Position Paper

Collaboration Oriented Architectures

Introduction

Collaboration Oriented Architectures (COAs) are information architectures that comply with the COA framework, outlined below. They enable enterprises that use them to operate in a secure and reliable manner in an environment of increasing information threat, and where it is the growing norm to interact without boundaries, irrespective of the location of the data or the number of collaborating parties.

This paper sets out the principal components that are needed in a COA to meet these requirements. Subordinate papers are published or are in development to describe these components. While many organizations are trying to respond to the de-perimeterization issue, they often lack a framework and set of guiding principles to organize and implement specific solutions. The paper aims to fill this gap.

The paper focuses on the need to have business processes that operate across and between multiple organizations, probably (but not necessarily) using the Internet as the common transport mechanism. In this environment, users and end-systems must securely interact with, or use services from, disparate systems that are outside any single locus of control or security domain.

Implementing a COA entails adoption of the Jericho Forum Commandments (JFC) (specifically Commandments #4 to #8[1]) covering the areas of operating in a hostile environment, trust, and authentication.

Problem

The traditional electronic boundary between a corporate (or 'private') network and the Internet is breaking down in the trend which we have called de-perimeterization.

Traditional approaches to architecting security solutions are aimed at securing organizational borders, and then the network, reinforcing a 'perimeterized' perspective. This is contrary to the future business needs of most organizations:

[1] JFC#4 - Devices and applications must communicate using open, secure protocols
JFC#5 - All devices must be capable of maintaining their security policy on an un-trusted network
JFC#6 - All people, processes, technology must have declared and transparent levels of trust for any transaction to take place
JFC#7 - Mutual trust assurance level must be determinable
JFC#8 - Authentication must interoperate/exchange outside of your locus of control

- Business is demanding more connectivity outside the enterprise
- Commoditization of technology is driving towards any-to-any connectivity on every electronic device, with those devices having ever lower cost with more 'intelligent' functionality built in
- Business 'relationships' of every type, from subsidiaries to relationships with other business that are also competitors in other areas, all require connectivity
- Pervasive, fast, reliable, cheap Internet connectivity is becoming available everywhere

Responding to the trend of de-perimeterization with a COA allows the business aspirations to be met by positioning processes and security controls appropriate to risks and needs, away from the traditional firewalls or gateways that organizations have turned to in the past to 'solve' secure collaboration.

The COA framework defines the key components within which interoperable, secure solutions can be provided to meet the needs of the business. Thus, systems, networks and whole 'enterprise architectures' can be considered to be compliant with the COA framework if all the components defined in the framework are present.

A COA enables provision of IT systems that are secure in a global networked world, able to keep pace with the growing threats and the business need for faster and more flexible collaborative business arrangements. These range from outsourcing to joint ventures, from merger today to divestment tomorrow, all within a global working, global manufacturing and global procurement environment.

Why I should care

De-perimeterization describes a problem driven by business and commercial pressures. It does not, in itself, suggest any solutions. The latter part of this paper describes a framework that will allow appropriately architected business-driven solutions to be developed and delivered. De-perimeterization is happening now, will continue to happen, and will inevitably impact virtually all networked IT systems. Implementing a COA ensures that de-perimeterization does not magnify the risks to your organizations.

Recommended Solution/Response

The COA framework generalizes conventional architectures as follows. It provides:

- increased emphasis on the requirements listed under 'principles' below. These are traditionally only seen as external or 'boundary' interface concerns in enterprise architectures.
- a user repository (keyed on people identifiers) is generalized into a contract repository (keyed on relationship, or obligation identifiers). A contract repository records agreements, and the obligations and capabilities that ensue from them.
- an accounting log (keyed on system events) is generalized into a reputation repository (keyed on business events). A reputation repository records user actions and compares them to applicable contracts, and, depending on whether or not the actions are in accordance with the contract, upgrades or downgrades a reputation.

The architecture formed by combining SOA (Service Oriented Architecture) with available security protocols (SAML or other XML) is insufficient to support COA. The following elements are also valuable[2]:

[2] Note that we include mention of brokers and repositories. While these are not strictly within the intended scope of this paper, they are mentioned because of their importance in the complete picture.

- The Standard Security Management System ISO/IEC 27001.
- Business processes that manage the collaborations founded on practises found in COBIT.
- Service Management capabilities detailed in ITIL.
- The architecture capabilities defined in TOGAF.
- A powerful language for describing access policies and delegations. (XACML version 3.0 is a promising candidate.)
- Access managers that will enforce an externally-required or end-to-end policy. (Current access management systems are beginning to gain this capability.)
- Attribute brokers that will establish a requester's identity, credentials and attributes to an appropriate degree of confidence, based on information from multiple authoritative sources (e.g. attribute authorities).
- Performance managers that will record what a user or system does at the level of business events, judge whether the user or system has acted in accordance with a contract or other agreed obligation, and report on their compliance profile. Today, this is a rather neglected field. It includes audit log managers and reputation systems.
- Contract brokers that will negotiate and agree new collaborative understandings between collaborating individuals in ways which do not violate their 'owning' organization's and jurisdiction's existing policies and contracts. These new contracts must be expressed in an open-standard language which can be interpreted by performance managers and access managers – eBXML is a strong candidate. The contract brokers must be able, in turn to read the open-standard output language of the performance managers and attribute brokers.

Conclusion

Implementing a COA builds a high level business framework that uses the capabilities of SOA, in addition to other relevant standards and practises, to enable effective and secure collaboration. While SOA meets many of the functional and non-functional requirements of COA, other standards and practises such as TOGAF, COBIT and ITIL also need to be engaged. A fundamental shift in thinking is required to implement a COA, moving from the thinking of an hedgehog, an animal that rolls into a tight ball at any sign of threat, to that of a Strawberry Plant, which puts all its key genetic material securely on its outside, as well as sending out suckers to extend the plants domain. The paper also provides a pattern for how a previously developed information system can be re-architected to support effective and secure collaborations across corporate boundaries. Enterprises that want to operate in a network of business partners will do well to implement a COA, and encourage their partners to do likewise.

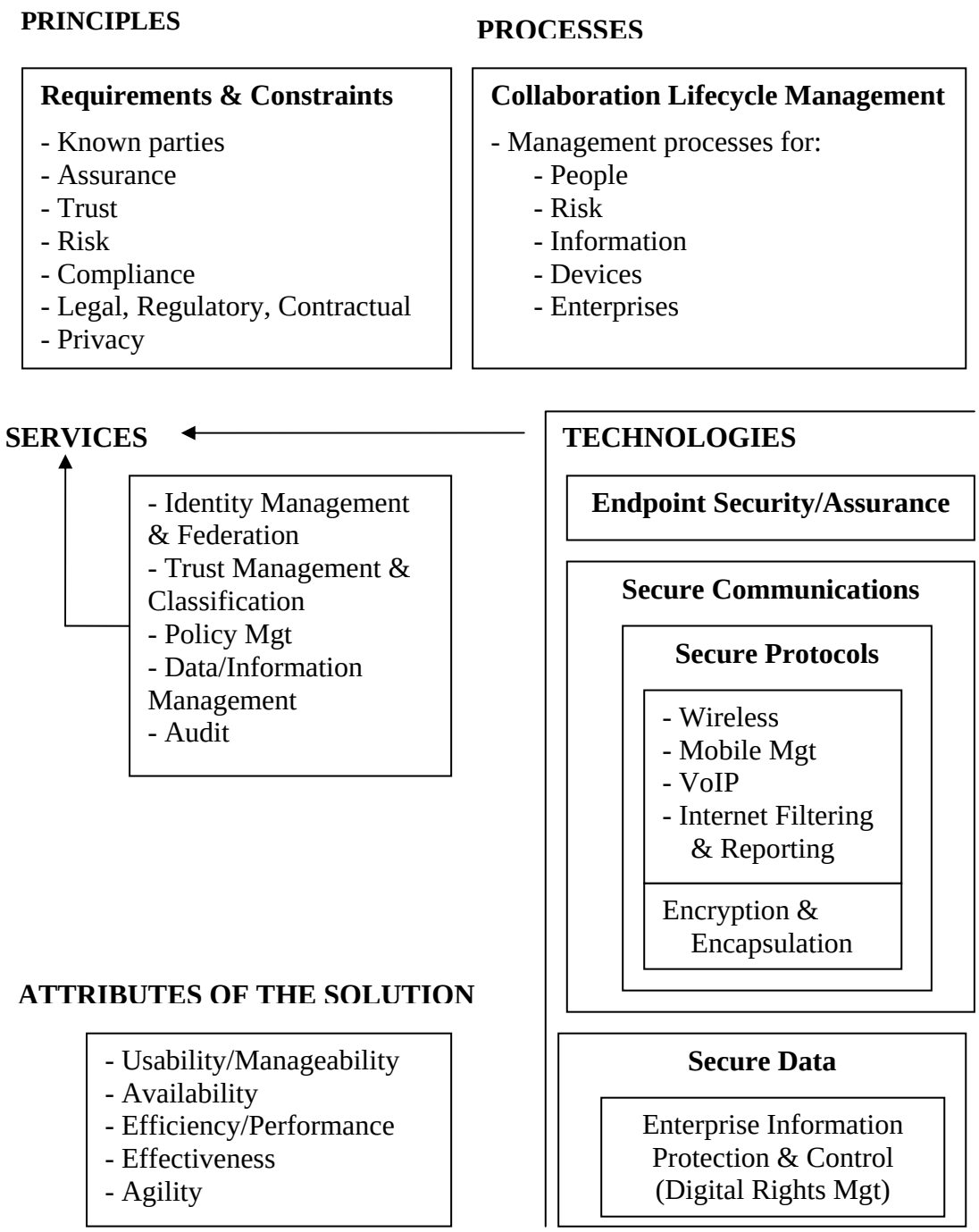
The way forward

Several elements of the COA have not yet been developed fully. In particular we need to elaborate upon the repositories introduced in this paper and their linkage to more powerful access managers, attribute brokers, and contract brokers than exist at present. We also need to encourage the development and definition of appropriate open-standard interfaces between these architectural elements. These dependencies will be addressed in supporting papers, currently identified as follows:

- Technologies
    - Endpoint security
    - Secure communications
    - Secure data (DRM)
- Processes
    - People Lifecycle Management
    - Risk Management
    - Information Lifecycle Management
    - Device Lifecycle Management
    - Enterprise Lifecycle Management
- Services
    - Identity management and federation
    - Policy Management
    - Information Classification
    - Information Asset Management
    - Audit
- Glossary

The COA Framework

Collaboration Oriented Architecture – Architects' View



Components of a Collaboration Oriented Architecture

The COA components are grouped into 4 main types:

1. Principles – Requirements (must haves) and Constraints (shall nots).

- *Participating Parties (know who – or what - you're transacting with):*
  All components of a transaction chain must be known to the contracting parties at all of its endpoints. These components are selected by collaborating parties, during contract negotiations. Collaborating parties are responsible corporate or individual entities, whose identities are well defined and whose activities are controlled by legal, economic, ethical, and technical means. A collaborating party may be a consortium, in which case the consortium must indemnify its members (and provide other economic, ethical, and technical controls) so that other collaborating parties may safely collaborate with consortium members. In the case where individuals are engaged, they will initiate interaction through an accredited Identity Service Provider.
- *Trust (agree the level of trust/confidence you will be transacting at)*
  The collaborating parties have the ability to agree/define appropriate (known) degrees of confidence in the components in a transaction chain, including the environment in which the components are operating.
- *Assurance (verify that the agreed level of confidence pertains)*
  Prior agreements between collaborating parties define their obligations to respect each other's intellectual property and to provide adequate technical security during a collaborative transaction.
- *Risk*
  The collaborating parties can make an assessment of any proposed transaction based on the communicated levels of trust with factors germane to the transaction: identity, confidentiality, integrity, availability, location, environment (space it is being used in), data-sensitivity, transaction value, time, etc.
- *Compliance*
  Collaborating parties agree to periodic inspections and security audits. The results of these inspections and audits are published within the collaborative group. Non-compliant parties may be sanctioned or expelled.
- *Legal/Regulatory/Contractual*
  The collaborating parties must comply with applicable legal, regulatory, and contractual requirements and be able to resolve conflicts that may arise between these. Compliance to local, legal and regulatory requirements alone is unlikely to be good enough to meet all business requirements. Contractual obligations, service level agreements, customer expectations, corporate policy, and norms of good corporate citizenship are requirements that need to be aligned and implemented.
- *Privacy*
  Privacy is a particularly important requirement that the collaborating parties must meet. Increasingly, privacy is being defined in legislative safeguards which are the consequence of widespread belief in privacy as a fundamental human right. At its root is an expectation by customers, suppliers, and employees that organizations will use information about an individual ethically so that it is not divulged if it is reasonably considered to be "private".

2. Processes

Enterprise processes are evolving as outlined in "Enterprise 2.0" by Professor Andrew McAfee of Harvard Business School, which defined Search, Links, Authorship, Tags, Extensions, and Signals (SLATES) as key transformational elements, that are changing the way organisations do business. A well-implemented COA will maximise the value of collaborations, using various SLATES elements, while managing information risks to an acceptable level. There are five key processes that need to be mastered by organizations that wish to achieve these transformations in a reliable and trustworthy manner.

- ***P**erson Lifecycle Management*
  Processes that manage an individual's joining, operational authentication and access management within, and departure from, a collaboration, including the management of individuals that are not employees or, more generally, members of the managing entity. Such processes take into account the identities, capabilities and potential impact of each of the individuals.
- ***R**isk Management*
  Processes, methods and approaches that identify, classify, and manage the information risks involved in collaborations.
- ***I**nformation Lifecycle Management*
  Processes that effectively and efficiently manage the creation, reading, update and deletion of information assets in a collaboration. These processes would include audit, monitoring and information protection activities.
- ***D**evice Lifecycle Management*
  Processes for introducing devices, identifying and maintaining device trust levels, and removing devices involved in collaborations. Removal of devices involves eradication of all information assets from the device.
- ***E**nterprise Lifecycle Management*
  Processes that ensure that collaborations are managed according to the risks they introduce and their lifecycle state. Initiating, operating, and closing down collaborations emanating from an enterprise would include a means of mapping relationships between all involved collaborating parties. Such processes would also have the ability to identify collaborating parties that are endangering the enterprise, and rapidly close down all relevant relationships.

3. Services

These services may be provided by one or more of the collaborating parties, or a 3rd party. Whichever one is used will have significant ramifications on how the services are provided.

- *Identity Management and Federation*
  The credentials of principals (organizations, individuals, systems, devices), and associated attributes required for identification, authentication and authorization decisions, are expressed in a standardised form. These credentials can be validated and accepted by the systems of any member of the collaboration or service providers.
- *Policy Management*
  The collaborating parties, and service providers, have the ability jointly or separately to evaluate, manage, and implement the policies and rules for authorizing and de-authorizing principals and collaborating parties.
- *Information Classification*
  The sensitivity of Information Assets is defined with causes of the information risk

(i.e. Confidentiality, Integrity, Availability) being defined against a commonly agreed classification model, aligned with risk-based assessment of business impact of an incident or threat. There are identity, legality and temporal components of information classification, all of these being context-sensitive.

- *Information Asset Management*
  Collaboratively-shared data is appropriately secured in storage, transit, and use, based on the agreed risk and performance requirements for the information contained in this data, as a result of the Classification. Principals accessing the data are identified, authenticated, and authorized. These requirements must be maintained through the complete document lifecycle, from creation through to destruction, by an appropriate records management taxonomy.

- *Audit*
  Transfers, storage, and retrievals of collaboratively shared data, and associated business controls, are auditable events. There is a common notion of 'event' across all collaborating parties and systems. Collaborating parties may require each other to conduct spot-audits on individual data objects and the actions associated with them, either overtly, or without alerting the individuals using these objects to the increased audit activity. The collaborative group may require summary audit reports on data transfers, storage, and retrievals to be published at some regular interval within the group. The audit information needs to be of adequate quality to meet the needs of the organization, including the rigor required for forensic evidence in law. A key driving principle in a COA related audit is transparency between partners.

4. Attributes

These enable you to measure whether you are achieving your objectives.

- *Usability/Manageability*
  Security measures are non-intrusive, and are easily understood by the individual end user.

- *Availability*
  A collaboration's information should not be rendered unavailable either by mistake or by an adversary. This implies that any 'at rest' encryption keys are escrowed, and that information is held in open-standard formats.

- *Efficiency/Performance*
  Security measures do not greatly affect the latency, bandwidth, or total cost of data retrieval, storage, or transmission. This implies that collaborating partners must possess the means to rapidly access decryption keys for all data in their possession for which they continue to have access privileges, allowing rapid data retrievals and offline malware scans.

- *Effectiveness*
  The COA framework provides an effective approach to organizing and controlling secure data transport and storage among a wide range of existing and future corporate information systems.

- *Agility*
  The COA framework takes into account the dimensions of timeliness and flexibility. It enables development of business-driven enterprise architectures that are appropriately flexible and adaptable to facilitate changes in business operations with optimal rapidity, and ease, with minimal disruption.