JANUARY 2003 (UPDATED)

The Importance of Application Security

By Matthew Levine
mlevine@atstake.com

Matt Levine is a Managing Security Architect at @stake, Inc and a member of @stake's Application Security Center of Excellence.

Protecting corporate assets from outside threats is important, but how effective is a secure perimeter when ports 80 and 443 are deliberately left wide open? Serious attackers target the applications themselves, making application security today's predominant security challenge. Increasingly sophisticated assaults transcend even the most advanced network and system security strategies. At a time when the majority of attacks are attempted from the inside, how can you best protect your business-critical applications and reduce your exposure to risk?

The Business End of Security

While enterprise spending on digital security initiatives is steadily increasing, resource allocation most often focuses on infrastructure security. Infrastructure security components, such as firewalls and intrusion detection systems, effectively contribute to network security. By design, however, the network must route legitimate traffic to the critical resources housing business logic in the form of applications. Network security protects the integrity and reliability of the traffic to critical resources, but application logic must determine what input or transactions are legitimate.

Manipulation and corruption of application logic is an attacker's approach to compromising business data. This reaches beyond crashing an insecure host or temporary business disruption due to a corrupted network; it is the actual theft or manipulation of your data and your user's data with or without your knowledge. A complete security solution should combine multiple tiers of application and network security processes and technologies to maximize the return on limited resources.

The Threat to Business Applications

Modern business applications typically consist of custom code modules, third party software components, and one or more servers. Improper integration of these components can sometimes result in interruptions to the flow of an application's business logic. This may be the root of an application vulnerability that can later be exploited to gain access to your data or manipulate the business logic that handles the data. Even with strong networking security, application level attacks and

encapsulating protocols have proven that vulnerabilities can be exploited over a single port of entry legitimately open for business needs. Your application may behave precisely in the manner that the designers intended through normal usage; but through unforeseen manipulation, attackers may use your application to gain access to restricted resources that may seem protected. Application security can act as your tool to control application usage and prevent malicious users from accessing critical data and resources.

A secure application not only prevents malicious external attacks from succeeding, it plays a major role in detecting internal attacks or other threats to your application. Proper logging, alerting and third party product integration are also just a part of an overall application security process that can provide the greatest protection possible for your resources.

Securing A Business Application

Securing an application is a dynamic and challenging process. Applications incorporate the use of commercial components, such as web or application servers, and integration with networking infrastructure. Often, commercial software products cannot satisfy the precise needs of a business; customized solutions are a de facto industry standard. Just as customized applications are necessary to meet business needs, customized security solutions must be engineered to match each application. This customization process includes tightening vendor products as well as integrating securely designed and implemented custom written portions of the application. Additionally, the network environment should be configured to further enhance security.

How do you approach this challenge? The best approach is often the simplest. Look to the fundamentals of application architectures to provide a strong basis for steering users from misuse and abuse. Properly implemented strong authentication and access controls, combined with comprehensive logging and state management, can significantly raise the bar on compromising an application. Protection of the back end processing is just as important as managing users. Segmenting application processes will help contain incidents in the event that they occur and minimize costs. Finally, integrate your security efforts as early as possible in the build process of your application. By designing a secure architecture at the outset, you can avoid the cost of retrofitting security measures after the application is deployed.

Assessing your Application Security Risk

By performing a subset of steps necessary to secure an application, a strong notion of just how vital this security can be becomes evident. Begin by identifying the assets encompassing a core business application; including any customer or internal data that the application processes and dependent procedures such as financial or accounting practices, etc. Then, through understanding the business value of an application, estimate the costs of the application being corrupted or taken off line for an hour, a day, or permanently.

Now we need to identify the factors for justifying a proactive stance on securing the application level: foremost is the protection of critical data. Customers want to know that the firms they do business with are carefully handling their sensitive information. That means protecting it from the time it leaves their hands to your systems and back again. Data must be protected in transit and storage, while maintaining proper authentication and access control. It is not difficult to find evidence that clients favor a secure transaction system over an insecure one. A fancy user interface, responsive customer support, and great monthly statements won't matter in the slightest, if a customer feels that their information is not being handled responsibly.

The next step is to model potential threats to your application. Before doing so, a responsibility to bear your customers' privacy as if it were your own, must be accepted. Concerned customers will ask what steps you have taken to ensure the privacy of their data. It makes sense to anticipate these questions and have your infrastructure speak for itself in terms of satisfying their security demands. It is simply good business sense. The best answer you can provide your clients regarding security is that you have anticipated their concern as a risk and have implemented solutions or preventative measures to safeguard their interests.

Threat modeling may sound like a daunting task, but risk areas tend to be clearly evident, even in large-scale, complex applications. A few basic models to rely on include external threats such as denial of service issues, loss of connectivity, or corruption of data through exposed interfaces. External threats are better understood and usually get a decent amount of attention, particularly from the networking perspective. Internal risks tend to be more costly and also more difficult to prevent or mitigate. Access control is not always maintained as strictly on internal resources as it is for external ones. Critical data may be restricted from external view, but quite accessible from the inside. Internal connections include employees, contractors, temps, partners, co-location or hosting facilities, and vendors.

Only after threats are identified and understood can effective defenses be implemented. Determining the best approach to mitigating a potential risk is not as straightforward as determining basic approaches to compromising an application. A few basic application security fundamentals are a good place to begin:

- Protecting data in transit with encrypted channels
- Validating user supplied inputs
- Strong authentication mechanisms
- Access control and secure state handling

These are concepts that are normally built in to applications in one way or another. A good exercise is to perform a gap analysis and determine how the current set of security measures included in your application off sets the potential threats identified in the previous step. Of course, basic application security principles extend well beyond this list, but starting here will help give you an understanding of how comprehensive your security defenses are currently.

While these fundamental steps are not difficult to bring to bear in analyzing an application, the greatest inhibitors of comprehensive security are time and money. It may be costly to perform an analysis and schedule security modifications to an existing application. While the cost of retrofitting is a factor, it is insignificant when compared to the costs of losing business due to a compromised application via attack, network disruption, or malicious worms or virus.

Reducing the Cost of Application Security

Hallmarks of software engineering and development maintain that the earlier a problem is corrected, the lower the cost in the overall process. Security measures are no different in this situation. If multiple threats can be mitigated by opting for a certain design over another, then that design will save in the long run over retrofitting another at a later phase. Development groups should strive to analyze their application's security as early and as often as possible. Consider what risks may arise at that time or in the future based on the functionality of the application.

Just like developing an application, securing an application is a process that must be fine-tuned and improved to best fit an organization's needs. By integrating security into planning and implementation, your engineers and designers will gain proficiency in identifying and correcting potential security risks, reducing the cost of fixing it later or after an incident. For further information on getting the most from your application security investment, read "The Security of Applications: Not All Are Created Equal," written by by Andrew Jaquith, Managing Security Architect, @stake, Inc. at http://www.atstake.com/research/reports/acrobat/atstake_app_unequal.pdf.

The Bottom Line

Securing the business logic of an application protects reputations while enabling high value business applications. Security should not be viewed as a priority over accomplishing business goals by restricting an application past the point of usability. Good application security should provide the assurance that an application can function as intended without risk of loss or compromise of data or assets. The early integration of secure engineering principles into the application development process lowers the cost of security and reduces the cost of adding security mechanisms or fixing vulnerabilities. Strong security practices enable you to reliably and safely open applications for business.

About @stake, Inc.

@stake, Inc., the world's largest independent digital consulting firm, provides digital security services and award-winning tools to secure critical infrastructure and protect electronic relationships. The company's SmartRisk℠ services cover all aspects of security, including applications, critical infrastructure, wireless and wired networks, storage systems, and forensic analysis. @stake consultants combine business experience and technical expertise to create comprehensive security solutions for leading companies in financial services, information technology, energy & utilities, healthcare, and telecommunications. Using the @stake Security Blueprint™, clients keep security investments in line with business requirements. Headquartered in Cambridge, MA, @stake has offices in London, New York, Raleigh, San Francisco, and Seattle. For more information, go to www.atstake.com.