October 7, 2013

FoIP (T.38) Traffic Security

Is real-time fax using SIP (T.38) trunks just as secure as using regular lines?

Using SIP trunks to fax is just as secure as using regular PSTN lines and can be made even more secure by use of encryption, which is not available with regular lines.

Fax is transmitted over regular lines using T.30, the original fax protocol designed for faxing over the public switched telephone network (PSTN). With SIP trunks, fax is transmitted using T.38, a protocol that implements T.30 for IP based networks. Both T.38 and T.30 can work in conjunction when a fax call involves both IP and PSTN paths.

With T.38, fax content is transmitted over IP in much the same way it is transmitted using T.30 over the PSTN. In both cases it is possible for a hacker with sufficient knowledge to inspect the image content by perpetrating 'man-in-the-middle' breach of the network and using specialized tools to reconstruct the image.

In effect the security threat to fax traffic is no different over IP than over PSTN, however, the option to encrypt is available for IP traffic but not telephone traffic, so fax can be made more secure over IP than over the PSTN.

Is there a security advantage inherent to real-time T.38 fax?

With real-time T-38 fax the image stream can be encrypted and is never stored. This eliminates the possibility of an intruder altering or compromising the privacy of the content.

Moreover, real-time call traffic is handled by telecom carriers who go to great lengths to secure their networks[1]. On the other hand, any entrepreneur with a fax server can be a service provider for non-real-time fax so potential customers must perform a great deal of due diligence to ensure that such a service provider has in place the necessary security measures and, because non-real-time traffic involves storage, complies with all applicable regulations.

Securing fax is not just about its security while in transit. A crucial aspect of securing fax has a lot to do with how well the document is secured at locations that store it.

Without encryption, how does T.38 fax security compare to that of the PSTN?

Without encryption, the security of real-time faxing over IP is comparable to that over standard PSTN lines. In both cases faxes can be intercepted by someone 'wiretapping'.

[1] babyTEL safeguards its IP network with techniques like network address translation, port redirection, IP masquerading and non-routable IP addressing schemes then secures the network perimeter with multiple firewalls and session border control devices that are monitored by intrusion detection systems.

In the PSTN world, hackers are deterred by the need for physical access to the telephone wire. In the IP world physical access to the network is required.

Within a company, employees pose an equal risk for both IP and PSTN faxing. A security breach is equally possible by an employee who has access to IP traffic inside the network as by an employee with access to the telephone wires. An employee with access to the fax machine can compromise hardcopy fax security regardless of whether it uses a SIP or PSTN trunk.

I heard that hackers can use Domain Name Spoofing to intercept my Internet traffic. Is this possible with T.38 FoIP over Internet?

Hackers can use domain name spoofing to subvert Domain Name Servers (DNS) so that a look up of an intended recipient gets the wrong address.

Avoiding this potential security breach means avoiding the use of DNS and using static addressing instead. This is part of the 'hardening' that needs to be done to ensure your FoIP system is secure.

Does encrypting my FoIP traffic make it safer?

Yes, encrypting the FoIP traffic makes it more difficult to access but it does not add significant difficulty to thwart a sophisticated enough attacker. Researchers have uncovered ways that criminals can spy on Internet users even when encryption is used.

The research has shown that determined hackers can sniff around the edges of encrypted Internet traffic to pick up clues about their target's systems and then use this information to subvert the systems that initiated the traffic, bypassing the secure encryption protocols altogether.

This does not take away from the power of encryption for securing the real-time traffic. It does however underscore the important task of securing the systems that initiate and receive the traffic.

Reference: http://www.physorg.com/news199681942.html

Is encryption necessary for meeting standards and compliance requirements?

Encryption may not be necessary with respect to regulations that consider telecom carriers as merely conduits that transport information but do not store it. Since no disclosure is intended, and the probability of exposure of any particular protected information to a conduit is very small, many regulations do not typically cover the conduit.

Note that there are different international, federal and state level data protection laws that have varying applicable security and privacy requirements. Whether you use encryption or

not, refer to the guidelines of each applicable regulation to fully understand your obligations.

Are the following entities considered "business associates" under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?

No, the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity, and the probability of exposure of any particular protected information to a conduit is very small, a conduit is not a business associate of the covered entity.
http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/245.html

babyTEL T.38 real-time FoIP is considered a conduit and thus meets the HIPAA Privacy requirements.

Is it safe to use T.38 FoIP for 'high sensitivity' documents?

The answer to this question depends on your corporate policy. Within any organization, faxing, like e-mail and other records management processes, is typically governed by information privacy protection policies and practices based on the sensitivity level of documents.

Essentially, if you are reviewing your existing policies regarding traditional faxing with the intent of extending them to cover FoIP then note that with respect to privacy and security, T.38 FoIP is as secure as traditional faxing and encrypted T.38 FoIP is more secure than traditional faxing.

How can I encrypt my T.38 traffic over the Internet?

babyTEL has incorporated within its architecture a mechanism that allows for real-time secure and encrypted communication between your device (IP PBX, Fax Server, etc.) and our network edge where state of the art Session Border Control (SBC) elements protect all IP call traffic within our network.

Another way to encrypt traffic is to use a virtual private network (VPN) connecting the network where your FoIP server resides and the FoIP service provider network. Your FoIP server would then communicate with the service provider over a secure VPN to carry the T.38 traffic. Tests with several customer environments reveal that VPN connections are not stable and result in excessive failed fax calls making then a poor encryption option for real-time fax traffic.

Standard-based approaches to encrypting voice traffic exist but, as of this writing, babyTEL's encryption mechanism is the only available solution[2] for encrypting real-time fax traffic.

For any further questions, please contact:

Daniel Dorsey
Vice President – Channel Partnerships
babyTEL Inc.
(514) 448-0415
ddorsey@babyTEL.net
www.babytel.net

[2] The standard protocol for securing SIP traffic requires that media is transported using a secure version of the Real-Time Transport protocol (RTP), however T.38 implementations today use UDPTL rather than RTP to transport the media.