Ebusiness technologies: foundations and practice
Customer Security

v/o
Web services also promise much in terms of security including authentication and authorisation, integrity and non-repudiation. However, at present, it appears that developers prefer to rely on HTTPS and SSL and other network-based solutions and accept the limitation that such solutions only apply to point to point connections.

Man
Probably the principle technology that is used from a point to point perspective is SSL. Probably used in conjunction with some sort of authentication technology. It would be quite complicated to try and give a generalised answer as to how a transaction might traverse from one end of an application for structure to another, but from point to point, it would be looking at generally using an authentication technology to authenticate the end point. The type of authentication technology would be commensurate with the risk, obviously slightly more expensive, sophisticated authentication technologies would be used for higher risk transactions. Then you would need to provide some sort of privacy on the wire and from, also integrity to ensure that none of the data was altered en route. The second two points would be principally provided by transport layer security.

Man
From our perspective because some of the web services that we use there were mostly for internal purposes, even where it was enterprise level, the security was a mixture of re-using things like HTTPS but also where we have say a Windows network or active directory kind of system using the security built into those things, and also things like firewall deployments. In terms of actual security inside a protocol such as SOAP we've not explicitly used those.

v/o
Although OASIS standards provide a fine grain security model, it appears that most developers have yet to encounter solutions that require their deployment. There is also the question of how such securities convey to potential consumers. Longer term, it is expected that security will be migrated down to the Enterprise Service Bus.

Man
As well as SSL perhaps being used as the underlying protocol then for the brokerage type of system, you'd probably need specific authentication methods and whether that's going to be specific to each business, or each business can agree to provide a common implementation, it's a bit difficult to see at the moment. So that's a bit difficult to foresee how that might pan out.

Man
Looking beyond the point to point hubs that the transaction is taken from one end of the application to another, or from client right through to endpoint, the point of consumption, it's actually quite unusual at the current point in time to secure that at the message level. If you look at this in the context of a web application, you're probably talking about an SSL pipe with arbitrary data traversing that pipe. If you were to use some sort of message level transactual security, you would probably look to use a web service using either a bespoke data type with its own WSDL or possibly something like user name token, though it would be important to kind of qualify that as a relatively unusual set of circumstances. Uptake is quite modest for those types of requirements at the moment.

Man
Different systems of course will have different levels of security implementation and if that's not clear amongst all the different services that they are consuming, how you need to implement that from a consumer point of view, that could definitely make service consumption difficult or tricky at least.

Man
What we're trying to do increasingly however from an SOA perspective is to encapsulate those kinds of mediations within the layer of the infrastructure. So the enterprise service bus is trying to take responsibilities for those kinds of areas, at the mediation level, embedding within it the need to manage secure socket exchange over SSL or whatever it happens to be, or X25 or LU6.2 or whatever it happens to be. So the network and inter-operability to those network components is managed through the ASB and so it's very much a productised environment that if you subscribe as a web services, you know, consumer of services, you go through that mechanism, that's something that you don't have to concern yourself with as an application developer and that's the way it probably ought to be. OK? And so I think that that level of distinction, that's the way I would draw the discussion and taking it up a level of abstraction because if we've not done that piece right, then all that we've said before, you know, just falls down in terms of an ability to be managed secure exchange.

v/o
The publish and re-use strategy for web services is well established but it seems there maybe some practical issues.

Man
The potential for re-use when it comes to web services is quite good but it's also important to be able to define those services well. That's not always easy to do depending on the changing business environment that you might be in. But if that can be tackled then you've potentially got services which can cater for a wide variety of usage.
In a practical sense it might be difficult to provide a truly brokered service, one that offers reliability and also those who provide the services, that they're definitely consistent amongst each other.