T.38 fax transmission over Internet – Security FAQ

*Give me a rundown on the basics of T.38 Fax over IP security.*

Real-time faxing using T.38 SIP trunks is just as secure as sending faxes over standard telephone lines because faxes are transmitted in very similar ways over both mediums and both mediums are subject to the same security breach potential. If anything, real-time faxing over IP can be more secure because the option to encrypt is available for IP traffic but not telephone traffic.

In both the PSTN and IP world, fax images are transmitted by being disassembled and encoded into binary chunks that are sent over the network then decoded and reassembled on the other side to rebuild the images. On IP, these chunks are sent as data packets, while on the PSTN they are sent as analog signals. In both cases it is not possible for a hacker to inspect the image content without sufficient knowledge to be able to first perpetrate a ‘man-in-the-middle’ breach of the network and second use specialized tools like Wireshark or DataProbe to reconstruct the images.

It is also worth noting that the way faxes are transmitted, whether packets over IP or analog signals over PSTN, incorporates checks on the image stream sent between devices, so even if a malicious attacker is able to gain man-in-the-middle access there is no opportunity for them to alter the content in real-time without disrupting the fax transmission.

In effect the security threat to real-time fax traffic is no different over IP than over the PSTN. But securing the fax is not just about its security while in transit. In fact a crucial aspect of securing fax documents has a lot to do with how well the end points are secured.

To ensure its customer’s faxes are protected, babyTEL safeguards its network equipment 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.

*Is sending a real-time T.38 fax over the internet just as secure as sending it over a traditional analog telephone line?*

Yes it is. Real-time faxing over IP is just as secure as faxing over standard PSTN lines. In both cases faxes can only be intercepted by someone physically connecting to the wire (‘wire-tapping’). Given all the laws against this form of intrusion, wire-tapping is very rare.
In the PSTN world hackers are deterred by the need for physical access to the telephone wire or switching equipment and the laws that exist against wiretapping. This makes faxing over standard PSTN lines inherently secure.

In the IP world, there are many tools for ‘sniffing’ packets on the network wire, but just like in the PSTN world, physical access to the network wire or switching equipment is required to make use of these tools and once again, in most countries, strict laws are in place against unauthorized access to network traffic.

In the IP world, a security breach could conceivably occur by an employee internal to the company who has access to the IP traffic inside the network, but that is a security issue that applies equally to fax as to other IP applications and is not much different than similar breach potential that exists with employees having access to the telephone wires. So real-time faxing over IP presents no additional security issues of this sort.

**Can someone ‘wire-tap’ the Internet and see the contents of my fax?**

Just like the regular analog telephone line, the Internet connection to your enterprise has the same physical access security exposure. A person with physical access to the router or internet circuit could eavesdrop on the packets going in and out of the enterprise network. The main difference is that the FoIP packets are mixed in amongst all the other data packets (ie. E-mail, Image downloads, Internet surfing or FTP requests), making it that much more complex to find them.

The regular telephone line has no such capability and sends a fax or phone call down an exclusive wire, making it easier for someone to tap the wire and intercept the communication. So while the same opportunity for ‘wire tapping’ exists in both cases, eavesdropping on FoIP traffic requires a much more knowledgeable hacker.

Without physical access to the Internet connection to your enterprise, ‘wire-tapping’ your IP traffic becomes an even more complex task that only very sophisticated hackers can accomplish. In most countries there are strict laws against this type of activity and it is considered a criminal act.

**I have 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 a technique called domain name spoofing, which involves the very difficult task of corrupting or subverting Domain Name Servers (DNS) so that a sender who looks up the address 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 both systems at the two ends of a FoIP session are secured. In effect, while a FoIP communication session, like any other data session over the Internet, can be secured with VPN-like encryption and authentication this is not as necessary as the security provided inherently by the ‘hardening’ of well managed systems that initiate and accept FoIP sessions.

**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 more important task of securing the systems that initiate and receive the traffic. babyTEL uses carrier grade equipment to secure its infrastructure. This is the same network gear that the largest Internet backbone providers use to secure and exchange their data traffic.


**Is encryption necessary for meeting HIPAA standards and compliance?**

Encryption is also not necessary with respect to regulatory requirements such as HIPAA or Sarbanes–Oxley since these regulations consider telecom carriers as merely conduits that transport information but do not access it, other than on a random infrequent basis as necessary for the performance of the transportation service or as required by law. And since no disclosure is intended, and the probability of exposure of any particular protected information to a conduit is very small, a conduit is typically not covered under the regulation.

It is important to note however that there are many other international, federal and state-level data protection laws that may have security and privacy requirements that apply. (The guidance provided here should not be considered legal advice. Please see the HIPAA regulations found in the following link to HHS).

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 health 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 good as traditional faxing.

Simply put, T.38 FoIP is no different than traditional faxing when determining whether a document can be faxed at all.

I know T.38 FoIP is just as secure as traditional faxing but can I still secure my T.38 traffic over the Internet?

Yes. T.38 FoIP uses SIP to carry fax traffic between FoIP end-points. The SIP portion of the connection can be secured at the transport layer by encrypting data. SIP provides a secure URI scheme called SIPS. According to the standard (RFC 3261) a call to a SIPS URI is guaranteed to be encrypted from the originator to their SIP service provider. Typically this covers the IP traffic path from end-to-end however some SIP providers peer with other providers, for termination or origination purposes, and as a result the SIP call may traverse additional hops from one end to the other. Care must be taken in this case that the SIP provider respects the security requirement if peering with other providers as SIPS only guarantees encryption over the hops from the customer premise to the target domain which is typically that of the SIP provider.
Note also that SIPS is not widely supported and there is a chance your FoIP server is not capable of initiating or receiving secure calls. In this case, secure encryption can still be accomplished by adding a session border control (SBC) device at the customer premise. The customer’s FoIP server would then communicate through the local SBC, which in turn communicates with the service provider SBC over a secure session to carry the T.38 traffic.

Also note that T.38 FoIP end-points may connect to the PSTN to terminate/originate a fax to/from a traditional fax machine. In this case, the PSTN portion of the connection is not encrypted. It is basically a traditional fax call where the fax is modulated as an analog signal using the T.30 protocol.

For any further questions, please contact:

Daniel Dorsey  
babyTEL Inc.  
(514) 448-0415  
ddorsey@babyTEL.net  
www.babytel.net