

Virtual Office Website (VOW)  
Security Issues

Adopted Policy Version

National Association of REALTORS®  
Center for REALTOR® Technology

June 2003



# Virtual Office Websites Security Issues

## Table of Contents

	<b>Section</b>	<b>Pages</b>
<b>I.</b>	<b>Introduction</b>	<b>3</b>
<b>II.</b>	<b>Basis for the Policy</b>	<b>3</b>
<b>III.</b>	<b>Data Transmission</b>	<b>4 - 8</b>
<b>IV.</b>	<b>Registration</b>	<b>8 - 9</b>
<b>V.</b>	<b>Privacy Policy</b>	<b>10</b>
<b>VI.</b>	<b>Breaches of Security</b>	<b>10 - 11</b>
<b>VII.</b>	<b>Data Misappropriation</b>	<b>11 - 16</b>
<b>VIII.</b>	<b>MLS Required Security</b>	<b>16 - 19</b>
<b>IX.</b>	<b>Glossary of Terms</b>	<b>20 - 24</b>

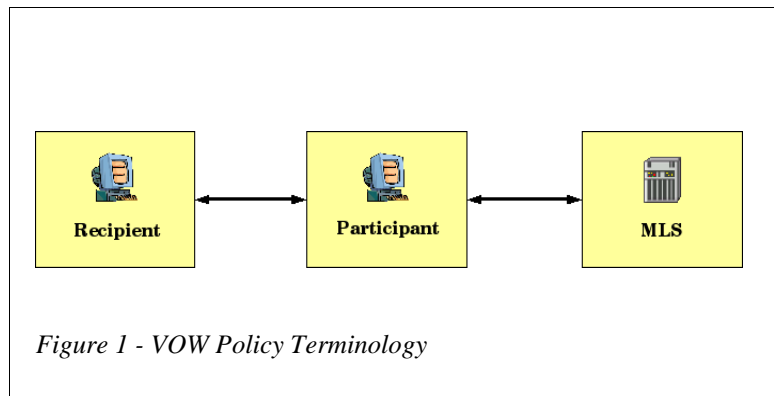


## I. Introduction

Virtual Office Websites ("VOWs") are used by an increasing number of real estate professionals to conduct marketing and brokerage activities over the Internet. To help REALTORS®, Association Executives, MLS Administrators and others make informed, effective decisions regarding establishment and oversight of VOWs, this white paper provides an overview of the technology that enables VOWs to function; and looks at fundamental technology issues, options and choices to be made by MLSs and by MLS Participants operating VOWs. Particular emphasis is given to security issues and concerns. Where appropriate and available, technology solutions (including pro's and con's, pricing, and alternative approaches) are incorporated.

## II. Basis for the Policy

The fundamental premise of the VOW policy is that VOWs are the functional equivalent of real estate broker's office, with brokerage services being delivered over the Internet. Another term that can be used to describe VOWs is an "electronic brokerage"



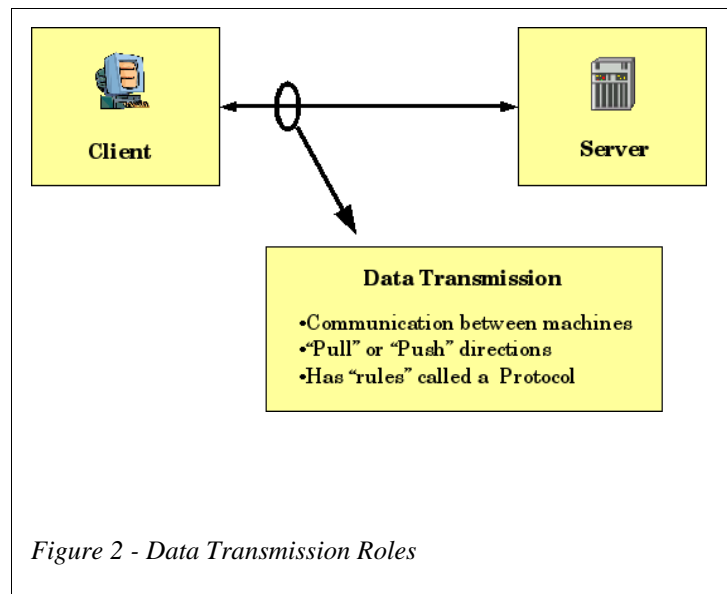
The VOW policy differs from the IDX policy in that the IDX policy addresses Internet advertising activities, while VOW is premised on the establishment of broker-consumer relationships and delivery of brokerage services.

Three important terms that will be used throughout this document are defined in the VOW policy. They are MLS, Participant and Recipient. The MLS hold the master version of property listing information, the Participant operates a VOW and the Recipient is the consumer who accesses listing information from the VOW. **Figure 1 - VOW Policy Terminology** illustrates these terms.

### III. Data Transmission

This section is a brief overview of mechanisms used for the transmission of data. A cursory understanding of these mechanisms is important for understanding certain security issues associated with the VOW policy.

Data transmission terminology begins with describing the function any particular machine (server/computer) plays in the transmission. There are two important roles to focus on; the Server and the Client. The Server is simply a source of information and the Client is the entity requesting information. **Figure 2 - Data Transmission Roles** illustrates this concept.



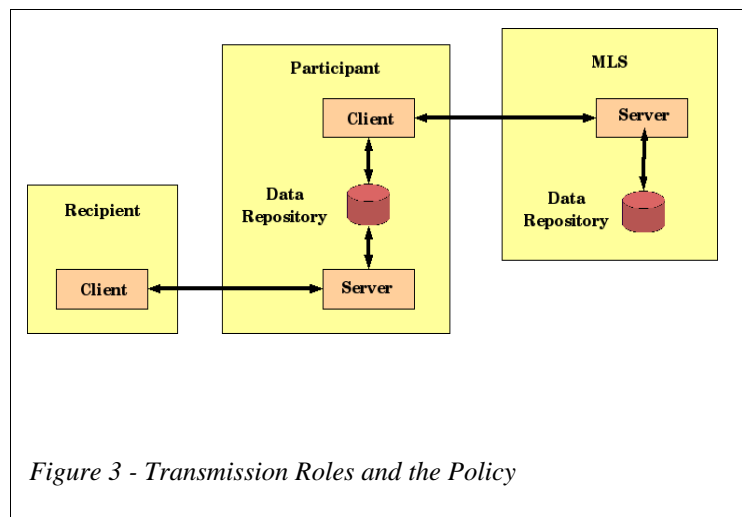
The act of transmitting data can be initiated by either the Server or the Client. If the Server initiates the transmission, the transmission is called a "push" transmission since it is the Server that is aware of updates that are available to interested Clients. If the Client initiates the action, the transmission is called a "pull" transmission, because the Client asks for a refresh of its information without knowing if new information is available. Both "push" and "pull" transmissions use rules to govern transmissions. These rules are called the "protocol" and detail exactly how the two machines handle details of the movement like "failure processing" and "handshaking".

Popular "push" protocols include the Simple Mail Transfer Protocol (SMTP) and the File Transfer Protocol (FTP). SMTP is commonly called e-mail and FTP is commonly used by Brokers to upload property information to an MLS.

Popular “pull” protocols are Hyper Text Transfer Protocol (HTTP) and FTP. HTTP is the protocol that supports web pages and FTP is used by Brokers to download property information from an MLS. The Real Estate Transaction Specification (RETS) standards are based upon the HTTP protocol.

On the Internet, the use of FTP has been declining in favor of more secure approaches such as Secure Shell (SSH). There is not widespread use of SSH in real estate today. Participants and MLS who might be interested in this more secure mechanism can obtain SSH, in Open Source form, at no cost.

The terminology used in the VOW policy can be directly linked to the roles used to describe data transmission. Beginning with simple cases first, the MLS as the source of data performs the role of a “server”. The Recipient, as an entity that is interested in receiving information, performs the role of a “client”.



A more complex entity to examine with respect to transmission roles is the Participant. When receiving information from the MLS, the Participant acts in the “client” role. When servicing the Recipient, the Participant role changes to a “server” role. Because the Participant's role shifts from “client” role to “server”, it is important to consider that there may be a copy of the MLS datafile on the Participant's server. This copy may be written to the hard drive, in which case, the data feed would be termed “persistent” since data resides on an ongoing basis on the Participant's server. **Figure 3 – Transmission Roles and the Policy** illustrates these concepts.

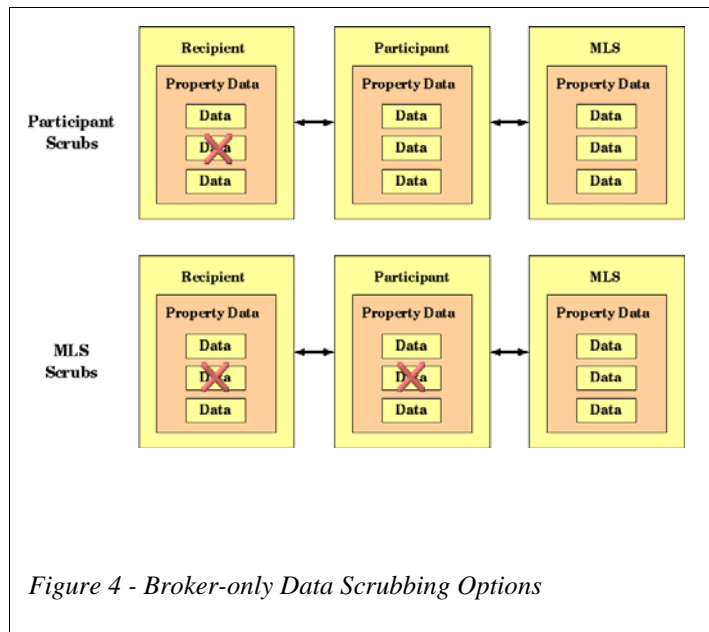
A copy of the MLS data, on the hard drive, is not essential for a Participant to perform the “server” role for a Recipient. It is possible for the Participant to use software that performs the “client” and “server” roles without writing a copy of the MLS database to the hard drive. This approach uses the server's memory to store data while switching roles. The common term for this approach to data storage is called making a “transitory”

copy of the data. If the computer is shut down during the process, the data being moved is lost.

From the security perspective, “transitory” data transfer approaches are preferable to “persistent” approaches because data is always more secure if there is not a copy available on the hard drive. Once data is on the Participant's hard drive, it is available for anyone with access to the Participant's server. Anyone with access to the data can copy it onto a diskette (or “burn” a CD), e-mail the data to a friend, or send a copy to a printer. This is the single most popular method of fraud and abuse of electronic data. The press popularizes computer “break-ins” because they are more sensational, but most abuse is actually “inside jobs”.

### Removing “Broker-only” Information

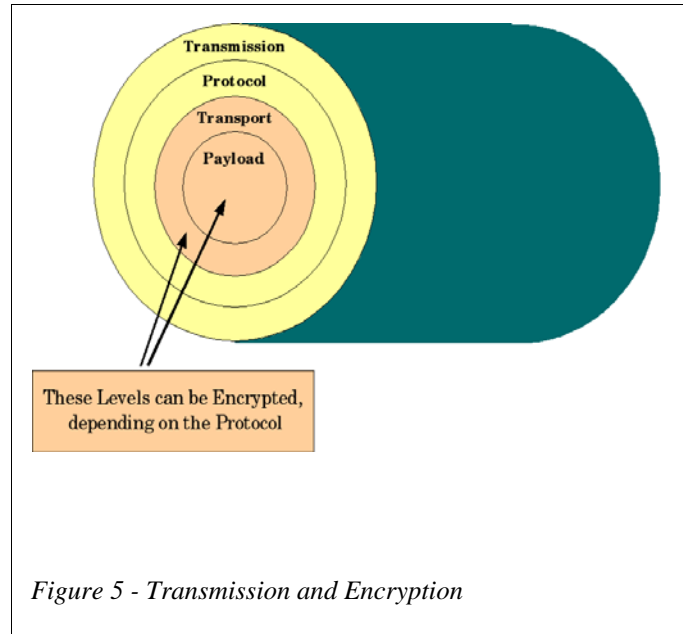
The policy requires Participants not to make information intended exclusively for potential cooperating Participants available to consumers. This includes cooperative compensation, type of listing agreement, certain seller information and property showing/security information. Removing this information prior to transmission to consumers is a process called “scrubbing”.



There are two approaches to “scrubbing” VOW data. The first is for the MLS to “scrub” before transmission to the Participant; the other is for the Participant to “scrub” before transmission to the Recipient. Transmitting “scrubbed” data from the MLS is preferred because data is more secure if it doesn't exist. If the Participant does not receive “broker-only” data as part of their VOW data feed, it can't be transmitted to Recipients.

Rules for “scrubbing” are best applied at the source of the data, the MLS. **Figure 4 – Broker-only Scrubbing Options** illustrates this concept.

## Data Encryption



The next level of security involves understanding how data is packaged during data transmission. This understanding will aid the later discussion of encryption technology. A protocol facilitates moving data with a mechanism called a “transport”. The “transport” provides information about actual data being transmitted. The information contained in the “transport” is called “headers”.

The actual user data moved by a “protocol” is called a “payload”. A good analogy to apply to protocols comes from the postal service; the “transport” being the envelope and the “payload” being the letter inside the envelope. **Figure 5 – Transmission and Encryption** illustrates these concepts.

Encryption is a complex topic that can be simplified for our purposes as the scrambling of data so that it is no longer “human readable”. The process of scrambling data is commonly called “encrypting”, while the unscrambling is commonly called “decrypting”.

Both “encrypting” and “decrypting” are performed using special strings of data called “keys”. Keys are used to drive mathematical models (algorithms) that convert “human readable” text into unrecognizable characters. A simple example of encryption uses a number to represent the number of characters by which a “plain text” string would be “shifted”. For example, if the key was the number 1, the word VOW would be converted

to WPX. Modern encryption is exponentially more sophisticated and is very difficult to decipher or “crack”. The process of “cracking” is finding the key with no information other than the encrypted string. Guessing passwords to computers is a basic example of “cracking”.

Some of the key terms used in encryption technology are:

- Public Key Infrastructure (PKI)
- Asymmetric Cryptography
- Digital Certificates (an artifact used in Asymmetric Cryptography)
- Symmetric Cryptography
- Password (an artifact used in Symmetric Cryptography)

A detailed discussion of these encryption approaches is outside the scope of this paper.

The protocol used in data transmission determines whether it is the transport or the payload that is encrypted. One popular encryption protocol used to secure e-commerce transactions is closely related to HTTP and is called Secure HTTP (HTTPS or S-HTTP). The difference between HTTP and HTTPS is that the web pages the consumer sees with HTTPS are encrypted at the “payload” level and there is special information in the “transport” facilitating decryption.

HTTPS protects data in transit, and does not control the usage of the data. If the desired effect is to ensure that the data arrives at its intended destination, HTTPS is helpful. If the desired effect is to control the use of information after the Recipient receives it, HTTPS is not very helpful at all.

The HTTPS protocol is built-in to most web servers today. When a Recipient is accessing the Participant's web site with HTTPS, most browsers show a padlock symbol in the lower left hand corner.

#### **IV. Registration**

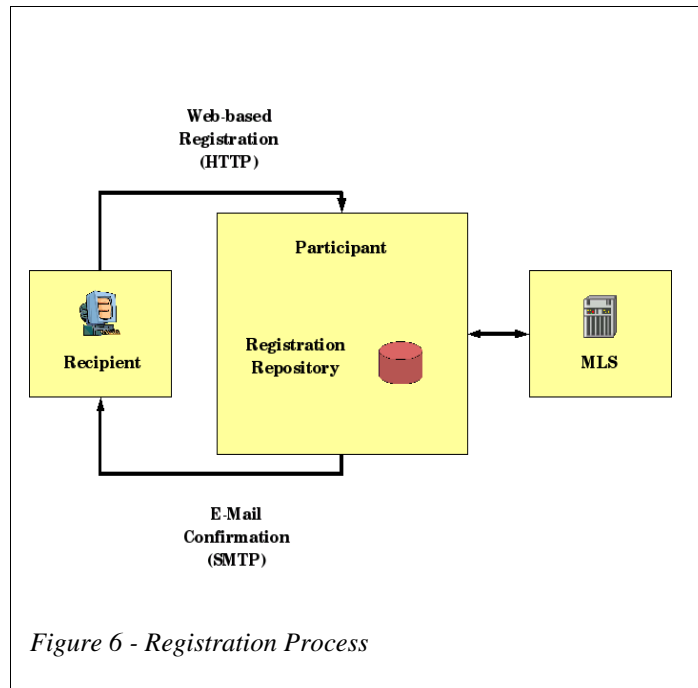
The registration mechanism outlined in the VOW policy requires Recipients to provide two pieces of information; the consumer's name and an e-mail address. Only a Recipient's e-mail address is validated. **Figure 6 – Registration Process** illustrates this concept.

The e-mail information entered by the Recipient is validated when the Participant confirms registration by sending a return e-mail via the SMTP protocol.

A valid, operational e-mail address does not identify an individual. Within a security context, a valid e-mail address only ensures that e-mail sent by a Participant is actually being received by the person using that e-mail address. It is very difficult to determine



the actual identity of any individual who is using the e-mail address. Tracing an individual requires cooperation of the Internet Service Provider (ISP) operating the domain. In some cases, the identity of e-mail users is not actually kept or even known by the ISP. An example is “free” e-mail services and promotional CD's offered to the public. In these cases, users are anonymous. If there is no charge for the service, the ISP does not ask for credit card information.



The registration information must be made available by the Participant to the MLS upon request. There is no assurance that the name supplied by the Recipient will be of use in instances where false information has been supplied and MLS data is misappropriated.

The anticipated costs to Participants to implement the Registration mechanism established in the policy is between \$500 and \$4,000. The lower end of the range represents only that part of a commercial VOW package performing the registration function. The higher end of the range represents what fees a Participant could expect to pay for a third party consultant to develop/implement a customized registration solution.

## V. Privacy Policy

This section focuses on the privacy of Recipient's information. The policy requires that a privacy policy needs to be displayed to consumers during the registration process. Consumers should be informed why the registration information is being requested and how it may be used. This is especially important due to the relationship between Participants and the MLS. The privacy policy should disclose that consumer-supplied passwords will be provided to the MLS when a security breach is suspected.

Privacy policies are common practice on the Internet, especially when requesting information from consumers. Many consumers will not provide information without the disclosures of a privacy policy being made to them.

It is also important to consider that passwords only demonstrate that the consumer knows the password, and passwords cannot be used to identify the consumer.

## VI. Breaches of Security

The policy provides that if an MLS believes a breach in security has occurred, the MLS will request Recipient registration information from the Participant(s). Registration information includes the name and e-mail address.

Potential "misusers" will almost certainly give false registration information, while having a "validated" e-mail address. They will almost always be aware of the difficulty of tracking down an individual based solely on their e-mail address.

The Recipient information (as discussed in the Registration process section of this document) is not a reliable means of identification. The account information cannot be used to identify particular consumers. In the case of a suspected breach, relying on the measures presented in the policy, it will be very difficult to identify individuals misusing VOW information.

One technique to identify breaches and prevent subsequent misuse is to audit Recipient's activity on Participant's VOW. This involves detail as to when a particular consumer was "on" a Participant's VOW; what information was transferred, etc.

In addition to security uses, however, audit information can be used to gauge overall marketing effectiveness by businesses using the the Internet. This is the Internet equivalent to looking at metrics like response rates on mailers or demographic profiles associated with lead generation tools. The **Data Misappropriation** section of this document deals with audit trails in more detail.



Participants providing Recipient data to MLS can expect to pay between \$200 and \$3,000 for the capability. The lower end of the range represents that portion of a commercial VOW package performing the function as part of a comprehensive VOW package. The higher end of the range represents the fees a Participant could expect pay for a third party consultant to develop /implement the necessary software.

The policy does not discuss the type of transfer mechanism that is to be used by the Participants when an MLS requests Recipient information. Because this information includes user names and passwords (as well as consumer information), the security of this transmission is important. Choices that the Participant has includes FTP, SMTP, HTTP, S-HTTP or SSH. More information about these mechanisms can be found in the **Data Transmission** section of this document.

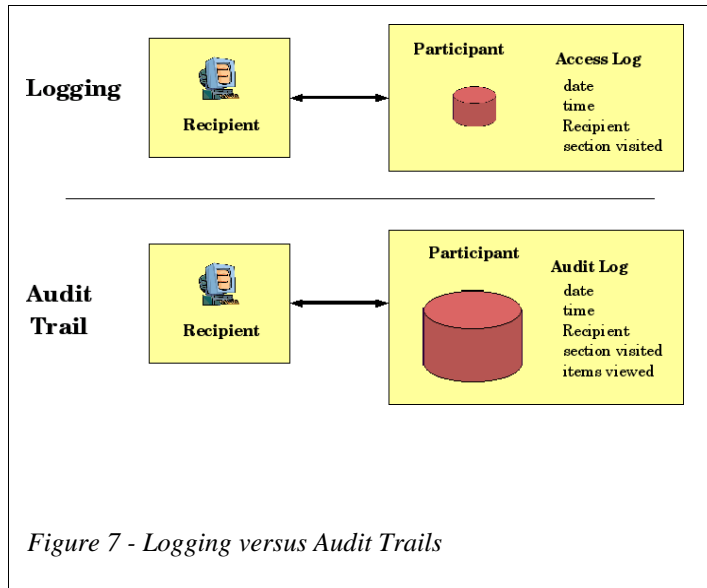
## **VII. Data Misappropriation**

The policy obligates Participants to monitor and prevent “scraping” or misappropriation of the data from their VOW sites. Although the policy does not require audit trails, “monitoring” arguably implies Participants will keep track of Recipient access attempts.

Tracking of data access attempts can be accomplished either through simple logging, or through a detailed auditing mechanism. Logging keeps a simple list of when and who attempts to access the site in an “access log”. Auditing is much more complex because it involves recording who sees what pieces of information in an “access log”. Before a page is sent to the Recipient, auditing VOW servers record an entry for every field and image that the transmission includes. By example, a VOW site that displays twenty field of information would require at least twenty entries per view with auditing versus one entry per view with logging. Auditing requires more disk space and processing than simple logging, driving up the cost. **Figure 7 – Logging versus Audit Trails** illustrates this concept.

Although auditing is much more expensive than logging (due to its complexity), it provides benefits beyond the obvious security uses. Just as a business might employ a general manager to oversee operations, software that analyzes audit logs can identify “patterns” of usage by customers and help businesses determine the effectiveness of their marketing efforts. Pattern detection is also called audit trail analysis.





Logging information can also be used to identify “patterns” but only from the access perspective. All web servers have logging built-in, making this measure inexpensive for Participants to implement. Logging information does not serve the business planning function like audit trails do.

From a security perspective, audit trails can be used to identify “patterns” of use that may actually be misuse. One example would be heavy downloads by a series of Recipients within a very short time period. These cycles, if happening at the same time of the day, could actually be a single entity “farming” the VOW with multiple “fake” registrations.

Participants can expect to pay between \$1,000 and \$6,000 for audit trail capability. The lower end of the range represents that part of a commercial VOW package performing the audit trail function. The higher end of the range represents the fees a Participant could expect to pay a third party consultant to develop/implement audit trail software.

Taking data from Internet websites is commonly referred to as “screen scraping”. It is important to understand how “screen scrapers” work before discussing measures to prevent it.

Web pages are created using language called HyperText Markup Language (HTML). HTML packages data and images with formatting instructions allowing browsers to “render” a view of the data. HTML itself is human readable or in other words, in “plain text” format. **Figure 8 – Scrapers and HTML** presents this concept.

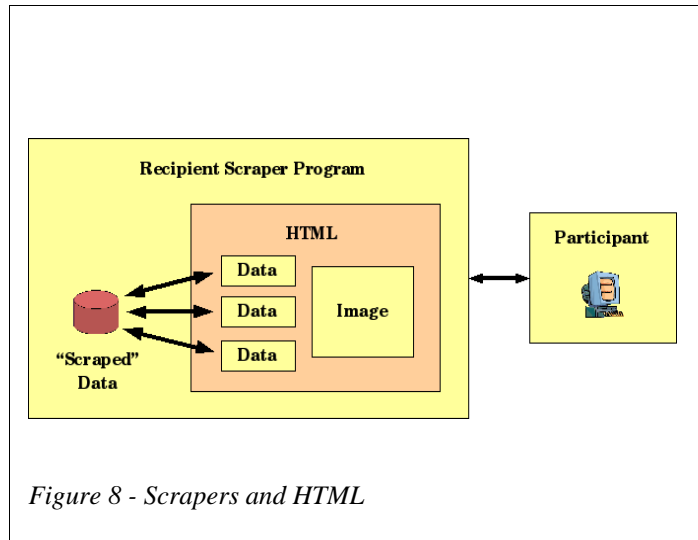


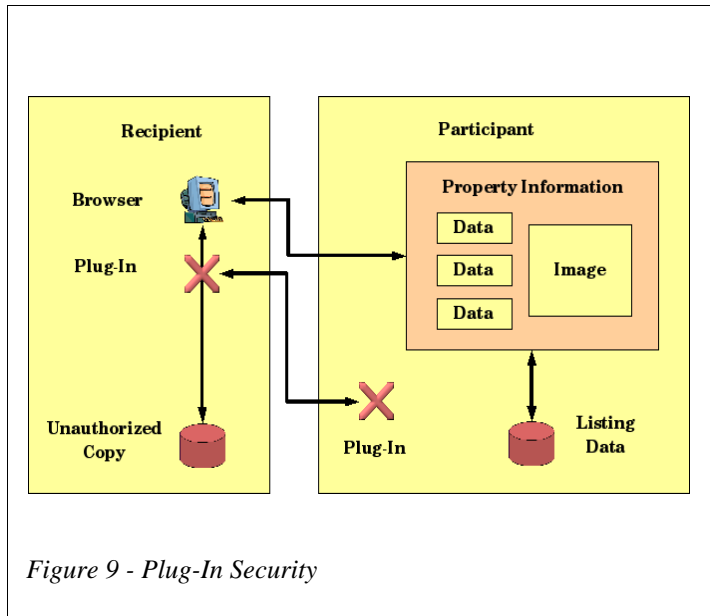
Figure 8 - Scrapers and HTML

“Scraper” software depends on the “plain text” nature of HTML to operate. A “scraper” connects to a server and “masquerades” as a legitimate browser. Typically, the server cannot tell the difference between a “scraper” and a browser.

There are three general approaches to preventing screen scraping, each having a different level of effectiveness. The first, and most inexpensive approach to defeating “scrapers” is have the server ask the client software to “identify” itself. The server then checks the client's response (usually the manufacturer's name) against a list of acceptable browsers. More sophisticated “scrapers” are aware of this technique though, and typically identify themselves as being a version of Microsoft's Internet Explorer.

A second approach uses the “plug-in” capability built into browsers. The server asks the browser if a specific plug-in is present in the browser. If it is not, the server sends the plug-in to the browser. If it is present, further communication is conducted between the plug-in and the browser in an encrypted manner. The plug-in then passes information to the browser for rendering. Some plug-in programs even disable browser functions such as cut-and-paste or printing. **Figure 9 – Plug-In Security** illustrates this concept.

Participants may expect to pay between \$100 and \$500 for commercial plug-ins that disable browser functions.



A new class of “plug-ins” with Digital Rights Management (DRM) capabilities built in will hit the Internet over the next couple of years. DRM is the ability to control what a consumer can do with information once it has been accessed through a browser. This is achieved by either encrypting the data transmission, or by using a “digital watermark”. The business purpose driving development of DRM was the downloading of music files. The DRM approach is often termed “getting a footprint” on the consumer's browser. DRM plug-ins are controversial because they eliminate the “freedom” consumers enjoyed before Intellectual Property rights on the Internet became a major issue.

A downside of DRM plug-ins is that consumers are wary of plug-ins because they modify (or remove) functionality on consumers' computers. Because consumers don't understand how the disabling of functionality happens, they are wary of it and are less likely to use it, even if it is offered at no charge. Because human nature is at play, the “no charge” offer can accentuate aversion to things not understood. The counter to this would be to create a compelling case for the benefits of the information that can be accessed with plug-ins. In the case of DRM, consumers have not yet been convinced of the value.

Browsers or “scrapers” that do not have the plug-in (DRM or disabling) are unable to view the information. Only the most sophisticated “scrapers” would come close to matching the plug-in capabilities of a browser. The act of “scraping” is supposed to be a cheap endeavor, making this level of “masquerading” economically unfeasible

Participants can expect to pay between \$500 and \$8,000 for DRM plug-in capabilities. The lower end of the range represents the portion of a commercial VOW package performing the “plug-in” processing. The higher range of the cost represents the fees a

Participant could expect to pay for a third party consultant to develop/implement “plug-in” software.

The third approach provides the best defense against “scraping”; the Participant sends only an image to the Recipient. The image resembles a page from a brochure and includes both property information (textual format) and graphic images. With this approach, a scraper looking for textual information finds only an image. The party looking to misappropriate property information would have to “re-key” the information, which is time consuming and costly. **Figure 10 – Single Image Security** illustrates this concept.

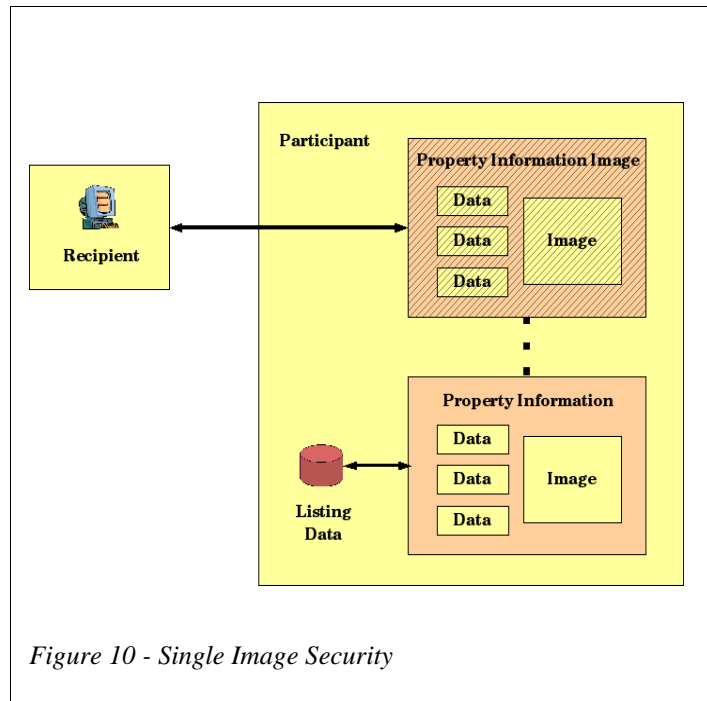


Figure 10 - Single Image Security

The single image approach is used by companies working with financial information. Account numbers and other sensitive consumer information is sent over the Internet as a image providing an additional level of security.

There are two downsides using single images to defeat “scraping” software. The first is availability of software. The commercial software market is not following this approach because of their business interest in installing software in consumer's browsers, the so called “getting a footprint” on the browser. The single image approach does not require installing additional software on Recipient's computers.

The other downside is providing service for sight-impaired Recipients. Sight-impaired consumers can use special browsers that “read” websites and generate an audible version for users. The technology behind these special browsers is identical to the “scrapers”

discussed earlier. Single image measures would prevent the sight impaired from accessing information from VOWs.

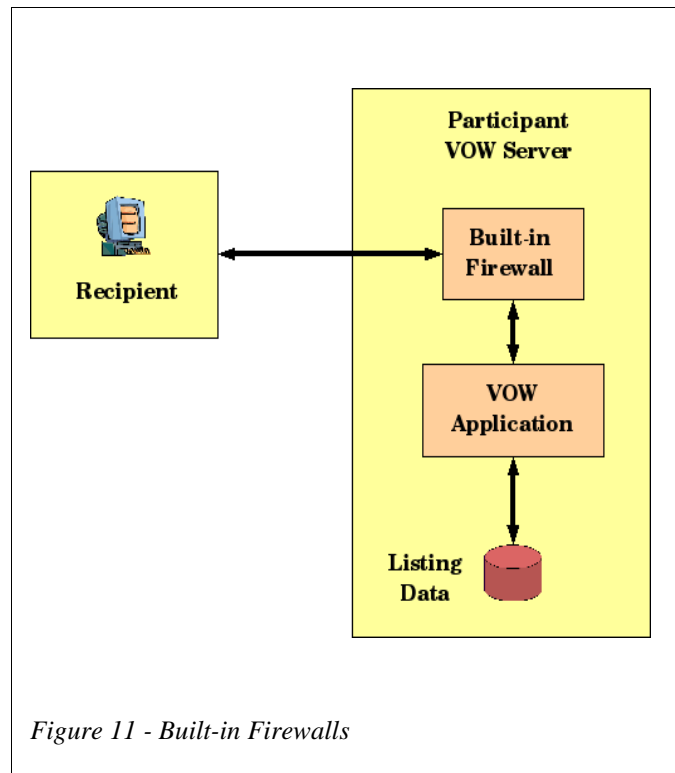
Participants can expect to pay between \$300 and \$4,000 from single image capabilities. The lower end of the range represents the portion of a commercial VOW package performing the “imaging” function. The higher end of the range represents the fees a Participant could expect to pay for a third party consultant to develop/implement imaging software.

### VIII. MLS Required Security

The policy states the MLSs that utilize “persistent” downloads to enable Participants' VOWs may require Participants to utilize firewalls to protect their VOWs. Firewalls and other intrusion-prevention approaches are part of the overall security scheme that anyone conducting business over the Internet should have in place.

Firewall technologies can be divided into three major categories. In ascending order of effectiveness, the following sections describe each type of firewall.

#### Built-in Firewalls



A built-in firewall uses rule-based filtering and other techniques on the web server to provide a measure of intrusion protection. Filtering rules are applied to all traffic entering or leaving the computer to accept or reject data based on the identity of the other computer. An example of a rule is to only accept FTP requests from known computers. **Figure 11 – Built-in Firewalls** illustrates this concept.

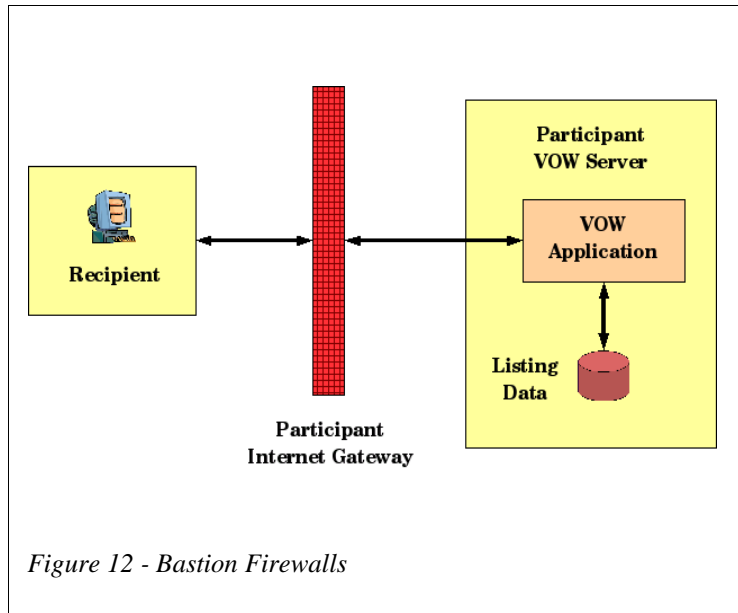
Built-in firewalls are typically bundled with the Operating System when new computers are purchased and would be the most inexpensive and simple firewall approach that can be chosen by VOW operators. The firewall operates on the same computer that acts as a server to the Recipient.

Positive points of Built-in Firewalls are that they are inexpensive and easy to setup/configure. The downsides are that attempts to compromise the VOW must pass through the security of a single computer and that most computer owners do not bother to (or incorrectly) setup/configure their firewalls properly.

### **Bastion Firewalls**

A bastion firewall uses a dedicated computer that acts as the gateway between the Internet and the internal network of computers. Separating the networks is important to security because the only access to the protected computers comes through the gateway computer. Access rules can be written specifically for the gateway computer instead of in a generalized fashion for many known computers on the Internet. **Figure 12 – Bastion Firewalls** illustrates this concepts.





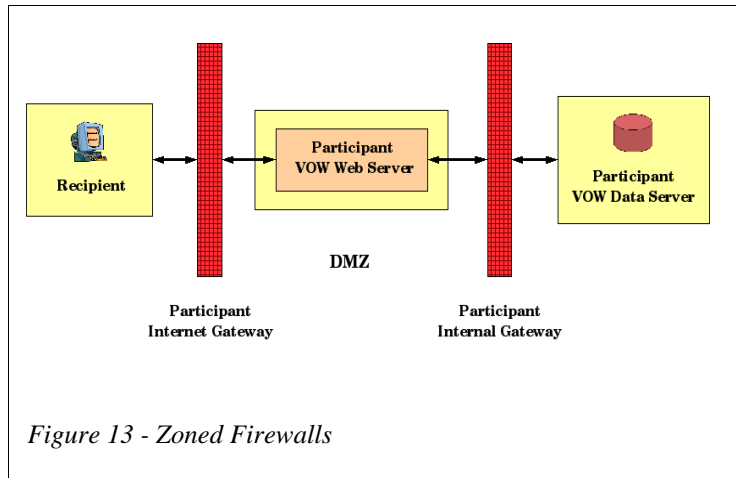
Participants using a bastion firewall will need a dedicated computer (in addition to the VOW server). This represents an additional cost of between \$1,000 and \$3,000. Third party consultants may be required to setup bastion firewalls at a cost of approximately \$3,000.

The positive point of Bastion Firewalls is that any attempt to compromise the VOW site must pass through the security of two machines; the bastion computer and the VOW server. The negative points are the expense and complexity of configuring.

### Zoned Firewalls

Zoned firewalls use one machine to act as gateway between the Internet and the “DMZ” and a second machine is used as a gateway between the “DMZ” and the internal network of machines. The DMZ is a common term used to describe a network of computers that service Internet requests such as Web servers, DNS and FTP servers. Data servers operate on the internal network, separate from computers in the DMZ. **Figure 13 – Zoned Firewalls** illustrates this concept.

If a Participant uses a zoned firewall the VOW is separated into two separate web and data servers. This arrangement requires four dedicated computers in total. Two of these computers act as gateways, one as a VOW web server and the fourth as a VOW data server. This represents an additional cost of between \$4,000 and \$8,000. Implementing Zoned Firewalls is technologically complex and will cost between \$1,500 and \$5,000 to have a third party consultant implement.



The positive points of Zoned Firewalls are their flexibility and ability to stop intrusion attempts. They are designed to handle many different kinds of Internet requests (HTTP, DNS, etc.). VOW information requests are only one type of Internet request (HTTP) . If a Participant wanted to add services in the future, they would be easier to add with Zoned Firewalls. Any attempt to compromise the VOW site must pass through the security of three machines; the gateway to the Internet, the gateway to the internal network and the VOW data server.

The negative points are the expense and complexity. A Participant may never need to add the kind of services that Zoned Firewalls are designed for, making the implementation cost ineffective.

### **Firewall Conclusion**

Most MLS operations utilize either Bastion or Zoned style firewalls. Most Participants utilize Single Server firewalls. The cost difference and effectiveness between the implementations is considerable. The policy might lead an MLS to specify that Participants use the same style of firewall that the MLS uses.

## IX. Glossary of Terms

The following terms relate to topics addressed in this paper and are defined as follows in the on-line encyclopedia Webopedia (<http://www.webopedia.com>).

<b>Asymmetric Encryption</b>	See Public-key Encryption.
<b>Bastion Host</b>	A bastion host is a gateway between an inside network and an outside network.
<b>Bits</b>	Short for binary digit, the smallest unit of information on a machine.
<b>Client</b>	An application that runs on a personal computer or workstation and relies on a server to perform some operations.
<b>Computer</b>	A programmable machine.
<b>Decryption</b>	The process of decoding data that has been encrypted into a secret format.
<b>Digital</b>	Describes any system based on discontinuous data or events.
<b>Digital Certificate</b>	An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.
<b>DMZ</b>	A Demilitarized Zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network.
<b>DNS</b>	Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember.



<b>DRM</b>	Short for Digital Rights Management, a system for protecting the copyrights of data circulated via the Internet by enabling secure distribution and/or disabling illegal distribution of the data.
<b>E-mail</b>	Short for electronic mail, the transmission of messages over communications networks.
<b>Encryption</b>	The translation of data into a secret code.
<b>Gateway</b>	A node on a network that serves as an entrance to another network.
<b>Firewall</b>	A system designed to prevent unauthorized access to or from a private network. See Bastion Host and Zoned Firewalls.
<b>FTP</b>	Abbreviation of File Transfer Protocol, the protocol used on the Internet for sending files.
<b>HTML</b>	Short for HyperText Markup Language, the authoring language used to create documents on the World Wide Web.
<b>HTTP</b>	Short for HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.
<b>HTTPS</b>	Identifies Secure HTTP (or S-HTTP); the ability to operate HTTP over SSL.
<b>IMAP</b>	Short for Internet Message Access Protocol, a protocol for retrieving e-mail messages.
<b>Internet</b>	A global network connecting millions of computers.
<b>Intrusion</b>	An attempt to break into or compromise a system.



<b>IP address</b>	An identifier for a computer or device on a TCP/IP network.
<b>Key</b>	A password or table needed to decipher encoded data
<b>Machine</b>	See Computer.
<b>Module</b>	A part of a program.
<b>Networks</b>	A group of two or more computer systems linked together.
<b>Node</b>	A processing location on a network.
<b>Open Source</b>	A program in which the source code is available to the general public for use and/or modification from its original design free of charge.
<b>Operating System</b>	The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.
<b>Packet</b>	A piece of a message transmitted over a packet-switching network.
<b>Packet Filter</b>	Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules.
<b>Packet-switching</b>	Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message. TCP/IP is a packet-switching network.
<b>Password</b>	A secret series of characters that enables a user to access a file, computer, or program.



<b>Payload</b>	The data section of a transmission.
<b>PKI</b>	Short for Public Key Infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.
<b>Plug-in</b>	A hardware or software module that adds a specific feature or service to a larger system.
<b>POP</b>	Short for Post Office Protocol, a protocol used to retrieve e-mail from a mail server.
<b>Program</b>	An organized list of instructions that, when executed, causes the computer to behave in a predetermined manner.
<b>Protocol</b>	An agreed-upon format for transmitting data between two devices.
<b>Public-key Encryption</b>	Also called Asymmetric Encryption. A cryptographic system that uses two keys – a public key known to everyone and a private or secret key known only to the recipient of the message.
<b>Pull</b>	To request data from another program or computer. The opposite of pull is push, where data is sent without a request being made. The terms push and pull are used frequently to describe data sent over the Internet.
<b>Push</b>	To send data to a client without the client asking for it.
<b>S-HTTP</b>	See HTTPS.
<b>Server</b>	A computer or device on a network that manages network resources.
<b>SMTP</b>	Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers.
<b>SSH</b>	Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.



<b>SSL</b>	Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet.
<b>Symmetric Encryption</b>	A type of encryption where the same key is used to encrypt and decrypt the message.
<b>System</b>	See Computer.
<b>TCP/IP</b>	Abbreviation for Transmission Control Protocol/Internet Protocol, the suite of communications protocols used to connect hosts on the Internet.
<b>Transmission</b>	See TCP/IP
<b>Transport</b>	The portion of a transmission that provides instructions about payload handling.
<b>Trust Hierarchy</b>	See PKI.
<b>Watermark</b>	A pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.).
<b>Zoned Firewall</b>	A firewall that uses two machines to form a DMZ.

