics of a private key.</p> <p>During authentication, which is an online process, the decrypted key is required to generate a response to the authentication challenge.</p> <p>If the authentication fails because an incorrect key was used, the invalid PIN counter is incremented and, just as with a hardware-based solution, the server can lock any access to the ArcotID container after a configurable number of invalid attempts. Therefore, the attacker is able to attempt only few passwords and is then prevented from further validation attempts.</p>



ArcotID – Protection Against Internet Attacks

Threat	Attack Description	How Arcot Defeats the Attack
Chosen Plaintext	Attacker tests every possible key against a known piece of text (known as "plaintext") that has been encrypted with the public key, and can tell when he has discovered the true private key as it would correctly decrypt the plaintext.	The attacker cannot mount this attack since he does not have access to the ArcotID public key. In the ArcotID scheme the public key used for authentication is encrypted by the domain root key thereby making it possible to control its release to only trusted parties.
Challenge / Response Intercept	Attacker intercepts the challenge and the signed response. Attacker then uses every possible private key to recreate the signed response and discover the true private key.	<p>The authentication challenge/response is sent over a secure SSL channel.</p> <p>Even if an attacker were able to break channel security – which is extremely unlikely - this attack fails because the Arcot authentication protocol includes padding the challenge with a random hash before signing it. Only the authorized authentication server which can access the plain public key can verify the signature.</p>
Protection of Private Key in Memory	The user is roaming and downloads the ArcotID into memory. The user does not close the browser. Is the private key in memory?	<p>When the ArcotID is downloaded into memory, the private key is still camouflaged – it is not in the clear. Only when the challenge is to be signed, the user is prompted for the PIN and the private key derived. Immediately after signing the challenge, the private key and PIN are cleared from memory; only the response (encrypted challenge) is sent back to the server, the private key and PIN are never sent to the server. Even if the user does not close the browser, only the protected ArcotID may be in memory. This can also be removed by the web page that downloaded the ArcotID – by clearing it immediately after the authentication.</p> <p>The Arcot authentication step can be configured to be done in a new browser window. In this model, the new window itself can be closed after the Arcot authentication is completed. The ArcotID will be destroyed when the browser window is closed.</p>