21st National Information Systems Security Conference 1998
Conference paper submission

Type of submission: paper
Title or Topic: Security and e-business: is there a prescription ?

Abstract

Over the past few years it has become increasingly common for organizations, government agencies and businesses, i.e., enterprises, to position some or all of their information assets in close proximity to the Internet.

Do enterprise architectures and designs apply to secure e-business computing? Issues of classification and management of data assets beyond the enterprise boundary, plus legal liabilities of electronically executed business transactions suggest that new approaches are needed.

This paper analyzes the conceptual similarities and differences of the design intra-, and extra-enterprise design environments in an effort to highlight some complexities of creating an e-business architecture.

This paper concludes that the network/security architect cannot effect comprehensive e-business security for all aspects of an enterprise. The strategy and the solution needs to be addressed in a more fundamental way than firewalls, SSL or PKI.

Author

Jim Whitmore
IBM Corporation
717-796-3264 (voice)
717-796-3414 (fax)

whitmore@us.ibm.com

Introduction

Over the past several years it has become increasingly common for organizations, government agencies and businesses, i.e., enterprises, to position some or all of their information assets in close proximity to the Internet and serve them to remote, often anonymous audiences.

Throughout those same years I have had the opportunity to work with individuals representing enterprises in each category, performing requirements analysis, design, planning and integration phases of Internet-related projects, including building: the "nth" firewall, web server, demilitarized zone, split-DNS, Socks servers, mail gateway, etc. Beginning in 1997 the questions and engagements were more often than not about leveraging the reach of the Internet to a greater extent for customer self-service and electronic commerce... and the mechanics of security in the environment now generically called e-business.

I have discussed requirements and plans with insurance companies that want to deliver or receive policy information to/from brokers and clients, government agencies that desire to interact with employers for taxes or unemployment notification and credit card issuers that needed to deliver account statements quicker than possible by standard mail

I am familiar with the issues: confidentiality, integrity, non-repudiation, etc., through education, experience and attendance at previous NISSC conferences. I agree with Guy King in his assessment that a paradigm shift is necessary (King,1997). I also concur with Ira Winkler with regard to the difference between technical security and information security. Still, most writings provide descriptive heuristics, and as an architect/engineer I am in search of a prescriptive methodology or model which might apply to the wide range of situations which I have encountered. Finding none, I decided to experience and consider some current customer self-service applications and commerce transactions, looking for "best practices", trends, etc.

In the role of information consumer I was surprised at what I found,... I did not sign up for the information service that asked for my birth city as a distinguishing characteristic in setting up a profile, I did not like the lack of care taken by a frequent flyer program used for initializing Internet access to accounts using only information found on ticket stubs which I routinely left with the emergency instruction card located in the seatback in front of me. I was pleasantly surprised that a medical reference website now only asks for my e-mail address at logon, and not the password that I forgot long ago. I think I'm pleased with the newspaper that sent a replacement password to an e-mail address (which I no longer use). I was disappointed at the fact that passwords on client certifications are optional in browsers. I was most distressed at losing my infrequently used client certificate as a consequence of erasing my disk drive prior to turning in my laptop for bigger/faster/better.

My conclusion, from a very nonscientific study, was that both design and implementation for some basic e-business transactions is inconsistent. I noted that most sites in my experiment used the basic security elements, but often I did not feel secure, or confident in their design, and sometimes I felt that my privacy was being abused. Some issues were due to the state of laptop computing and current GUI clients. There appeared to be some unique aspects of these seemingly

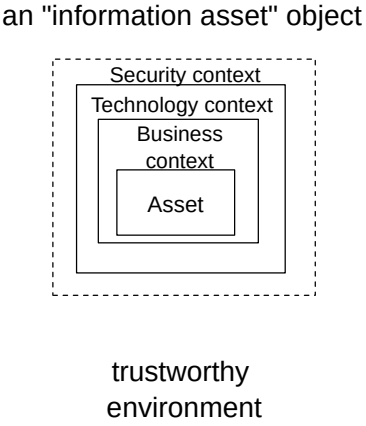
similar solutions. Why? What's the issue, what's the essence of the resolution? Is there a prescription for e-business design and e-business security?

A system representation using nested design constraints

Today's open computing architectures are structured by nesting objects which interact through standardized boundary later protocols and services (Bass, Clements, Kazman. pp 99-100). That concept can be extended to nested systems design as well (Rechtin, 1991. pp 31-32). In an effort to visualize the prioritization of design constraints for the initial phase of a typical enterprise computing design process I have constructed the nested system model shown in Diagram #1. My approach is to consider the information asset as the core object or constraint. The system construct can be described as the nested contexts which apply to some coded representation, or data object, that has a meaning and value inside of, and outside of, a computing relationship. I have chosen these contexts to be: technology, business and security, which are applied uniquely in a given design, in order of preference/necessity, i.e., any design has the same basic considerations, however, the constraints may be ordered differently, based on business practice, ethical criteria, or as prescribed by law.

Diagram #1

Nested constraints for enterprise computing design



The "dotted" perimeter for the security context represents the fact that often the implementation of security within enterprise computing is largely contained within employment guidelines, information use policies and facilities access security rather than robust I/T-based implementation. Note the "trustworthy environment" label.

This simple illustration has survived for several months, offering some practical value as well. Once established during initial brainstorming discussions it can justifies deferral of less significant issues and debate, like technology selection. Technology can sometimes be reduced to a "preference" rather than a design constraint, since most technology features are available on a

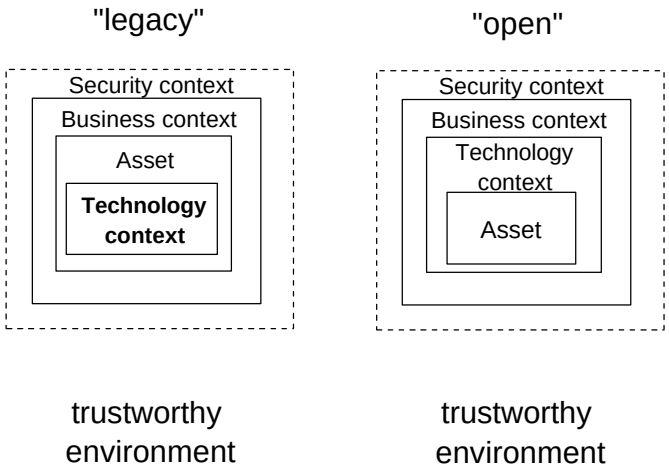
wide range of platforms from PC to mainframe. The primary technology issues are reliability and scalability.

Because information objects are created, stored, moved among systems and through networks, Diagram #1 could correspond a snapshot of an information asset at a specific position in the computing system. The characteristics of the asset, and its related contexts might change based on a number of factors.

Diagram #2 provides two examples: (1) “legacy” designs where technology is adjacent to, and most times inextricably linked with, the information asset, and (2) “open” designs where some aspects of technology selection are reduced to “preference” rather than “mandate” because of ubiquity, or standardization, of protocol, service, etc.

Diagram #2

Prevailing designs for enterprise computing



An example of “legacy” design would be a set of information assets built upon mainframe-based 3270 terminal service. An example of “open architecture” is an object oriented repository which services standards based clients.

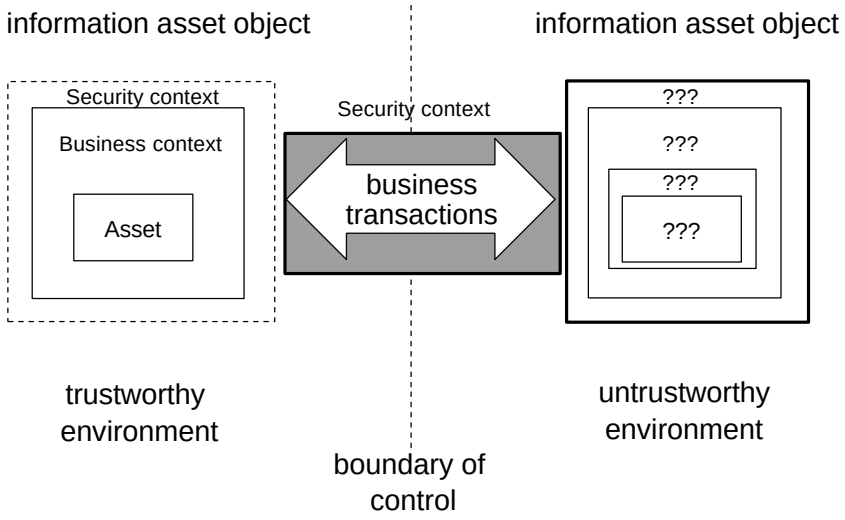
To bound the concept, an “ideal” environment assumes that there are no specific technology dependencies, and the “practical” environment recognizes that there will most likely be a set of alternatives with regard to vendor, a software product, proprietary GUI, or standardized protocol which excludes other members in the set.

Crossing the enterprise boundary

A substantial portion of recent NISSC conferences have focused on the boundary control function provided by firewalls, the transport privacy function provided by SSL and the PKI infrastructure necessary to support the creation of encrypted pipes (or secure channels) through the network and its security components. This focus area is represented by the shaded area labeled **Security context** in Diagram #3.

Diagram #3

Crossing the boundary of control



How will the information asset be interpreted/used/protected once it passes beyond the enterprise boundary ? To what extent is the role of the network/security architect complete once the asset is served through the firewall, across the VPN, and delivered to the computing entity "who is who they say they are" ? Some insight into the answer can be found by considering the design constraints of an information asset which has been served across the enterprise boundary.

Design constraints for information assets which have crossed the enterprise boundary

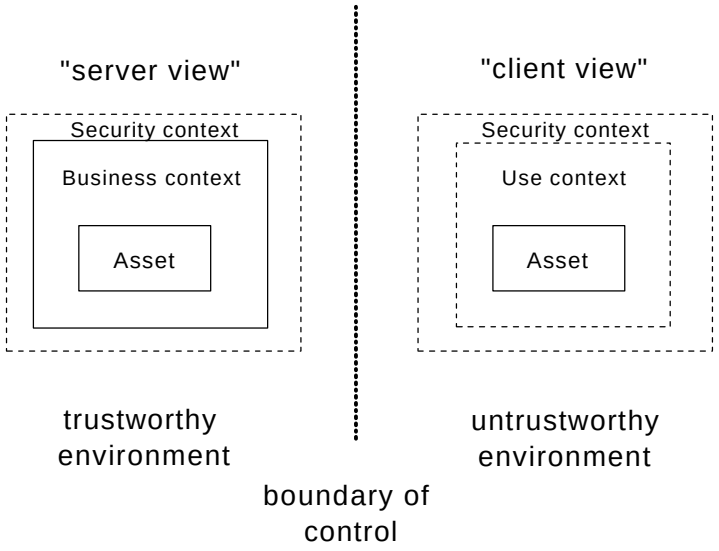
Now that web serving has reached some level of maturity, organizations are beginning to consider the Internet as a delivery mechanism for transactions of higher value, in the sense that valuable information assets are being imported and exported through the enterprise boundary, and that business interactions which currently exist entirely within the enterprise (under appropriate policies and practices) are being adapted for electronic delivery.

As with enterprise computing, we can hypothesize as to the construct of an information asset once it is beyond the enterprise boundary. To follow the taxonomy of contexts, the technology context will be derived from the union of available technologies, viable technologies and technologies supportable by both the server and the client; the business context represents the interpretation and use of the data asset as established by the owner of the asset vs. the

interpretation and use of the data asset as actualized by the user; and the security context can be described for both the server and the user as either in a defensive posture, i.e., steps necessary to avoid loss or liability due to technological negligence, in a proactive posture, i.e., maintaining ethical ownership, or trusteeship, or as a combination of both.

Diagram #4

Nested constraints for remote client in e-business computing



There are two main design constraint sets which need to be applied in order to normalize the differences between the server and user business contexts: constraints resulting automating a business process, and constraints resulting from distribution of data assets.

Design constraints in automating a high value business process

Using any of a number of network security architectures and mechanisms (SSL, VPN, etc.) , it is a straight forward exercise to develop a secure transport channel between server and client. However, given that the enterprise environment is (worst case) untrustworthy, and the user environment is (best case) untrustworthy, Can an architect assign a measure of effectiveness to *"sufficiently normalizes the business/use context" and "sufficiently protects the integrity of information assets"* ? and if so, how? Is there a potential for "architectural malpractice"?

Solutions must seek to enforce the business context of the information asset, such as: the interpretation and classification of the asset, a measure of value, a measure of liability, time to live, etc. from the perspective of the information provider, trustee and user. These characteristics have been represented in Diagram #5 by the box labeled **Use Policy**.

In today's world "use policy" are most often implemented with legal contracts, agreements and use policies. As the value of transactions flowing across open networks increases, we need

mechanisms to integrate policy within technology to enforce business contexts, similar to our use of technology to enforce confidentiality, integrity and availability (BS 7799) for channel security.

Diagram #5

Building trusted processes in e-business computing

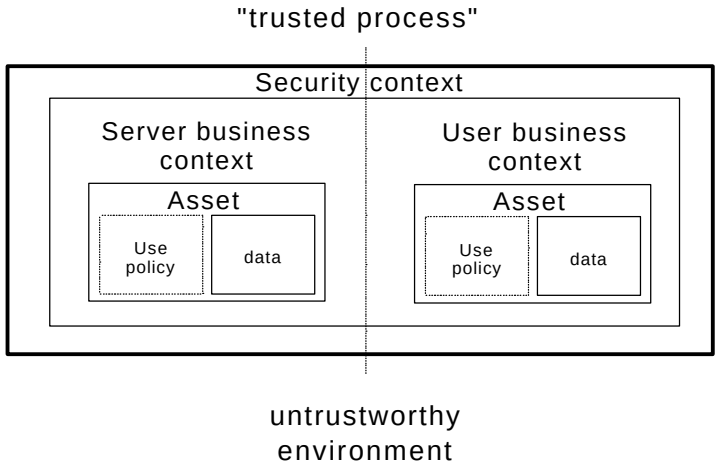
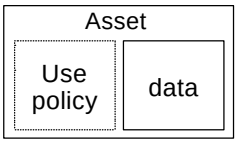


Diagram #6 provides an example of differing “use policy” based upon data classification, and a partial list of candidate technologies.

Diagram #6

Options for enforcing the intended business context in e-business computing



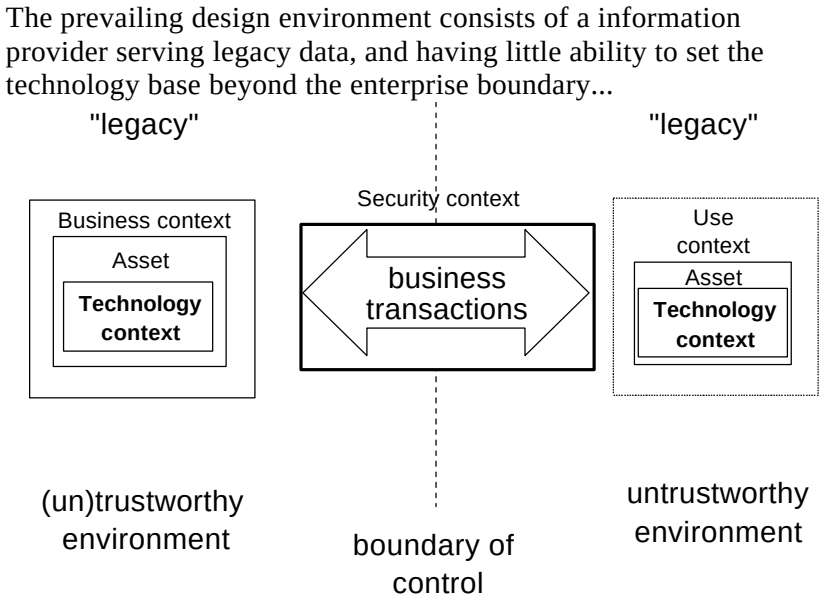
Classification	Action	Technology / policy
unclassified	✓no encryption ✓no audit	✓html ✓other
sensitive, with low value	✓channel security ✓authenticate on access ✓encrypt when transferred ✓log the event	✓SSL V2 w/ UID & PWD ✓PKI & SSL V3, S/MIME? ✓PKI & SET? ✓VPN? ✓PGP?
secret / private, with high value	✓process security ✓authenticate on access ✓encrypt when transferred ✓encrypt when stored ✓authenticate on open ✓audit on use/transfer ✓timestamp ✓relay to backend process	✓agreement or contract ✓trusted server process ✓trusted client process ✓trusted viewer ✓appropriate channel security ✓other?

Trusted processes are more than processes running within a trusted computing base. Trusted processes could include any/all prudent measures necessary to implement a legally defensible automated business process, or to re-engineer an existing policy based process for electronic delivery.

Design constraints resulting from prevailing technology at remote clients

With the enormous momentum behind major e-business initiatives, whether electronic government, electronic commerce, or customer self-service, the single largest risk to information providers results from under-engineering of asset delivery beyond the boundary of control, as a consequence of not factoring important characteristics of the information asset, from the perspective of both the information provider, trustee, and the information consumer. See Diagram #7.

Diagram #7



This situation occurs for several reasons:

1. the information provider has no control over the technology base of the target user community or market segment
2. the architect/designer has applied the technology context prior to, or without factoring the business context
3. external forces

The result is a solution which has the appearances of being robust, incorporating firewalls, SSL, and digital certificates, while having diminished effectiveness because of little, or no, security or audit after assets are transferred to the remote platform.

Conclusions

It appears that many of the existing e-business solutions are technology centric, rather than information centric. While technology-centric design works within enterprise computing when there is control over the technology base, it may not be practical or prudent for e-business solutions.

Information assets need to be served and managed in a manner consistent with the business intent, ethics, liability and assumed role of information trustee. Any I/T solution which transfer assets across the enterprise boundary should be reviewed during the design phase with the asset trustee or DBA, analyzing the flow of the transaction and any transfer of control as it relates to both the server, the intended consumer and the unintended recipient. Additionally, businesses processes which are re-engineered for electronic delivery should potentially be evaluated with regard to prevailing legal criteria for "all reasonable measures".

At a roundtable during the 1997 NISSC Conference, Steven Bellovin expressed the concern that in spite of continuous advancement in the area of network level security, virus detection, authentication mechanisms, etc., we have only succeeded in securing the connections between insecure computers. This paper echoes Mr. Bellovin's observation in different terms, by suggesting that asset protection is the ultimate goal of information security, and by encouraging network/security architects and designers look beyond the network security tool kit and engage all stakeholders in the solution development process.

So, is there a prescription for security in e-business ? My conclusion is that, at this time, the prescription includes individualized analysis and solution design, with a view toward end-to-end trusted processes. Secure technologies can create insecure solutions.

Jim Whitmore. July 2, 1998

References

Bass, Clements, Kazman. Software Architecture in Practice. Addison Wesley, 1998.

Code of Practice for Information Security Management, British Standard 7799: 1995.

Rechtin, Eberhardt. Systems Architecting, Creating & Building Complex Systems. Prentice Hall, 1991.

Winkler, Ira S., Information Security is Information Security, 20th NISSC Conference, paper.

IBM Systems Journal, Vol 35 No.2 1996, Object Technology.

King, Guy. Secrets, Lies and IT Security, 20th NISSC Conference, paper.

Hance, Olivier. Business and Law on the Internet, McGraw Hill, 1996.