



Multipeers Security

Multipeers works with your enterprise security infrastructure to protect against unauthorized access to critical data.

Audit and Compliance

Tighter compliance regulations coupled with tougher penalties for data breaches has raised the profile of who can access company data. MultiPeers has been designed and built with security as a priority. MultiPeers architecture has also been thought to integrate with all the existing security mechanisms in order to ensure that only authenticated users can view your data.

Easy Integration with Security Infrastructures

MultiPeers ties into the existing gateways, firewalls, Microsoft Active Directory, LDAP services, security policies, and group policies to ensure that data is protected from source to destination, and can only be accessed by properly authenticated users.

For communication, MultiPeers uses REST Webservices that supports HTTP and HTTPS. Authentication is provided using basic, digest, challenge-response. User credentials are input as needed using session-oriented login components in the application.

MultiPeers minimizes the possibility of displayed data being vulnerable to man-in-the-middle-attacks. It uses a scheme of asynchronous keys that are randomly exchanged and validates the authenticity of every digital signed dataset of information. MultiPeers' datasets are all digitally encrypted using strong encryption algorithm.

Protecting Sensitive and Private Information

To prevent unauthorized access to intellectual property in the form of executable code, MultiPeers ensures that five things happen:

1. The amount of sensitive data and intellectual property rendered as code is minimized
2. Embedded intellectual property is protected from cursory examination
3. Application hardening techniques increase the difficulty of reverse engineering the algorithms and keys involved in decryption/de-obfuscation
4. Runtime hardening techniques increase the difficulty of discovering the intellectual property through forensic analysis of RAM images and stepwise debugging
5. The user decides if it's local data storage is stored or not, and all the storage is also encrypted

Security Challenges

Issue	Solution
<p>Data interception (man-in-the-middle-attacks). Without transport layer encryption (SSL), data could be intercepted by a third party, leading to possible account compromise and disclosure of sensitive information.</p>	<p>Secure data transmission. MultiPeers makes validation of the chain of trust involved in signature systems, such as SSL, coupled with resistance to reverse engineering, improves the security of data transmissions and reduces the possibility data being compromised.</p>
<p>Unauthorized Access. If access control mechanisms are inadequate, authorized users may have access to data for which they do not have the correct privileges. Unauthorized individuals may be able to use already active instances of an application to view data.</p>	<p>Profile Access. With MultiPeers, deployment managers can distribute indicators that are easily authenticated against Active Directory or LDAP to ensure the correct level of privilege access.</p>

MultiPeers security includes:

- Microsoft Active Directory support
- Cryptographic services
- Strong Actionscript sandboxing

It supports industry standard protocols:

- SSLv3
- TLS

And it incorporates important standards:

- PKCS-1
- SHA-1 and SHA-256
- AES