Security Overview

Introduction

ShowMyPC provides real-time communication services to organizations and a large number of corporations. These corporations use ShowMyPC services for diverse purposes ranging from support, marketing, project management and sales. These corporations represent a variety of market sectors including technology, finance, manufacturing and healthcare. ShowMyPC endeavors that its service offerings meet the most security requirements of corporations so they can use ShowMyPC services effectively and routinely, secure in the knowledge that their sessions are safe and private.

ShowMyPC assigns data security the highest priority in the design, deployment and maintenance of its network, platform and services.
The purpose of this document is to provide information on the data security features and functions that are available in the various ShowMyPC services and inherent in the underlying ShowMyPC communication infrastructure. We discuss the following items in this document:

- Application
- User Interface
- Architecture
- SSH/SSL Encryption
- Facilities Security

ShowMyPC services include:

- Meetings for highly interactive sessions
- Training to deliver the most effective training via the Web
- Web-based seminars
- Support Center, optimized for helpdesk and support sessions

Application

ShowMyPC implements security at the application layer primarily using ShowMyPC SSH client and several local machine software components that make data collaboration possible by coordinating with ShowMyPC Services clusters servers located across the globe. The ShowMyPC SSH Core has many features that make it a safe and secure method for data collaboration.
It is impossible to participate in a ShowMyPC session without the close coordination between the SSH Core and the ShowMyPC Services cluster. Since the data in a ShowMyPC session is shared using the SSH Core software, which must establish a connection with a ShowMyPC Service cluster, these security features are inherent throughout the session. In short, each session is dynamic and involves a handshake between the client and the ShowMyPC Service cluster, and the communication between these components is by default encoded and optionally SSH/SSL encrypted.

Firewall Compatibility

The ShowMyPC SSH Core communicates with the ShowMyPC Services cluster to establish a reliable and secure connection. At the time of client instantiation, the ShowMyPC SSH Core attempts to determine the best path for communication. In the process of establishing this connection, the ShowMyPC SSH Core attempts to connect using TCP/HTTP/HTTPS (port 80/443). ShowMyPC travels over firewall friendly ports. ShowMyPC SSH Core will tunnel all ShowMyPC session initiation activity using HTTP/HTTPS. ShowMyPC site incorporates an SSH/SSL connection, all the traffic is carried over HTTPS (port 443). Regardless of the connection that is established at the time of client instantiation, by establishing this communication between the SSH Core and the ShowMyPC Cluster, firewalls do not have to be specially configured to enable ShowMyPC sessions.

Content Security

ShowMyPC provides several controls to prevent unwittingly sharing data. Unlike other Web conferencing solutions, ShowMyPC restricts application sharing to specified applications. With ShowMyPC, when a Presenter shares a web page or a specified application, other applications running on the Presenter's desktop will not show on Participants' machines.

Finally, ShowMyPC is the only provider of 256-bit SSH encryption that encompasses all session data, from the session creation and join pages, to the actual session itself, to the Web pages that follow an interactive session.
ShowMyPC provides a highly secure environment for data collaboration. The ShowMyPC Application Core is designed to deliver in real time, rich-media content securely to each Participant within a ShowMyPC session. All content that a Presenter shares with the participants in a ShowMyPC session is only a representation of the original data. In addition, all content that is shared with the participants in the session is encoded with a proprietary encoding process.

The ShowMyPC SSH Core Application:

- Can be started as application and Viewer can be on Mac and Linux with appropriate JRE 1.4 or above.
- Is the only application to provide the option to deploy private servers to isolate Conference data to individual clients
- Can optionally be certified with a signed certificate of Clients Company, or one that ShowMyPC provides
- Is the only means possible to participate in a ShowMyPC session
- Is entirely dependent upon connections established on a session basis with the ShowMyPC cluster
- Performs an industry standard encoding process that encodes all shared data.

The encoded content contains no executable code and it is viewable only by the ShowMyPC SSH Core.
ShowMyPC Services never sends session content in clear text. Prior to sending information from a Participant's SSH Core to the ShowMyPC Service Cluster, the ShowMyPC SSH Core encodes all data in a SSH format. Moreover, ShowMyPC uniquely identifies session Participants with individual session IDs that ShowMyPC uses to thwart hackers from reassembling session content. These techniques provide safeguards to prevent reconstruction of the data conferencing portion of the ShowMyPC session. VNC inherently can protect against repeated session gain attempts.

Session Security

In every ShowMyPC session there is only a logical connection between each local machine via the ShowMyPC Cluster; there is no direct network connection between the local machines. The logical connection is fixed and only application functions can be performed. There is no way to perform general-purpose tasks outside of what the ShowMyPC Service allows.

A ShowMyPC session connection is composed of several layers superimposed on one another. The lowest layer is TCP/IP that allows for general data communication and underlies all communications. Above this is the application (web) layer that provides for logical connection of a web browser to a web server. The ShowMyPC SSH Core software, which establishes an end-to-end connection between the SSH Core software and the ShowMyPC Cluster, also communicates at the same application layer as the web browser.

Each layer serves a different purpose and has different capabilities. While the lowest level provides arbitrary data communications, higher layers are more specific and less flexible in what can be done. As each layer is established, the network connection is further constrained by the limitations of each layer.
The end result being that the total connection is limited to what can be done at the ShowMyPC layer.
The layers can be characterized by connection flexibility, protocols used and capabilities allowed. The following table summarizes each layer.

Client Connection Security

Every ShowMyPC SSH Core connection must authenticate properly prior to establishing a connection with the ShowMyPC cluster to join a ShowMyPC session. The client authentication process uses a unique, per client, per session token to confirm the identity of each Participant attempting to join a ShowMyPC session. Each ShowMyPC session has a unique set of session parameters that are generated by the ShowMyPC Service cluster.

Each authenticated Participant must have access to these session parameters in conjunction with the unique session token in order to successfully join the ShowMyPC session.

TCP/IP Can be used to create connections between network components. TCP/IP Capabilities allowed subject to limits imposed by network security (e.g. firewalls). Although TCP/IP underlies all communications, it is only directly used
by the web browser to initiate a connection to a web server. In many cases, this will be a connection to a proxy server that is internal to the respective company. There are no other connections being initiated outside of the web connection. Currently ShowMyPC may not work with every possible proxy network.

Web Can only be used to establish a connection between a web browser and a web server. Connection must be initiated by the web browser and made OUTBOUND to the web server. HTTP, SSH/SSL HTTP allows a rich data stream that can implement a wide variety of application-specific capabilities. The Web layer provides a secure connection between the web browser and the web server. No other use of the connection is allowed. Once established the endpoints are fixed.

ShowMyPC Endpoints are fixed between the ShowMyPC Server and the Web browser plug-in. Industry standard SSH protocols specific to ShowMyPC services Capabilities are defined explicitly by the ShowMyPC server and the application running in the web browser. No other capabilities allowed. ShowMyPC components are running on each end of the connection.

User Interface

ShowMyPC security is also enforced through a variety of mechanisms exposed through the ShowMyPC user interface which include web pages devoted to site maintenance, Host profiles, and creating sessions, as well as the session interface itself.

Roles and Responsibilities

There are 2 roles in a ShowMyPC session – Host and Participant A Host can create, schedule and maintain ShowMyPC sessions. Only the Host can view and edit these session parameters. Hosts are identified and created either by self-registration, a site administrator or via ShowMyPC on behalf of our customer. (Self-registration can be disabled. Password protection of the website is available)

Meeting Parameters

Hosts can specify the following meeting parameters relating to security:
• Unlisted meetings
• Meeting passwords
• Participants must have a Host ID to connect.
When a meeting is created, ShowMyPC assigns a randomly generated, non-sequential meeting number to uniquely identify the meeting. Unlisted meetings ID appear on the user interface. They are accessible through a link sent via the email invitation process or by a Participant explicitly providing the meeting number on the ShowMyPC join page. In either case, the Host must explicitly inform the Participant of the existence of the meeting.
The ShowMyPC site can also be configured to disable email invitations. This allows the Host greater control over the distribution of the meeting access information.

Host and Participant Privileges

Only a Host can start a ShowMyPC meeting. Each Host is required to log on to the ShowMyPC site with a Host ID and password. Once the Host is authenticated on the site, the Host can start a ShowMyPC meeting. The Host has the first level of control in the meeting and is made the Presenter. The Host can also terminate his session at any time.

A Participant within the ShowMyPC session can view the data and file system of remote Host that is being shared by the Presenter.

Site Administration Configuration

ShowMyPC Site Administration permits password configuration.

- Change and apply password to the main client site
- All meetings must have a password.
- Ability to have View or Present only application binaries.

Summary of Host responsibilities:

- Start/Schedule ShowMyPC meetings
- Restrict access to the meeting
- Terminate ShowMyPC meetings
- Setup optional US based teleconference number, can call in up to 99 users.

Capabilities that are available to the Presenter:

- View the list of Participants in the session.
- Enable Participants to send text messages to other Participants, the Presenter (or both).
- Enable Participants to record the session.

Architecture

ShowMyPC uniquely deploys a globally distributed network of high-speed switches. With this architecture, session data originating from the Presenter's machine and arriving at the Participants' machines is switched – never stored -- through the ShowMyPC Cluster. No session data is stored on the ShowMyPC cluster; ShowMyPC sessions are completely transient.

It is useful to compare the ShowMyPC switching network with the telephone system, where voice is carried across the PSTN in a sophisticated, switched manner. From a security standpoint, this architecture has an advantage in that there is no persistent storage of any session data within the ShowMyPC infrastructure. There is no need to upload content to the ShowMyPC Services cluster; dynamic session content displayed during a ShowMyPC session originates only from the Presenter's machine; Participants see only representations of this data. At the conclusion of a session, all such representations dissipate – similar to what happens when a voice telephone call terminates. Like the phone system all that remains of a ShowMyPC "data call" is ancillary information like billing records, not a record of the conversation itself.

ShowMyPC has invested much time and energy into developing and deploying a secure environment for our services. ShowMyPC employs state of the art firewalls, network monitoring, and intrusion detection tools. Production servers undergo a hardening process prior to deployment. Strict change management is employed and additional policies and procedures are enforced. To further ensure adherence to best practices with respect to data security.

SSH/SSL Encryption

In addition to all the safeguards discussed herein, for utmost security, ShowMyPC provides the option of securing all session content with 256/128-bit encryption using Secure Sockets Layer (SSH/SSL), which is the most widely used Internet standard for securing sensitive data communications. With SSH/SSL, ShowMyPC encrypts all data within a ShowMyPC Service cluster, including the ShowMyPC session data. This will prevent third parties from accessing any data in transit.

Facilities Security

ShowMyPC session services are provided through points of presence (POPs) in various geographic locations, including the US, Canada, Europe and Asian Data Centers. The facilities have on duty personnel, 24 hours a day and seven days a week.
To gain access to any facility, one must first be on the approved access list and then be authenticated by additional security controls.

Conclusion

ShowMyPC services have undergone exceptional increases in usage. This would not be possible without careful attention to the incorporation of security principles and standards in the design and operation of the ShowMyPC infrastructure and services. Data security will remain the highest priority at ShowMyPC, enabling ShowMyPC to continue achieving the goal of providing the most efficient and secure online real-time communication service.