Network World

Managing trust in our digital world

Juggling collaboration, contracts and reputation is key
The Jericho Forum Outlook By John Arnold , Network World , 06/09/2008

In this month's piece, John Arnold, chief security architect at Capgemini UK, discusses the Jericho Forum's concepts of online trust and collaboration-oriented architecture. The Forum is an organization dedicated to encouraging innovations in e-commerce security.

Would you trust someone you've never met?

Lack of trust is the most serious problem with the Internet today. Lack of trust encourages phishing and spam, and limits the Internet to low-value transactions. Trust cannot be developed using technical security concepts alone; it must come from examining how humans create trust. The Jericho Forum's collaboration-oriented architecture addresses what we see as serious shortcomings in traditional approaches to online trust. Let's take a closer look:

We'll start by establishing a common understanding of key terminology, derived from the non-electronic world:

- Trust is a precondition for choosing to rely upon a collaboration with another party.
- Collaboration is an interaction between parties for some mutual purpose. A collaboration is governed by a contract between the parties involved.
- A contract is a mutually understood set of obligations between parties backed up by an accountability mechanism to handle non-performance. A contract is a legal entity but it does not have to involve lawyers – there are unwritten and implied contracts, for example.
- Reputation is an opinion that one party has of another that a collaboration between them is likely to succeed. If I have a high reputation with you, it is because, based on my previous history, you believe some combination of the following:
    - That I am well disposed towards you.
    - That I have an incentive to collaborate with you properly and not to misbehave.
    - That I have the resources and skills to perform my part of the collaboration.

Reputation, contract and collaboration are relatedIf I have a high reputation then I will find it easier to contract with people. If I collaborate as expected by the contract, then my reputation will rise; and so on.

We all know that reputation is hard-earned, but easily lost. Just one failure to honor a deal can set you back almost to square one. Even a suspicion (not proven) of dishonorable dealing can ruin a reputation – as credit rating errors have amply demonstrated many times. The saying "Would you buy a used car from this man?" has entered our language as a good measure for deciding trust. Indeed, reputation is something that business traders truly value higher than all else.

OK – now that we agree on the basic concepts underlying what trust is about, let's ask the

question: How do they relate to modern security architectures in the e-Business world? The answer is not very well!

A directory (of the Microsoft Active Directory or LDAP type) contains information about people and organizations, so we can think of it as a reputation repository. But most directories include only identity information: name, e-mail and, if we are lucky, home address.

This gives us some basic accountability (if I know where you live, I can sue you), but it doesn't tell me anything about how our previous collaborations have gone. This type of information can be stored in human resources databases and audit logs and in proprietary reputation systems like eBay has. Unfortunately it's not in a standardized form and it's not available to the right systems.

How do electronic systems track contracts? Virtually every business IT system creates or manages contracts or their fulfillment state in some way, such as transactional systems, order systems, HR and workforce management systems. These systems are usually siloed, with no common way of encoding or accessing contract details. As a result it is very difficult for most organizations to track their partners' contract status, or even their own.

So, at this point we can agree that most IT systems exist to support collaboration in one way or another and they need to be secured so that their users are able to do their jobs and are not able to misbehave. We can also agree from our discussion that user permissions and provisioning should be driven ultimately by contracts. However, in most cases today permissions must be specified manually or hard-coded in a very low-level fashion.

The outcome of all of this is that most secure systems have a very poor relationship to the "reputation, contract, collaboration" trust framework described above. The result is that many trust processes are hard to standardize and automate; enterprises are not very flexible or agile; and there is a severe mismatch between what people need to do and what they are able to do (being given too many or not enough permissions).

Apart from creating a great deal of unnecessary cost, this situation limits the transactions that can be done online to a very small subset of what is possible. Frequent low-value transactions are OK, but high value or infrequent transactions are very difficult. Also, large players with a brand are favored unfairly over small to midsize enterprises. These are significant barriers to the growth of e-Business.

The Jericho Forum believes that this undesirable state of affairs arises because most IT systems were developed for a perimeterized world and have not kept up to date with modern de-perimeterization trends. Our response to de-perimeterization is collaboration-oriented architectures (COA). COA treats the three components of trust (reputation, contract and collaboration) as first class security concepts.

For solutions to work globally in e-Business transactions, they need to use commonly adopted standards. Below is my list of the top three areas where security-interesting standards are being developed:

- Reputations – this is a very new area, but OASIS is setting up an Online Reputation Management System (ORMS).
- Collaborations – eXtended Access Control Markup Language (XACML) is a security policy markup language that allows security decisions to be made based on the contents of

a database, such as a contract database.

- Contracts – again, standardized contract encoding is a new area and not one that most people would consider security related up to now. I am impressed by ebXML, which is based on the UN/Cefact Modelling Methodology (UMM), which is in turn based on the Resource Event Agent (REA) business ontology.