Delivery latency & security of data in transit across email services in the cloud.

With the move to the cloud often both the sender and recipient have outsourced their email platform. We'll take a look at how our fictitious lawyer Michael goes about his day using the standard business cloud based email system and then we'll compare it to using an assured email platform. Before that a short recap on email.

The Common Business Email System

When email was invented everyone had their own on premise email server which periodically dialled out to a list of partner servers to deliver and pickup email. Systems like ccMail worked like this. The world was good, inter domain email wasn't expected to be fast.

Internet email changed that somewhat with email being sent and received as and when it was sent by the user. Everything was fine, we all got our email quite quickly until the spammers came along when we started seeing large amounts of junk mail in our inboxes, this was the start of the email queue and the associated delivery delays.

To counter the spammers (and later the phishing emails, and targeted trojan attacks) aggressive spam and virus filters were deployed but this quickly overwhelmed most system administrators, the task of managing these filters was too expensive. Along came the managed email security companies, they filter the email, life is good again.

Not long after the hosted email security companies became established the hosted mailbox market picked up significantly so suddenly the whole mail platform is out sourced, the server, the mailboxes, the spam filtering, the archiving and it goes on. We've outsourced the email platform but we're now sharing it with thousands of other organisations.

Unfortunately the achilles heel of massive shared email platforms is volume of traffic. These systems have to handle all the bad email that heads to their customers as well as the good. We return to the inevitable email queues, with good email getting caught up in bad, and a situation where email delivery times become elastic.

An Assured Email System

Early email systems like AOL and Compuserve were silos until SMTP (Simple Mail Transport Protocol) came along as a federated protocol. Before federation email platform owners had control of both the sender and recipient mailboxes so were able to maintain a mailbox to mailbox service level. Federated (internet) email changed that because the sender and recipient mailboxes could well be on different email platforms making it impossible to offer a mailbox to mailbox service level.

An assured email system returns to the email silo model so that we can offer deliver service levels around mailbox to mailbox latency and security but we do it using a standards based protocol, the same SMTP protocol that regular internet email uses. Using standards based email means we can connect to the internet so that our customers can send and receive email to and from other organisations but we do this in a strictly controlled way with terms of service that protect us from the bad things on the internet.

This is essentially a premium private email platform, designed and deployed with speed of delivery and security as the main drivers. Because the service is private we don't suffer the deluge of spam and denial of service attacks from malware. Because we're not hosting thousands of customers at rock bottom prices we're not overloading the systems running the service. Because we control the sender and recipient mailboxes we can maintain quality of service.

Michael's Story

As he heads out for an important meeting Michael calls Annie and asks her to email the [confidential] documents he needs as soon as she gets them. Here's what happens to that email after Annie sends the email via her hosted email platform, and how it then traverses Michael's hosted email platform to his inbox.

From:	Annie.Smith@threatforensics.com	To:	Michael.Jones-Smyth@rapidlegalhelp.co.uk
Subject:	Urgent documents for 1:30pm meeting [SEC=CONFIDENTIAL]	Priority:	High

Mapping the emails route through the internet

When Annie sends the documents she assumes that the email will get to Michael in time for his 1:30pm meeting and probably doesn't give security much thought, she's heard the IT Manager talking about security and knows about SSL on web sites. Email's secure, isn't it?

The following chart is a shortened and anonymised edit of an actual email route as it went from the originating hosted email provider to recipients hosting provider. The Delay column is exaggerated because we combined delays from a few hops, but the total Elapsed Time is accurate. The Protocol column shows the secure (green) and insecure (red) connections.

From here	Protocol		Next Hop	Time received	Delay
Annie's Mailbox	SMTPS	→	smtp.emailserver4.com	9 July 2015 13:16:14	
smtp.emailserver4.com	ESMTPS	→	mx1-eu1.ex42hosted.com	9 July 2015 13:17:31	1 min 17 sec
mx1-eu1.ex42hosted.com	ESMTP	→	out1-eu1.ex42hosted.com	9 July 2015 13:18:45	1 min 14 sec
out1-eu1.ex42hosted.com	ESMTP	→	mx56.gate.hostedofapps	9 July 2015 13:18:58	13 sec
mx56.hostedofapps	ESMTP	→	imap.mail.hostedofapps.net	9 July 2015 13:31:03	12 min 5 sec
imap.hostedofapps.net	IMAPS	→	Michael's Inbox	9 July 2015 13:31:23	20 sec
	(Secure)			Elapsed Time	15 min 09 sec

What does this mean?

Very simply that Michael was late for his important meeting because he had to wait for the email to arrive. He couldn't really walk in without the confidential documents he needed. It's not a big deal,

unless that delay was 30 minutes, or maybe an hour. We've all experienced long delays, or hope we won't have to. Even if we are using some type of document drop box or sharing platform often the link to the document, or the notification that it's posted is delivered by email.

The 'gotcha' here is that once the meeting starts the client asks if Michael's iPad is secure and if he's sure emailing the documents was secure. He'll say yes because he assumes email is secure. It's only the next day when his client calls to ask if he's seen the front page of the national papers that he starts to wonder who may have intercepted that email on route to him.

Interception and Meta data

Although improbable the risk of illegal(and legal) interception of email at an ISP or email hosting is real, and should be considered when sending sensitive information by email. The meta data (eg email headers) could also be valuable giving away addressing and routing information. By minimising the number of insecure hops an email has to tak to the recipient you minimise the risk of interception and meta data loss.

An Assured Email System

An assured email service give you certainty that an email, sent to a previously designated recipient on the same platform, is delivered over secure connections within a few seconds.

It takes the good things about the cloud and leave the bad things behind. Simply put it's a premium private email platform, designed and deployed with speed of delivery and security as the main drivers. Not bulk email processing on a massive scale that is open to the internet.

Because the service is private it doesn't suffer the deluge of spam and denial of service attacks from malware. Because it's not hosting thousands of customers at rock bottom prices it's not overloading when running the service. Because we/you control the sender and recipient mailboxes quality of service can be maintained.

Let's take another look at Michael.

Michael's Story - Two weeks later

As he heads out for an important meeting Michael calls Annie and asks her to email the [confidential] documents he needs as soon as she gets them. Here's what happens to that email after Annie sends it via the assured email platform, how it traverses the system to his inbox.

The following chart is an actual email route from an assured email platform we ran, it went from the sender to the recipients mailbox. As with the model above the Protocol column shows the secure (green) and insecure (red) connections. There are no red connections.

From here	Protocol		Next Hop	Time received	Delay
Annie's Mailbox	SMTPS	→	smtp.assured.email	9 July 2015 13:16:14	
smtp.assured.email.com	ESMTPS	→	imap.assured.email	9 July 2015 13:16:16	2 sec

imap.assured.email	IMAPS	→	Michael's Inbox	9 July 2015 13:16:18	2 sec
	(Secure)			Elapsed Time	4 sec

What does this new model mean?

It means Michael no longer worries about getting documents late, if he sends documents he knows they will be with the recipient in seconds and importantly he can look his client in the eye and say his firm is using a secure email platform. In fact his client will already know this, they're already using their complimentary assured mailboxes.

Is it that simple?

As with most things that seem simple there's a lot of knowledge and expertise that goes into making something work. We've been working with messaging platforms of many types since 1999. Designing, building and running near real time instant messaging platforms and running hosted email services for many years.

Cleartext's managing director has been R&D and Product Manager at Dr Solomon's Anti-Virus, Regional Manager for Symantec Security Response and Technical Director at MessageLabs (now Symantec Cloud), responsible for the APAC email platform and on the product strategy board.

He designed a secure instant messaging platform (http://www.cipherim.com) in 1999 with a fully automated PKIand latterly hosted email platforms for ISP's and was early to market with a combined hosted email and managed email service (called ClearEMail) as early as 2005. ClearEmail ran from 2006 to 2012 with close to 100% uptime before the platform was decommissioned.

Our implementation of an assured email service is a simple but elegant concept, is built on a robust cloud platform at Rackspace UK and runs the powerful, secure and reliable Axigen ISP grade email solution in a load balanced, front end proxy, back end server cluster. Simply put that means we can scale up quickly to ensure speed of service.

All connections are secured with at least SSL but preferably with the latest TLS 1.2 where possible. We don't support POP mailboxes as these don't give us the 'push' email we need and of course we have a really nice webmail platform (60 second mail delivery SLA). Full end to end public, private key management is outside this platforms scope but available via systems like OpenPGP. Assured email aims to solve the latency and in transit security issues.

So how do we set this up?

The service is very simple to setup, just adding a new mailbox to the email program of the sender and recipient. Both are on the assured email service. We setup your account on the service using a sub domain on your company domain, so if your company email address looks like;

Annie.Smith@threatforensics.com
Then Annie's assured email address will be;

Annie.Smith@assured.threatforensics.com

Your IT administrator does not need to add this sub domain to your companies DNS because this new email address is not designed for public internet routing. However you could publish this sub domain in DNS and we can enable outbound public internet routing, and inbound routing under special circumstances.

As an alternative you could use your organisations name combined with our domain, for example;

Annie.Smith@42legalstreet.assured.email
This format is not dissimilar to some web based services which use personalisation URLs like;

http://42legalstreet.servicename.com/
Setup is quick and simple, no need for any web logins or apps on your laptop or phone, just use your existing email software. Simply decide how many mailboxes you need for your organisation and how many partner recipient mailboxes you will need. We'll give you an administrator portal login to create the partner sub domains and mailboxes. Then simply pass the partner mailbox account details to the recipients.

Summary

Delivery latency & security of data in transit across email services in the cloud will continue to be a problem for all types and sizes of organisations. With an ever increasing focus on data security it's important that the most common, but often least understood IT platform, email, is looked at carefully with regard to your data security and privacy policies.

Assured email is NOT an alternative to a GCSx, Ministry of Justice CJSM (although it is similar to this service) or secure email services offering email encryption. Assured email's focus is speed of delivery and security of the connections, accepting ONLY the SSL/TLS versions of email protocols, and removing the risk (of data and meta data leakage) from unsecured mail hops at or between different service providers on the public internet.

Assured email services are designed for organisations who rely heavily on email to transfer important information in a timely manner and understand the risks of using public internet routing and relying on a single business email platform.