

Is your data safe out there? -A white Paper on Online Security

Introduction:

People should be concerned of sending critical data over the internet, because the internet is a whole new world that connects businesses, scholars, and ordinary users with hackers and terrorists. The temptation of accessing personal information of others is something that a percentage of people will go to the extreme to do in order to possess valuable information either for personal amusement, theft, or even blackmailing. Therefore, internet users must fully understand the security risks in order to understand whether their web providers are supporting them with enough security, especially if the data is critical.

Online Risks:

When you send critical information over the internet, this information is mainly exposed to the following risks:

1. Eavesdropping
2. User Impersonation
3. Unauthorized Accessing

Eavesdropping:

Eavesdropping is not only a bad habit people have when overhearing conversations between two parties, it is also a risk encountered on the internet. Credit cards, passwords, and other critical data can be "overheard" on the internet. Whenever information is transmitted from one host to another on the Internet, it usually passes through several, perhaps many, routers. During this trip, this information may pass through Internet subnets other than the ones on which the sending and receiving hosts are located. Hackers could actually see the addresses of the sender and receiver using simple commands and also could modify the passing information. A person cannot be sure what path the data is traveling through.

User Impersonation:

The identification and authentication method most commonly used on the Internet is a username/password mechanism. When users log into an Internet host providing login or file transfer service, they are prompted for a username and a password. If this username and password is passed over the Internet, then it is subject to eavesdropping. Both the username and password are transmitted in plaintext. Intercepted usernames and passwords can be used to impersonate the user on the login or file transfer server host that the user was accessing. Obtaining passwords by eavesdropping on the Internet for the purpose of user impersonation is a frequent occurrence.

Unauthorized Accessing:

This is the biggest risk in internet security; for the internet connects to every computer into one large network. If the system is designed to grant or deny complete access for a system, this will eliminate the purpose of having the internet as a valuable business tool; having access anywhere anytime.

Security Solutions:

Anyone considering in using online services should really look into how the service provider solves these problems, several technologies and techniques have evolved as standards for the three major risks addressed above, and these mechanisms that resolve the risks respectively are:

Data Encryption
User Authentication
Access Control

Data Encryption:

Transferring data over an insecure link with out some sort of coding for the data can result in eavesdropping; the following techniques are what can be done to prevent a hacker from reading the data sent:

1. **Document encryption.** The documents that are placed on the Web server can be encrypted with a system such as PGP (Pretty Good Privacy). Although this encryption provides for effective privacy protection, it is cumbersome because it requires the documents to be specially encrypted before they are placed on the server and they must be specially decrypted when they are received by the user. In addition to that, document encryption does ensure the identity of the recipient.
2. **SSL (Secure Socket Layer)** is a protocol developed by Netscape for transmitting private documents via the Internet. SSL uses a cryptographic system that uses two keys to encrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message. All internet browsers support SSL nowadays and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with *https:* instead of *http:*. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery.
3. **Secure HTTP (S-HTTP).** Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. Both protocols have been approved by the Internet Engineering Task Force (IETF) as a standard.

When using an encrypted protocol, your security depends on several issues:

- The strength of the encryption algorithm
- The length of the encryption key
- The secrecy of the encryption key

Therefore, a user should ask their online applications about these issues.

User Authentication

There are several methods to authenticate users over the web. Table 1.1 summarizes these methods.

Method	Security Level	Implementation Effort	Server Requirements	Brief Description	Comments
Standard authentication	low	Low	User management	sends the username and password across the net in plain text	Although the password is encrypted, it can be easily decrypt by a potential "eavesdropper"
Form-based authentication without secure transmission	low	moderate	Implementation in the relevant application	A Web container provides an application-specific form for logging in.	Very tricky to implement, poor security unless used with SSL but provides faster transmission
Digest authentication	Moderate	Low	User management	Transmits username and password information in a manner that cannot be easily decoded. The Digest mechanism includes an encoding of the realm for which the credentials are valid, so a separate credentials database must be provided for each realm using the Digest method.	Unfriendly user interface, hard to implement
Form-based authentication using SSL	High	Moderate to high	SSL support in the server, implementation in the relevant application	Same as form-based authentication but uses a secure connection to transmit the data	Authentication information and data are transmitted encrypted.

Certificate-based authentication using SSL	High to very high	High to very high	Installation of server certificates. Certificate administration, public key infrastructure.	The client digitally signs a randomly generated piece of data and sends both the certificate and the signed data across the network. The server uses public key cryptography to validate the signature and to confirm the validity of the certificate.	Primarily used for secure transactions over the internet.
--	-------------------	-------------------	---	--	---

Access Control:

Authentication by username and password is only part of the story. Frequently you want to let people in based on something other than who they are. Something such as where they are coming from. Restricting access based on something other than the identity of the user is generally referred to as Access Control. Usually programs grant specific permissions to the users based on the resources the user needs to perform the certain tasks available. For example, a regular user should not be granted administrative permissions.

Genie Online Backup Security Solutions:

Genie-Soft addresses the security risks with the best state-of-the-art security standards that ensure the users that their data is safe. Even the genie-soft team cannot view, modify or delete the contents of the files and folders. There is no way that we or any other person can decrypt your password. The following thoroughly explains how this is all achieved by providing our customers with the following security features:

- Encryption
- Secure Socket Layer
- Authentication Methods
- Access Control
- Secure Ordering of the Product

Encryption:

Genie Online Backup uses encryption standards that are used by the federal government with the highest standards for two types of data:

1. Passwords
2. Documents

Passwords:

Passwords are encrypted using the SHA-256(Secure Hash Algorithm). This hash encrypted algorithm is one of the required secure hash algorithms for use in U.S. Federal applications, including use by other cryptographic algorithms and protocols, for the protection of sensitive unclassified information. This standard is called secure because, for a given algorithm, it is computationally infeasible to find a message that corresponds to a given message digest, or to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, results in a different message digest.

This Encryption methodology is a one way encryption; therefore it cannot be decrypted at the server's side:

The value stored in the server's database is the encrypted password; therefore, even if the server's database was exposed, the hacker will be unable to access the users' accounts, using the information shown in the server's database, even the administrator responsible of the server cannot recover any of the user's passwords; therefore if a user forgot the password, the server will only be able to reset the password and not recover it. The reset process will be sent to the user's personal email, this process prevents hackers from resetting the user's account, which is a great feature to prevent user impersonation.

Important note: Login passwords only can be reset, the Passwords protecting the user's files/folders CANNOT be recovered; therefore we extremely recommend that the user keeps the passwords in a safe place.

Documents:

The user has the option to encrypt the files/folders sent to the genie online backup using the AES (Advanced Encryption Standard). The National Security Agency (NSA) reviewed all the AES and stated that the standard is secure enough for US Government non-classified data. In June 2003, the US Government announced that AES may be used for classified information:

"The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use."_ CNSS Policy

This standard differs from the previous encryption method that it can also decrypt the file; therefore, the encrypted job is password protected, i.e. encryption password, using the SHA algorithm explained above. Genie Online Backup provides all key lengths for their users.

Secure Data transmission:

In addition of providing encryption options to secure the information sent to Genie online backup, the genie online backup supports a 128- bit Secure Socket Layer

(SSL) certified by the leading global provider of SSL certificates **Thawte**. This protocol uses RSA encryption algorithm.

Authentication Methods:

Authentication methods in the online genie backup are implemented in two ways:

1. Certificate Based Authentication
2. Form-based authentication

Certificate Based Authentication:

This Authentication is done to reassure the clients that they are sending their information to the right source. In other words, the certificate based authentication authenticates that we are who we say we are. This authentication is done by the SSL certificate provided by **Thawte**. An SSL Web Server Certificate enables the Genie Online Backup users to view the following information:

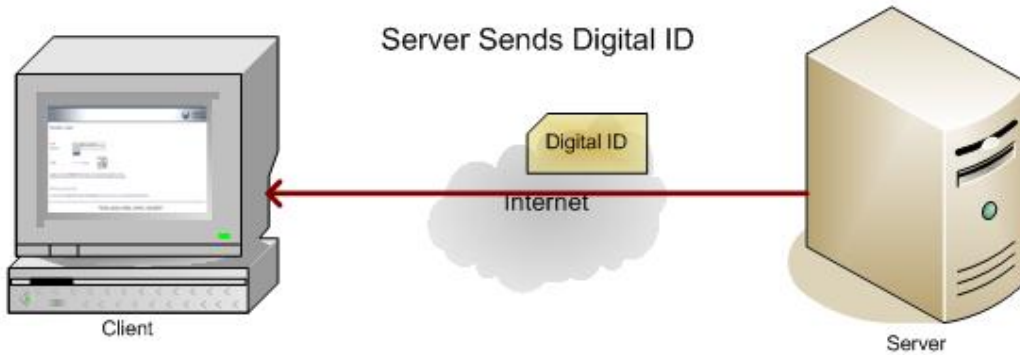
- The domain for which the certificate was issued. This allows them to check that the SSL Web Server Certificate was issued for your exact host and domain.
- The owner of the certificate. This acts as further reassurance, since customers are able to see whom they are doing business with.
- The physical location of the owner. Once again this reassures customers that they are dealing with an actual entity.
- The validity dates of the certificate. This is extremely important, since it shows users that your Digital Certificate is current. Figure illustrates the process of the digital authentication in order to establish a secure session:



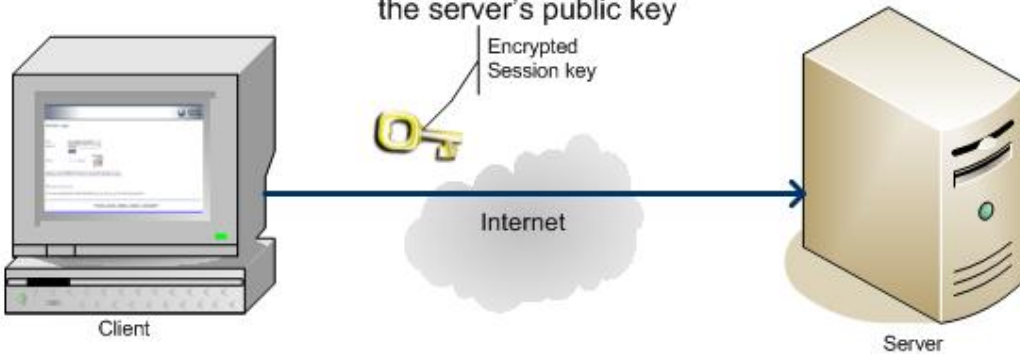
Client Initiates Connection by clicking Secure link on login form



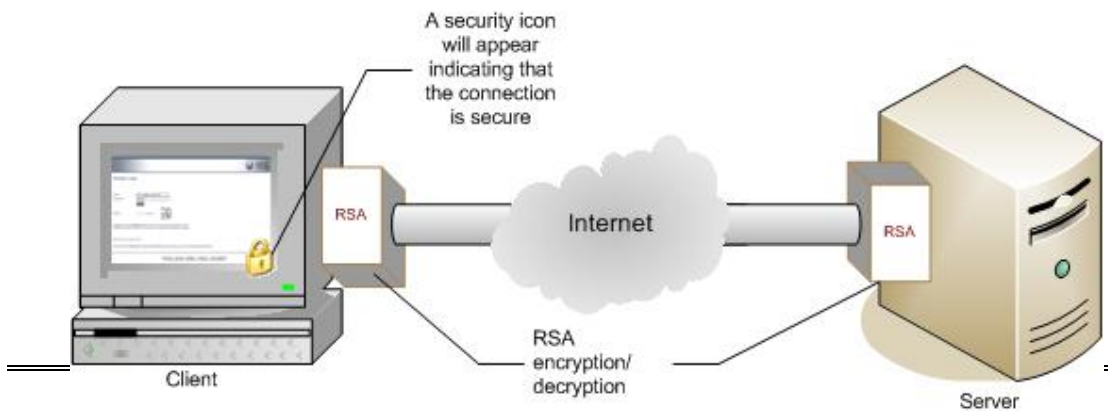
Server Sends Digital ID



Client sends the Session key encrypted using the server's public key

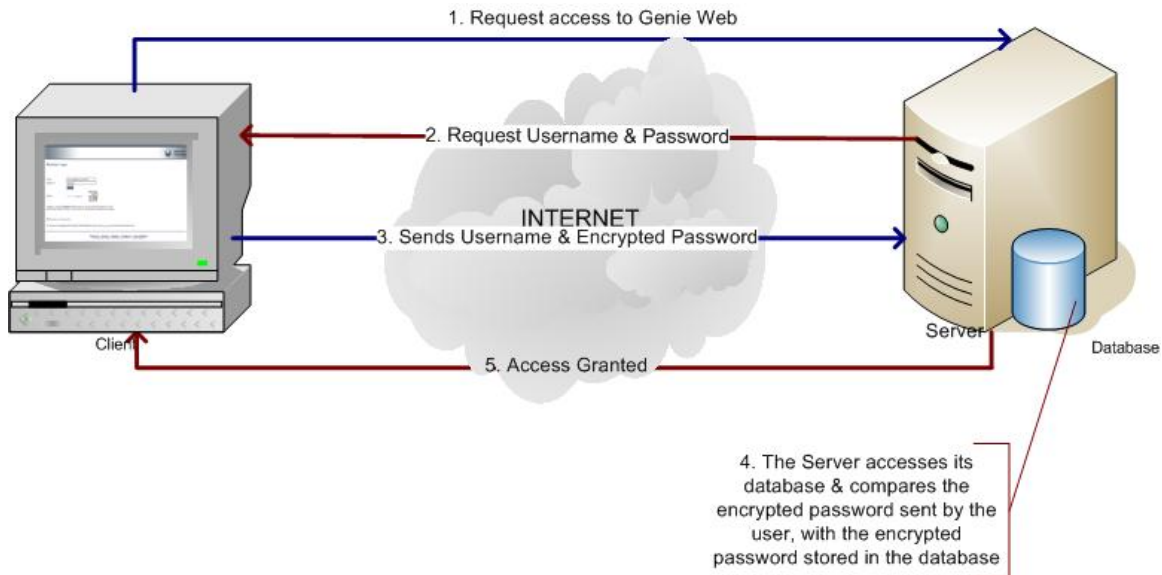


SSL Established



Form-Based Authentication:

This method is used to prompt the users to log in using their usernames and passwords, as mentioned above, the passwords are sent encrypted with the highly secure SHA encryption and are reset via personal email, making it extremely hard for user impersonation by hackers. This method is used to ensure that the user is a registered and valid user. Figure illustrates the process of password authentication:



Access Control

The Genie Online Backup allows the users to set access permissions of folder and file accessing and not backup jobs that are password protected. In other words, no one can access your documents unless you authorize to do so.

Secure Ordering of the Product

Users have a legitimate concern on ordering products over the internet due to the fear that credit card information will be exposed. Genie-soft acknowledges this fear and therefore, provides the customers with Plimus eCommerce solution. Plimus uses the highest level of encryption throughout the entire order and setup processes, from all order pages, through the storage of customer information, and credit card processing which is done by Wells Fargo, one of the largest and most trusted financial institutions.

Plimus also follows all internet standards for validating credit cards such as AVS, CVV2 as well as having their own fraud detection and prevention mechanisms which evaluate and verify many variables during the order process such as valid email addresses, names, addresses, zip codes, cross checking IP addresses against locations, zip codes and states, and also employs "Black List" mechanisms for known

and repeat offenders, and many more automatic mechanisms that for your and our protection shall remain confidential.

Conclusion:

There are many valid security concerns that must be considered using web applications that are used to send critical user data. Genie Online Backup addressed these concerns using very powerful security methods with keeping our system user friendly and affordable. Genie-Soft's envisioned road is to provide applications and utilities that others have failed to provide comprehensively, either for the lack of vision or for the lack of interest. Such utilities, like Genie-Soft's backup applications, can make the user's life easier and enhance his productivity at work and home.