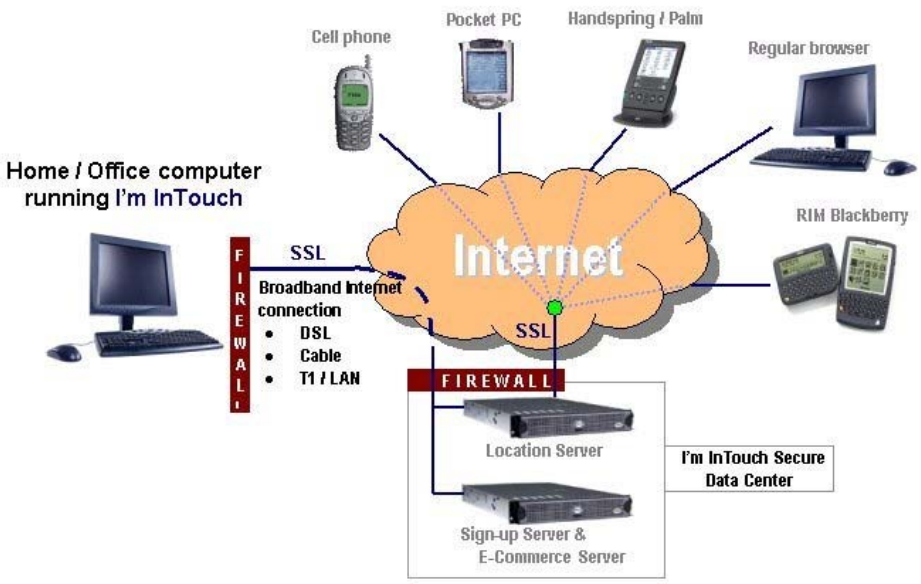
I'm InTouch Security Overview



I'm InTouch Desktop Edition Architecture

The I'm InTouch Desktop Edition provides users with a secure and cost effective method of connecting to their home or office computers to access the information and programs that they use in a typical day. They can run programs, transfer files, manage email, contacts and calendar events, and do most thing they do while sitting at their computer.

Remote access is accomplished by installing the software onto the PC the user wishes to be able to access remotely. The I'm InTouch patented technology (U.S. Patent Number 6,928,497 & 6,938,076) is managed by 01 Communique within a secure data center, and locates the user's computer connected to the Internet, regardless of whether its IP address is changing or static.

Encrypted Transport using Secure Sockets Layer (SSL)

The protection of confidential user data is critical and ensured by the utilization of the 128-bit SSL HTTPS protocol. All traffic between the browser Client, central I'm InTouch Server (housed in a secure data center) and Host computer, including screen images and file transfer, are protected with end-to-end 128 SSL encryption.

Authentication

The purpose of authentication is to ensure that the identity of the central Server, browser Client and Host computer are verified. I'm InTouch deploys a number of authentication processes to ensure that data exchange is between trusted sources.

During a remote session the central Server must first authenticate itself to the browser Client by supplying a digital certificate, issued by a trusted authority.

After knowing that the Server is a trusted source, browser Client authentication continues by the user inputting a user specified Computer Name (selected by the user during the installation of the Host computer software) that can contain up to 64 characters of both letters and numbers. Long and complex Computer Names naturally provide stronger protection. The Server checks to see that this is a valid Computer Name and that this computer is currently on and running the I'm InTouch software, thereby being "registered" or polling with the Server.

The Server then passes the login request to the Host computer. The Host computer prompts user authentication by requesting input of a Login name and Password that are stored only on the host computer and managed by the user. The Login Name can contain up to 254 characters and the Password up to 12 case-sensitive alphanumeric characters. This Login Name and Password is never seen on the central Server.

Ongoing authenticated browser Client and Host computer data exchange is encrypted and managed through the Server.

Security Features of the I'm InTouch Host Computer Program

To be remotely accessed, a Host computer must have the I'm InTouch software installed and running on it. Installation requires physical access to the PC, avoiding any inherent risks associated with attempted remote installs.

Authentication to the Host computer requires a user Login Name and Password that, for maximum security, are stored only at the Host, eliminating the possible risk of all system wide passwords being found at the I'm InTouch servers during a hacker attempt. A second password is required for access to the My Desktop feature, adding a further level of authentication control. Local management of the authentication passwords at the Host allows for regular and ongoing user password updates by end-users, a good security practice.

To help protect against dictionary attacks, I'm InTouch limits the number of times any user can attempt to login sequentially. By default, after three unsuccessful login attempts, access to the Host computer is disabled for five minutes.

To minimize the risk associated with users leaving a remote session initiated at a public PC without first logging out, inactivity time-outs are applied. After a few minutes of inactivity on the SSL session, the Host computer will automatically terminate the session.

I'm InTouch maintains workstation OS-level access controls already provided to the end-user. When a user logins in remotely, they only have access to their individual computer on the network and are subject to the access controls already in place for that computer.

They will be restricted to those domains, file drives, etc already assigned. I'm InTouch's design approach ensures that the introduction of a remote access solution does not allow users to suddenly have access to all the resources of the business or home network.

To provide assurance to the user that nobody can be silently accessing his or her PC, a notice is displayed on the host computer's screen whenever a browser Client establishes a remote connection with the Host computer. Further, at the time of each remote access login, the user can view within the I'm InTouch viewer, the time of their last login. Both of these tools are useful in assuring end-users that I'm InTouch is safe.

Conclusion

In conclusion, I'm InTouch is an affordable and secure remote access solution that easily integrates into a users existing network and security architecture. It provides protective processes and the necessary tools to ensure that resources are always safe. These include thorough authentication of all devices and users involved in a remote session. All of this is delivered within a secure system architecture that does not require change to existing network configurations and that assures that all data exchange is safe and encrypted.