

SecureAuth Whitepaper “Mitigates Man-in-the-Middle Attacks”

SecureAuth has created a unique methodology to combat phishing, replay and man-in-the-middle (MITM) attacks.

The IT industry is plagued with identity theft - with hackers maliciously stealing user's identity to on-line web sites. The reason is that over 99% of web sites still utilize username/password authentication and "cookie" technology for identification. These technologies are susceptible to hacking attacks such as "phishing", "replay" and "man-in-the-middle" (MITM) attacks.

It's important to note the token solutions, like the RSA SecurID token and other vendors tokens, Verisign, Vasco, etc, do nothing to solve these man-in-the-middle attacks.

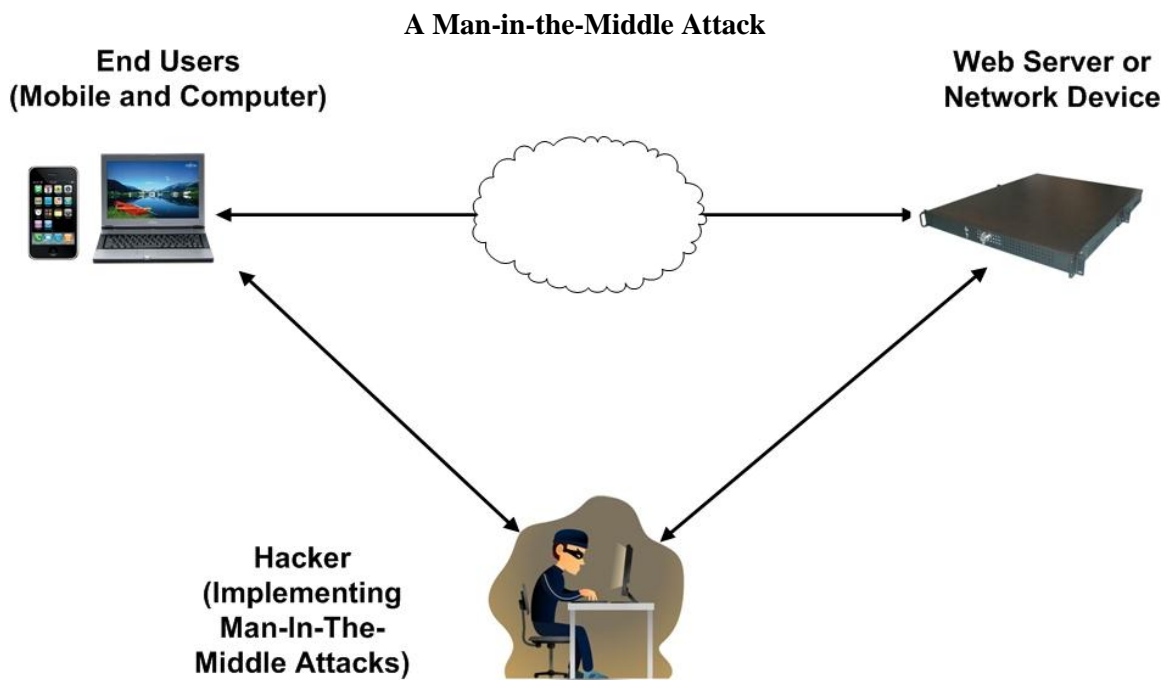


Diagram 1 – Man-in-the Middle Attack

The attacker lures the end user to his site via phishing, DNS attacks, or other methods.

Once there, the attacker utilizes vulnerable authentication methods (e.g.: username/password, tokens) to attack and replay the session – thus “stealing” the legitimate user’s ID.

The solution to the man in the middle attacks is to authenticate both the client and server. The technology to implement a safe transaction utilizes x.509 certificates in a public key infrastructure deployment.

A Solution to the Man-in-the-Middle Attack

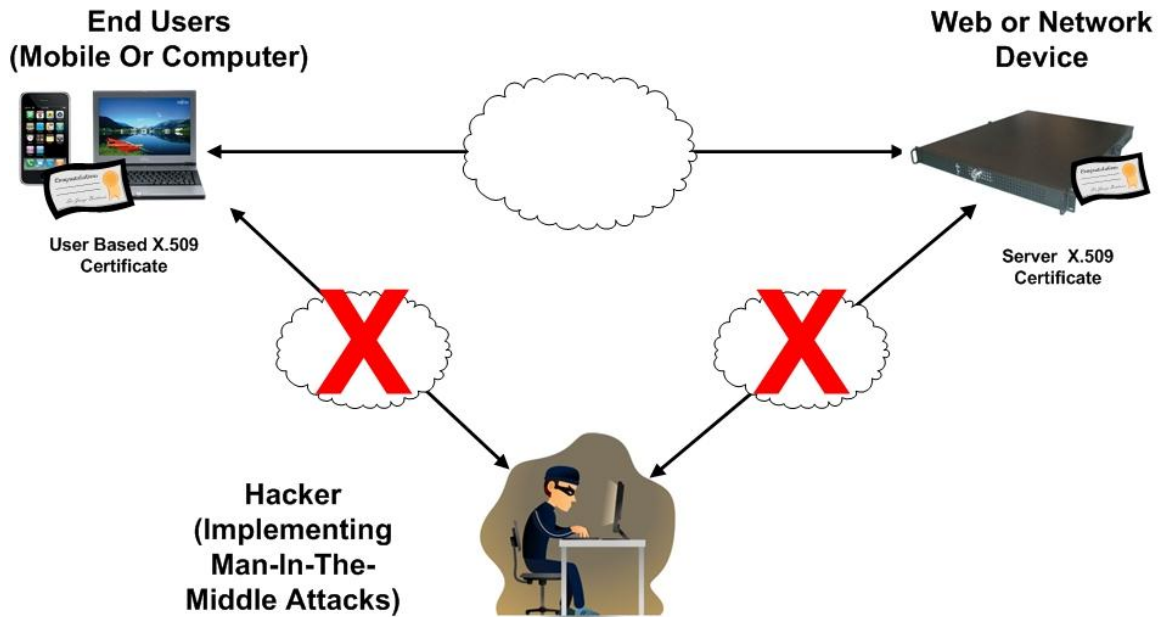


Diagram 2 – Man-in-the Middle Solution

The secret to stop man-in-the-middle attacks is to authenticate both the server and the client. Solutions that authenticate just the user are susceptible to man-in-the middle attacks.

The key to the solution is to deploy technology on both sides that can recognize and authentication the other side.

The problem is that the solutions to these man-in-the-middle attacks, prior to Multi-Factor Authentication, have been expensive, difficult to deploy and requires crypto specialist to maintain.

Traditional Infrastructure Required to Host a Solution to Combat Man-in-the-Middle Attacks

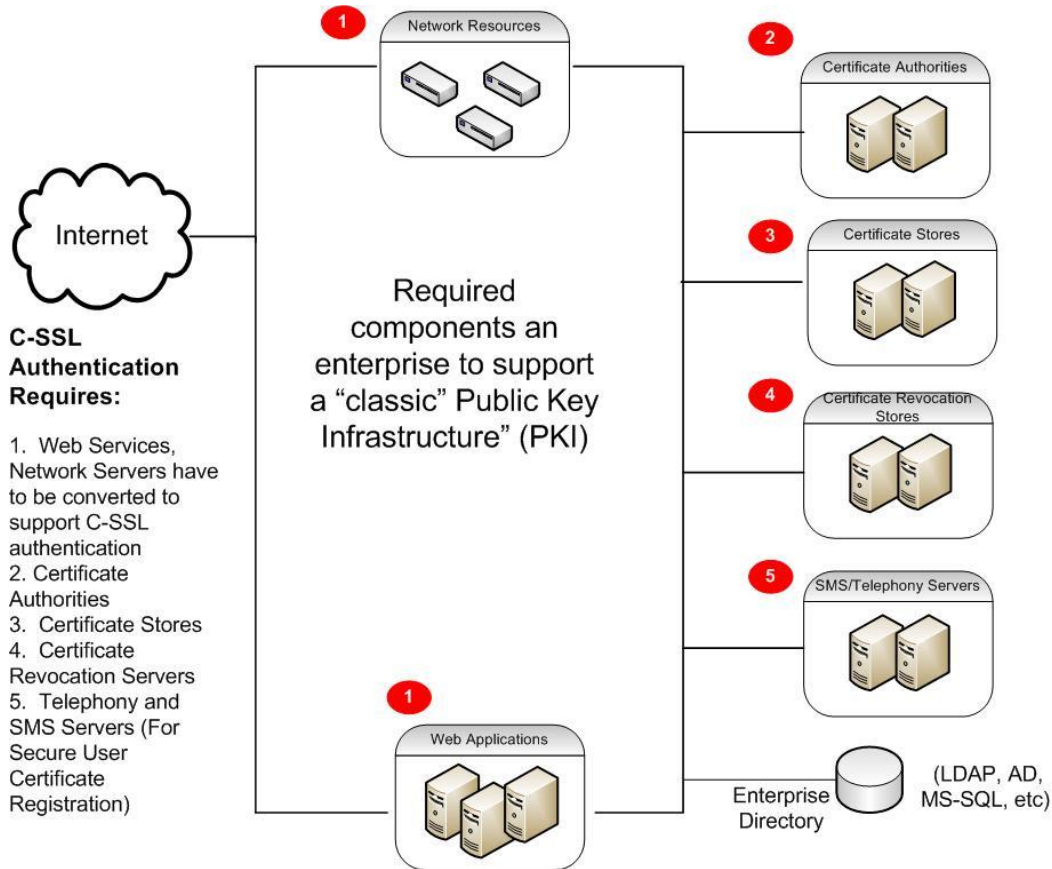


Diagram 3 – Traditional PKI infrastructure

The typical PKI deployment requires a range of services and servers:

- Modified Web Servers (Supporting "Client Side SSL"-C-SSL)
- Certificate Stores
- Certificate Authority Servers
- Certificate Revocation List (CRL) Servers
- Telephony Server (for Secure Registration)

If the infrastructure above wasn't intimidating enough – the burden is not just on the enterprise. End users are also burdened with certificate management and portability issues. For these and other reasons enterprises have chosen not to deploy X.509 certificates to the users, even though security-conscience team members realize this is the proper way to stop these identity attacks.

The SecureAuth Authentication Solution:

The SecureAuth, addresses these identity attacks by implementing X509 certificates to establish and maintain a user identity. By utilizing SecureAuth's patented X.509 distribution and authentication technology, enterprises can stop man-in-the-middle and other identity attacks.

Most importantly, SecureAuth combats these attacks in a manner that is easy to deploy and easy to manage for both the enterprise and end users.

SecureAuth has the following advantages over traditional technology because it:

- Does NOT require an enterprise to convert their web sites to be client-side SSL (C-SSL) compliant.
- Does NOT require the enterprises to issue any certificates. SecureAuth's hosted servers perform this task
- Does NOT require the enterprises to keep track of any of the certificates issued.
- Does NOT require the enterprise to keep track of any of the certificates revoked.

Traditional solutions require an enterprise to implement all of the above. (See Diagram 3) The uniqueness of SecureAuth is that it PROVIDES the same security – without the overhead.

SecureAuth involves a simple component on the client side and a SecureAuth component on the web server. With these 2 lightweight solutions and enterprise can utilize an X.509 authentication to validate the user's identity. SecureAuth allows the enterprise to solve the issues of cookies (phishing, identity theft, replay attacks) by utilizing SecureAuth's X.509 authentication solution. It allows an enterprise to deploy .X509 certificates and create secure authentication without requiring an enterprise to deploy all the components of a PKI deployment. (Contrast the traditional architecture, Diagram 3, with SecureAuth Authentication's design, Diagram 4.)

SecureAuth Secure Architecture for Web, VPN and SaaS Environments

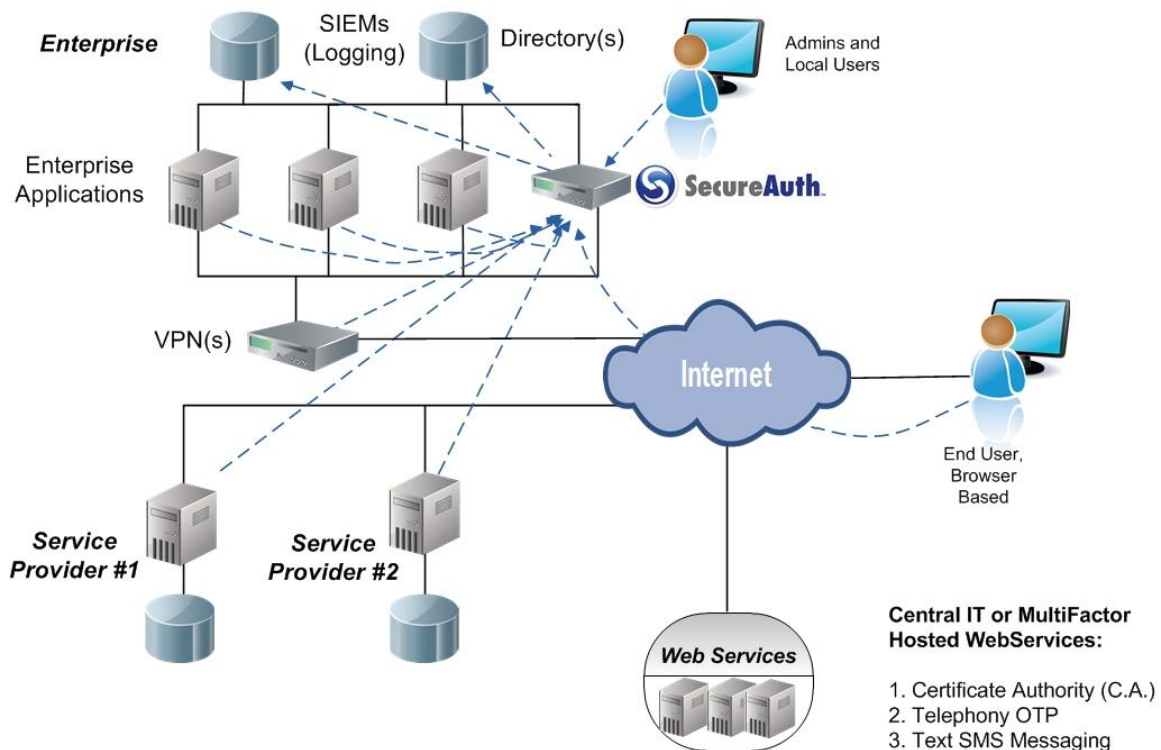


Diagram 4 – The SecureAuth Solution

The benefits of SecureAuth are:

1. SecureAuth does NOT add servers to the enterprise hosting environment
2. The enterprise does NOT have to convert their web servers to support client side SSL. (C-SSL)
3. The enterprise does NOT have to keep a store of the certificates – or revoked certificates
4. The enterprise does NOT have to maintain and staff for advanced technologies such as certificate authorities and telephony servers

SecureAuth Patent Pending Solution to X.509 Authentication

The key to SecureAuth's technology is its patent-pending method of distributing and authenticating X.509 certificates to the end user – without forcing the enterprise to turn on client side SSL technology.

SecureAuth Stops Man-in-the-Middle Attacks with Deployable PKI

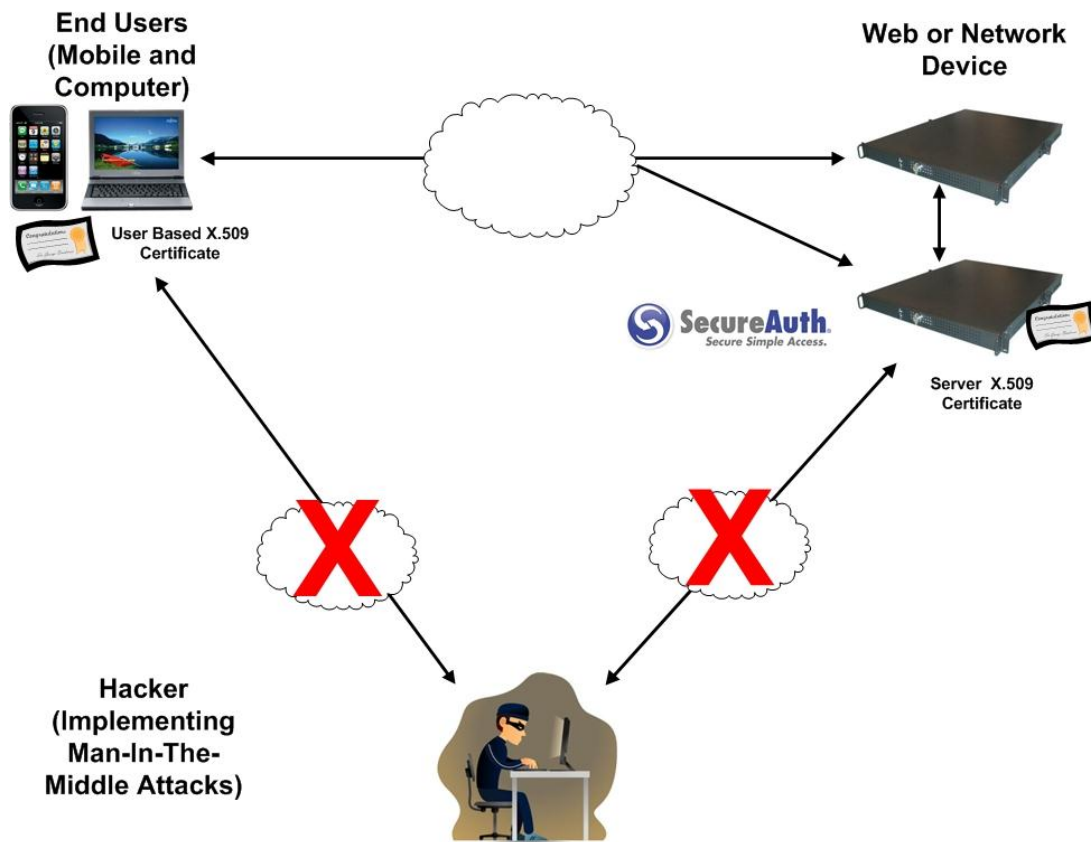


Diagram 5 – How SecureAuth Solves the MITM Attack

SecureAuth eases both the end-users and the enterprises experience in deploying a security solution that is not susceptible to the MITM attacks.

The end user is not overwhelmed with difficult certificate installs and management issues. Nor, is the enterprise burdened with certificate infrastructure. SecureAuth does not even require the enterprise to turn on C-SSL on the web server.



The primary components of SecureAuth include:

1. An X.509 certificate that resides on the client side computer.
2. A SecureAuth Authentication appliance that authenticates the certificate.

These two components in conjunction allow:

- A. The end user to receive, store and utilize an X509 certificate - without the user ever knowing anything about the details of certificate retrieval and archiving.
- B. The enterprise to receive and authenticate users utilizing X509 certificates - without having to set up their own web servers for client side SSL authentication. In addition the enterprise does not have to store the certificates nor does the enterprise need to keep a list of revoked certificates.

In addition SecureAuth utilizes the following hosted servers:

1. SecureAuth hosted certificate authorities
2. SecureAuth hosted telephony/SMS servers

The hosted certificate authorities and hosted telephony servers communicate with the SecureAuth web server plug-in. These web services allow the enterprise to enjoy the functionality of advanced PKI and advanced telephony authentication, without having to install the complex and expensive C-SSL components.