Who we are

The Open Group Jericho Forum®, a forum of The Open Group, is the leading international independent group of information security thought-leaders dedicated to advancing secure business in global, open-network environments. Members include top information security officers from multi-national Fortune 500s and entrepreneurial user enterprises, major security vendors, government, and academics. The Jericho Forum® provides a vendor-neutral place to meet, gain knowledge, and lead the development of approaches and standards for a secure, collaborative online business world.

What we do

Our members share their extensive knowledge and experience as CISOs and security practitioners, to enable secure business collaboration in an increasingly de-perimeterizing world. We do this by:

- Raising awareness of the security challenges we face as our corporate perimeters are increasingly being eroded by the effects of de-perimeterization
- Promoting the adoption of open collaborative architectures for secure business growth and flexibility
- Providing practical guidance to both customers and suppliers in identifying and responding to the challenges arising from de-perimeterization
- Demonstrating market demand for solutions to issues identified by the Jericho Forum®, and influencing IT vendors to respond effectively
- Showing how to analyze and test proposed solutions against our published security principles and guidance
- Supporting development of open standards that will underpin effective solutions

Why the Jericho Forum?

Through the 1990s, thought-leading CISOs shared their perceptions that increasing business demands for collaborations with their business partners, suppliers, and customers were undermining security defenses at their corporate perimeters. They saw this de-perimeterizing process was an inevitable trend which required a new approach to developing the security products, services, and solutions they needed. By 2004, they found no existing security group that was willing to take up this challenge. So they founded the Jericho Forum®.

Our approach

Enterprises today demand collaborative working with business partners, suppliers, customers, and out-workers, globally over the Internet. This significantly broadens the scope of what "information security" must cover. The future for effective security is to protect corporate business's greatest asset – its information – taking an information-centric approach by moving protection closer to the data, and ultimately by integrating the security with the data.

The Jericho Forum® commandments define the security principles for assuring effective security in de-perimeterized environments, and our Collaboration Oriented Architecture (COA) Framework supports architecting secure systems for de-perimeterized environments. Together they provide a design principles blueprint and practical framework showing how to create secure architectures for global business collaborations over the Internet.

The Jericho Forum® recognizes the huge potential of Cloud Computing – seemingly unlimited computing power, storage, applications resources, and services, all at almost immediate availability and low cost. There are a number of different Cloud types, however, and each poses different combinations of risks which enterprise business must understand how to manage. We have therefore extended our mission for "secure global business collaboration" to include securing the Cloud.

Industry liaisons

In October 2010, the Jericho Forum® transitioned from being a hosted forum to be a regular forum in The Open Group. It continues to have close working relationships with other forums in The Open Group, especially the Security Forum. It also enjoys mutually beneficial exchanges with other industry groups. Prominent among these is its collaboration agreement with the Cloud Security Alliance (CSA).

Become a member

If you would like to be part of our drive to influence our information security industry, steer our priorities and deliverables, and network with our members, become a member. Visit www.jerichoforum.org/join.htm.

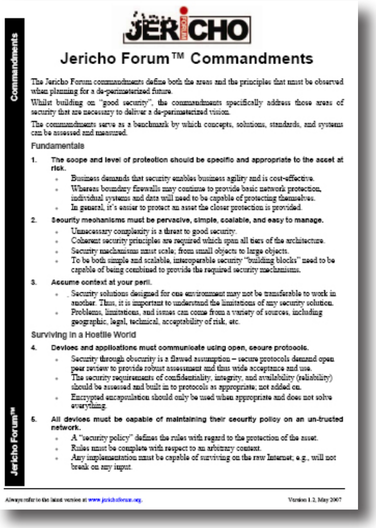
Current plans in 2011

- **Identity and Access Management** – the "digital identity" challenge; Identity Management, and Access Management, at the required levels of granularity.
- **Data-centric Security** – self-protecting data, where protection is bound to the data it is protecting**.**
- **Securing the Cloud** – continued collaboration with the Cloud Security Alliance on areas of joint interest, including development of CSA version 3 guidance.
- **Trust Management** – managing trust in business collaborations.
- **More liaisons with other industry groups** – mutually beneficial liaisons with ISO JTC1 SC27, ENISA, EURIM, ISSA, ISF, ISACA, etc.

Deliverables

- **Publications** – All freely available via links at www.jerichoforum.org/publications.htm:
  —De-Perimeterization Vision White Paper
  —Business Case for De-Perimeterization
  —Commandments – Design Principles
  —Collaboration Oriented Architecture – a set of 19 requirements papers grouped in 4 areas
  —Cloud Cube Model – selecting cloud types for secure collaboration
  —Contributions to CSA v2.1 Guidelines
  —Self-Assessment Scheme – for customers and suppliers to evaluate security solutions
- **Presentations** – delivered at numerous public events and all freely available as a re-usable resource at www.jerichoforum.org/presentations.htm.

Key accomplishments - the "noughties" decade of de-perimeterization



Commandments

Jericho Forum™ Commandments

The Jericho Forum commandments define both the areas and the principles that must be observed when planning for a de-perimeterized future.

Whilst building on "good security", the commandments specifically address those areas of security that are necessary to deliver a de-perimeterized vision.

The commandments serve as a benchmark by which concepts, solutions, standards, and systems can be assessed and measured.

Fundamentals

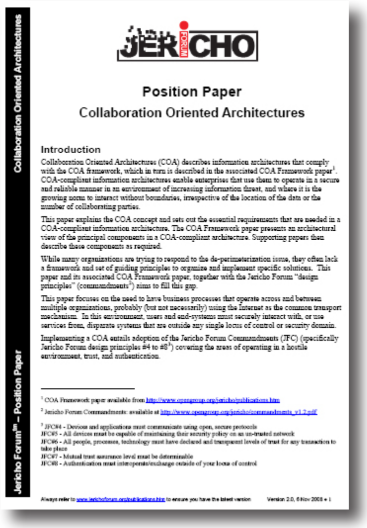
1. **The scope and level of protection should be specific and appropriate to the asset at risk.**
   - Business demands that security enables business agility and is cost-effective.
   - Whereas boundary firewalls may continue to provide basic network protection, individual systems and data will need to be capable of protecting themselves.
   - In general, it's easier to protect an asset the closer protection is provided.
2. **Security mechanisms must be pervasive, simple, scalable, and easy to manage.**
   - Unnecessary complexity is a threat to good security.
   - Coherent security principles are required which span all tiers of the architecture.
   - Security mechanisms must scale; from small objects to large objects.
   - To be both simple and scalable, interoperable security "building blocks" need to be capable of being combined to provide the required security mechanisms.
3. **Assume context at your peril.**
   - Security solutions designed for one environment may not be transferable to work in another. Thus, it is important to understand the limitations of any security solution.
   - Problems, limitations, and issues can come from a variety of sources, including geographic, legal, technical, acceptability of risk, etc.

Surviving in a Hostile World

4. **Devices and applications must communicate using open, secure protocols.**
   - Security through obscurity is a flawed assumption – secure protocols demand open peer review to provide robust assessment and thus wide acceptance and use.
   - The security requirements of confidentiality, integrity, and availability (reliability) should be assessed and built in to protocols as appropriate; not added on.
   - Encrypted encapsulation should only be used when appropriate and does not solve everything.
5. **All devices must be capable of maintaining their security policy on an un-trusted network.**
   - A "security policy" defines the rules with regard to the protection of the asset.
   - Rules must be complete with respect to an arbitrary context.
   - Any implementation must be capable of surviving on the raw Internet; e.g., will not break on any input.

Jericho Forum™

Always refer to the latest version at www.jerichoforum.org.   Version 1.2, May 2007



Collaboration Oriented Architectures

Position Paper

Collaboration Oriented Architectures

Introduction

Collaboration Oriented Architectures (COA) describes information architectures that comply with the COA framework, which in turn is described in the associated COA Framework paper[1]. COA-compliant information architectures 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 explains the COA concept and sets out the essential requirements that are needed in a COA-compliant information architecture. The COA Framework paper presents an architectural view of the principal components in a COA-compliant architecture. Supporting papers then describe these components as required.

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. This paper and its associated COA Framework paper, together with the Jericho Forum "design principles" (commandments[2]) aims to fill this gap.

This 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 Jericho Forum design principles #4 to #8[3]) covering the areas of operating in a hostile environment, trust, and authentication.

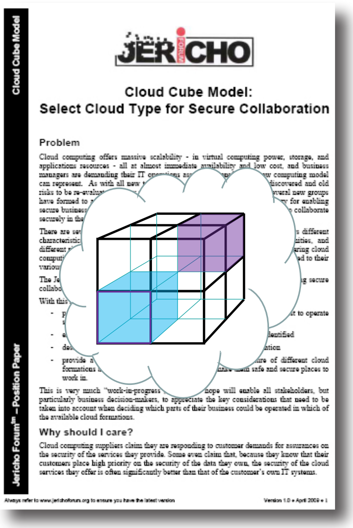
[1] COA Framework paper available from http://www.opengroup.org/jericho/publications.htm

[2] Jericho Forum Commandments: available at http://www.opengroup.org/jericho/commandments_v1.2.pdf

[3] 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

Jericho Forum™ – Position Paper

Always refer to www.jerichoforum.org/publications.htm to ensure you have the latest version   Version 2.0, 6 Nov 2008 • 1



Cloud Cube Model

Cloud Cube Model:
Select Cloud Type for Secure Collaboration

Problem

Cloud computing offers massive scalability - in virtual computing power, storage, and applications resources - all at almost immediate availability and low cost, and business managers are demanding their IT operations as
w computing model can represent. As with all new t
discovered and old risks to be re-evaluat
veral new groups have formed to a
y for enabling secure busines
o collaborate securely in the

There are sev
s different characteristic
ities, and different
ring cloud computi
ed to their variou

The Je
g secure collabo

With this

- p
t to operate
- e
identified
- de
ation
- provide a
ure of different cloud formations
make them safe and secure places to work in.

This is very much "work-in-progress
hope will enable all stakeholders, but particularly business decision-makers, to appreciate the key considerations that need to be taken into account when deciding which parts of their business could be operated in which of the available cloud formations.

Why should I care?

Cloud computing suppliers claim they are responding to customer demands for assurances on the security of the services they provide. Some even claim that, because they know that their customers place high priority on the security of the data they own, the security of the cloud services they offer is often significantly better than that of the customer's own IT systems.

Jericho Forum™ – Position Paper

Always refer to www.jerichoforum.org to ensure you have the latest version   Version 1.0 • April 2009 • 1

In computing terms, the "noughties" (2000-2009) was the decade of de-perimeterization:

2001	The "de-perimeterization" term coined.
2002	Addressing de-perimeterization becomes urgent.
2003	No existing security group accepts the challenge.
2004	Jericho Forum founded; host is The Open Group.
2005	Jericho Forum becomes a membership group.
2005	"Vision" white paper published.
2005	First conference hosted by InfoSecurity.
2006	Jericho Forum™ trademark granted.
2006	First requirements paper published.
2006	Jericho "commandments" published.
2008	Collaboration Oriented Architecture published.
2009	Jericho Forum® registered trademark granted.
2009	Cloud Cube Model paper published.
2009	De-perimeterization as an established concept.
2009	Commandments applicable to Cloud Computing.
2009	Self-Assessment Scheme published.