“SAFE AT INTERNET SPEED:
Fast Track to Internet Security”

Softwaremag.com, August-September, 2001

By Patrick McBride, METASeS, EVP

The e-business revolution may be rapidly changing how many people live and work, but CIOs and other executives concerned with Internet security issues might do well to take lessons from old-line economy players: home builders. At first glance, nothing might seem more unrelated to Internet security than brick-and-mortar contractors, especially since they take months if not years to complete a single product, an equivalent to infinity on the Web. But consider the method for selling many homes today: Potential buyers often view model homes, customize a few components and move into their development tract in short order. Time is saved, because homebuilders to some degree already have ideas about what clients need or want.

Similar kinds of "prefab" solutions are possible -- perhaps preferable -- when it comes to security architecture and design on the Internet. In other words, what model homes can do for homebuyers and contractors, "fast-path templates" can do for those of us concerned with Internet security.

Best-practice baseline templates considerably speed up the security development because there are certain givens, when it comes to security. The templates themselves are based on the premise that relatively few types of Web-based systems exist and that similar business systems -- business-to-business and business-to-consumer models, for example -- have similar information-protection requirements.

The templates (which we'll discuss in detail later) have been designed with speed in mind -- that most precious commodity of the Internet world. Using this fast-track method to security architecture can cut development time in half, shaving off weeks or even months without sacrificing efficiency or information-protection capabilities.

Everyone knows that when it comes to the Internet, speed matters. What few realize is that traditional architecture and design processes have drawn-out cycle times that typically are too slow-paced for today's e-business models, particularly since the ability to get to market more quickly with a business system than a competitor can give a company a decided advantage. With this in mind, fast-track methods allow security teams to cross the first big architecture hurdle by predetermining which model their business unit needs and choosing the template -- or templates -- to match it. The initial legwork has already been done.

The fast track is good for another reason, too. For most companies, a major source of vulnerability is the lack of security expertise. One industry report, META Group’s "Enterprise Security in Practice," estimates that as much as 93 percent of organizations still have unmet security needs. In some cases, security specialists are unavailable; in others, security technicians are part-timers.

One source of critical vulnerability is the general lack of awareness of standard security practices. Some crackers[1] pose as network administrators or even legitimate technicians who telephone unsuspecting workers to request passwords, user IDs, or other information they can use to compromise a system -- all as part of a "system test" of security.

Breaches of security are increasing. Computer viruses, destructive "worms" that replicate themselves, Trojan horses, Denial of Service (DOS) attacks such as buffer overflows that overwhelm an organization's ability to process data -- all are multiplying and growing in complexity as breakneck technological change continues.

The consequences of such breaches can be astounding, particularly since the Internet has begun to function as the world's next economic engine. Online retail sales, valued at about $3 billion in 1997, are now projected to exceed $40 billion in 2002. Online trading is projected at $500 billion this year, up from $11 billion four years ago, according to *Management Review*, and total spending on e-Commerce will climb to $1.3 trillion in three years, according to International Data Corporation.

With so much money flowing across the Internet, the need for security measures is significant and will inevitably grow. In fact, over the next few years, information security is expected to be one of the seven areas of greatest employment need in the future, right up there with Internet development itself.

Cyber vandals can make a site inoperable, and if the site is a company's "store front," the intrusion can cripple a business. And if customers migrate to online competition, the intrusion can result in future revenue losses and inevitably damage a brand name or discredit a reputation.

The U.S. government is by no means immune to crackers. One cracker, alias John Smith, successfully penetrated the White House Web site, where he then posted text with foul language. When interviewed by a reporter, Smith said he attacked the site simply "because it was easily exploitable … and was pretty high profile."

Organizations worldwide face daunting Internet security problems. But many are seeking inadequate solutions in the technology marketplace. While technology does play a vital role in any effective Internet security program, it is still only part of the solution. Throwing technology alone at a security problem won't solve it. And while an effective solution might call for firewalls and other perimeter security measures, vulnerability reduction, threat monitoring and more technical wizardry, an even more important component is an overall security plan.

One of the most important aspects of security architecture is the ability to trace architecture back to an organization's business goals. This is not unlike building a house, where a good architect or designer first spends time trying to understand the customer's needs as they fit into a few broad categories. The architect would consider space requirements based on the family's size, or life-style requirements based on preferences, before making specific design choices, like the size or location of room.

[1] The term "cracker" refers to someone who illicitly and electronically tries to break into a system. Technically, a "hacker" can refer to someone who is authorized to break into a system, often to test the system's vulnerabilities.

Security architecture functions in a similar way. Basic security goals provide direction for the security architecture. Some main security goals involve protecting the confidentiality of data, making certain that unauthorized persons or systems cannot inadvertently or intentionally alter data without being detected, ensuring that the information accessed is genuine, making the data accessible and usable, logging transactions and data exchanges, and verifying the identity of a person engaged in a business transaction.

These fundamental goals – called CIA (Confidentiality, Integrity, Availability) in security circles -- determine the foundation upon which security architecture is built. Understanding these goals can help an organization create a sound framework for protecting its information assets -- for building its security architecture.

But to build a solid security architecture, one should first understand precisely what is meant by the term -- to ensure that he or she is speaking the same language as IT security specialists.

Security architecture means different things to different people. Typically, at its highest level, security architecture functions as a set of goals that incorporate an organization's strategic vision. This vision serves as a roadmap, informing the security engineering process -- it includes detailed designs, product selection, construction, implementation, support and management of an information system and technology infrastructure. This enterprisewide architecture guides all of an organization's development activities, as well as information systems and infrastructure development activities, such as networks , servers, and middleware.

System-level architecture, on the other hand, typically refers to a subnetwork, or a specific business system, dealing more than likely with specific applications. Essentially, system-level architecture consists of the nuts and bolts -- such as controls that regulate access, application authorization, and encryption -- as well as nontechnical controls such as audit reviews, education, and incident recovery.

In our definition architecture is expressed as a set of business goals or requirements, while design basically is the logical and physical configurations for technical components needed to achieve those goals. In addition, design takes into account specific nontechnical security tasks or procedures. Information security architecture, for instance, may include the goal of restricting perimeter network access, but would not necessarily mandate a specific firewall, which might fall under design's purview. The various business models make use of the Web differently, each with its own security requirements and risk tolerances. Thus, approaches to security should be based on an overall strategy that ties these components together. Yet most people confuse system-level architecture (the nuts and bolts) for enterprisewide architecture (the goals). While the differences between architecture and design are not important, what is vital is that an organization express architecture in terms of specific goals or requirements, providing key linkages to business objectives.

Traditional Method

The traditional method of formulating system-level architecture is a lengthy process that at best builds upon certain knowledge gained from recently completed projects. Still, since a number of new variables must be considered, it is best to start fresh.

This "born yesterday" approach includes multiple levels of inputs and outputs. The first lines of consideration, or inputs, stem from business decisions. These should include fundamental security goals developed in discussions with senior business management.

Before attempting to define technical and nontechnical architecture requirements, it is especially important to know exactly what information must be protected (assets), what this information must be protected from (threats) and what the consequences would be if protective measures proved inadequate. These are all top-level inputs in the design process. Because the business team is dealing with many unknown variables, much of the input information will be sketchy, and more than likely multiple sessions will be necessary.

As for threats, the team should attempt to profile would-be attackers and the misuses or abuses they are likely to purposely or accidentally perpetrate. Also discussed at this stage are possible malicious activities that would negatively impact the business and the potential impact if an activity resulted in a security breach. Asset value should cover the nature and value of data or information to be protected by the design and other nontechnical controls.

Other top-level considerations focus on legal and regulatory requirements, such as meeting Security and Exchange Commission or health care regulatory agencies mandates. Current or future business goals should also be addressed. By considering future business requirements during the design process, the security team will not lock itself into a design that meets only current needs.

Second-order considerations in the design process include business and IT operational concerns that impact the security architecture. Here, middle-level managers would focus on how new customers will be set up, and by whom; how system users will receive updates; how disparate systems will be maintained; and whether the organization's security philosophy should be managed by central security administration or via a decentralized approach.

System use considerations deal with such questions as who and what will use the system, and when, where, and why will the system be used. For example, the end users must be determined -- will they be novice or expert users, employees or non-employees, etc.? Also how and from where will users access the system -- from home, office, via the company network, or across national borders?

In addition, the current technical environment should be analyzed for what may impact the IT infrastructure and either help or impede security. And the current and future direction of the organization, relative to security, should be discussed. Will the organization have the goal of separating the user authentication process from the applications, enabling easier administration of user rights and privileges? If so, how should this be accomplished for the system-level architecture?

System-level security architecture flows out of such second-order discussions. Ultimately, security architecture is aimed at addressing these risks and eliminating as many of the security vulnerabilities as possible, but final considerations should not be overlooked -- for example, how to recover from or mitigate the impact of inadvertent or malicious activity. Another good practice is to develop a recovery or failover capability for Denial of Service attacks and to incorporate public relations

experts in the response in order to put media spin on potential public embarrassment.

Effective security architecture requires sound design, construction, testing, implementation, maintenance, and training. But since a new system more than likely will be tied to existing infrastructure, the architecture team should consider whether the current infrastructure provides adequate baseline controls for the new system. Many organizations lack appropriate technical security standards and configuration procedures to serve as the basis for a secure infrastructure. Like a house built on sand, an application hosted on a vulnerable infrastructure is at risk.

Fast Path

The other, much faster way to develop security architecture is the fast path method with "prefab solutions" that can cut development time by as much as 50 percent. This method includes the same inputs and outputs as the traditional method -- such considerations do not change -- except, information protection requirements are here enumerated and captured on predefined sets of best-practice system level security architecture templates, as mentioned earlier.

As such, when a business unit decides what type of business model it will use -- such as business to business or business to consumer -- it can then select the best practice template established for this model. The template already has security solutions built into its design. To use the homebuilding analogy once again, the organization's security choices are decided in a process similar to the use of model homes. Homebuyers can pick a style, customize components, and move in when construction is done.

As the number of Web and e-Commerce applications continues to grow, certain network architectures have become common. Templates are tailored to support e-business and major Web applications across these common architectures. The baseline templates can be designed for popular types of web-applications including:

Public Web Presence -- Traditional organization Web sites designed principally to disseminate information. Typically, these sites include an organization's home page, news releases, product or service descriptions, employment opportunities and contact information.

Company Intranet Web Site -- A company's internal Web site. It supports information sharing among and across various business functions, such as human resources, finance, engineering and design, and marketing and sales.

Business to Business (B2B) -- These systems facilitate business relations among organizations by extending traditional business process and support systems beyond company borders. Business to Government (B2G) systems share similar characteristics.

Business to Consumer (B2C) -- These systems enable customers to transact business with organizations via the Internet, and vice versa.

Consumer to Consumer (C2C) -- These systems function as a cyber place, enabling customers to transact business with other customers.

Of course some systems combine more than one type of architecture, and all of the above types share many security threats, activities or consequences.

The first group of sites, Public Web Presence, are generally geared to establishing a public image and include static content, though some sites contain dynamically generated pages, allowing user customization, such as My Yahoo! These sites store user-provided data, needed to fulfill requests, survey data, or personalization preferences.

Theoretically, such Web sites are exposed at least partially to the entire world, meaning the server is open to attack from almost anywhere, including Hyper Text Transfer Protocol (http), that is, the Web service itself.

The fast-path template incorporates prevention of such attacks. The primary security goal is to secure the integrity and availability of information stored on the Web server, where integrity addresses accuracy and completeness of data and availability addresses service continuity and support. Bolstering integrity includes maintaining the security of the system on which the Web service is housed, as well as the server's content. The filtering device must be configured to restrict all types of unauthorized traffic, including any protocols or services other than those needed to offer Web server content.

The environments used to create these Web sites sometimes pose a risk. Advanced Web technologies such as Microsoft Active Server (ASPs), Allair ColdFusion and Sun Java Server Pages (JSPs) often have both subtle and not-so-subtle security ramifications that are not well understood by many Web developers. Examples include leaving debugging information on production sites that reveal sensitive data such as database user IDs and passwords.

For Intranet Web site architecture, information is provided to internal employees, including applications such as a company phone listing, benefits registration system or project management system. The major security goals -- established and met in fast-path template -- are confidentiality and content integrity. Yet these sites are commonly in danger of unauthorized access, sharing many of the same risks as public Web sites.

The major security challenges of business to business architectures, which handle data exchanges between commercial enterprises, revolve around confidentiality and integrity of data as well as interoperability and the standardization of security solutions. The potential failure of a critical network component -- such as a router or an encryption device -- prevents trading partners from communicating, or conducting business. Non-repudiation, the ability to prove an individual was party to a business transaction, is also a key goal. Due to the high dollar volume of business to business transactions, interest is high for using strong authentication measures and digitally signing business transactions. Yet these measures alone will not ward off threats. Certain political, policy-level, functional and technical issues must be examined and weighed, including concerns of who do you trust and how much do you trust them.

In the fast-path template for business to business architectures, the major network elements that help achieve security for business to business Web sites include routers and firewalls, digital certificates and a certificate authority.

Business to consumer systems entail transactions between organizations and customers. These include financial services sites, such as online trading, banking and shopping sites, even tax-return submissions. A major goal is confidentiality and integrity. Typically, attackers target the Web server, or end host where information is kept, so organizations must ensure that the highest security measures are met to protect the Web servers and back end data stores.

The fast-path template for a secure business to consumer system provides an overview of how a secure system might work. With the entire world able to visit the site, restricting access to a subset of people is impossible, making the security risk at least as great as in the case of a public Web site. In addition, the responsibility of maintaining a secure site falls squarely on the organization offering the service.

Confidentiality and integrity must be maintained during the transmission of data, which occurs between the consumer and the organization's Web server, and between the Web server and the organization's internal data bases. For this to happen, there must be a high degree of integration between the Web servers, local back-end data bases, and often the fulfillment systems, clearinghouses, or suppliers that the organization does not own or operate.

Finally, in consumer to consumer architectures, online applications such as Web-based auction sites in which consumers can exchange goods are a prime example. The fast-path template for such systems is built around ensuring that such transactions as bids, postings, or shipments of goods are secure and reliable.

As mentioned, prefab or template solutions can be used to get a secure Web site up and running in much less time than it would take when using the traditional method or "born yesterday" approach, despite the diversity of business models that now exist. An organization must of course perform its own due diligence for determining acceptable safeguards, drawing on these business models as building blocks. While no template will be a 100 percent solution, getting a running start with say an 80 percent solution can ensure both security and time-to-market goals are met.