

4 section four

Introducing Application Security



Today's enterprises and organisations know they have to protect their IT infrastructure, applications and information in order to stay in business. They are already protecting themselves with firewalls, antivirus and intrusion detection systems. They have also put in place recovery and incident response plans to ensure business continuity, as well as periodic audits and penetration tests to harden overall security.

However, perimeter and IT infrastructure protection is generally insufficient. For example, a faulty software application cannot be adequately protected by a firewall, because attacks may still come in through normal traffic. In that case, only a software patch from the development team can fix this vulnerability.

Furthermore, a once secure application may become unsecured if new functionalities are added or bugs are corrected during its production phase. Mismanagement of the application can have the same impact.

A secure application is an application that properly handles software security from the management, IT, development and audit domains, according to the desired level of trust, taking into account the type of data and the target execution context (legal, business and technological). It must be possible to prove that the predetermined level of trust was reached and maintained.

This paper will present the main concepts and activities required for proving that the predetermined level of trust for an application is reached and maintained.

Luc Poulin, M. Sc, CISSP-ISSMP, CISA, ift.a
CRIM Chief Security Officer
ISIQ Security Senior Advisor
Information Security Institute of Quebec (ISIQ)

1 The Application Security Problem

Today's enterprises and organisations know they have to protect their IT infrastructure, applications and information in order to stay in business. To begin with, all countries have laws and regulations identifying what personal information organisations have to protect. In some countries, it may be dangerous for an organisation and its managers to ignore the law and just do business as they want, or as they might do it in any other country.

No organisation can stay in business if competitors can get hold of its sensitive business data, or if it loses customer's confidence because of an information leak. It is never good for a business to appear on newspapers because of an IT security breach. Customers and partners won't care about the reason for the breach and will take their business elsewhere. Today, many customers and business partners will only do business with organisations in which they

have a "sufficient" level of trust. Aware of this fact for many years now, organisations are protecting themselves with firewalls, antivirus and intrusion detection systems. Their recovery and incident response plans ensure business continuity, while periodic audits and penetration tests harden overall security.

However, perimeter and IT infrastructure protection is generally insufficient. For instance, a faulty software application that must accept credit card transactions over the net, cannot be adequately protected by a firewall, because attacks may still come in through normal traffic, whether connections are encrypted or not. In that case, only a software patch from the development team can fix this vulnerability.

An organisation may identify the targeted application level of trust, not only from its characteristics but also from the business context, the legal context and the technological context where this application will run.

A same software application may be considered secure by one organisation and insecure by another because the first will use it only with non-critical information, or for a non-critical business process.

Application security is not only a matter of IT components and software, but also a matter of contexts: legal context, technological context and business context, or more simply where, how and why this application will be used by the organisation.

Furthermore, a once secure application may become unsecured if new functionalities are added or bugs are corrected during its development and production phases. Mismanagement of the application can have the same impact.

Finally, the cost to implement and maintain application security measures must be reasonable for the organisation. It must cost less than the damages of a security breach on this application. It is a basic risk-management rule.

2 The Never-Ending Responsibility Circle

Recently, I had to perform a security audit on an application for an organisation. We discovered many security issues. When I met with the development team, they told me there wasn't any security requirement on the request for proposal. The organisation who bought the system told me "This is 2007. We're expecting the developers to take care of any security issues by themselves. They are supposed to be software engineers!"

Developers are professionals, but as long as no standard exists or at least an organisation normative framework for Application Security, to help them secure their application, the final decision about trusting an application or not remains with the organisation that plans to use it.

3 Application Security Main Principle

The organisation must be able to identify new security risks introduced by using new applications in its business process. All application development, outsourcing or acquisition projects should be preceded by identifying risks and listing security requirements, in order to identify the target application level of trust. Before the organisation makes final approval to go online with the application, the project team must provide a proof that all security concerns were properly addressed.

Security certification is essential. No one should trust any application if he cannot receive a certificate from the supplier that all its security requirements were well addressed by processes and functionalities, which have been tested and verified to ensure than they are working as expected.

No proof, no security!
No one should trust an application without proof that security requirements were met.

4 Application Security Concepts

Application Security introduces concepts that define some organisation business realities. Important ones are:

Business contexts: a company selling airplane tickets may not have the same security requirements as a company selling telephony services. Both may use the same CRM application but the risk for these organisations to use this application may be different, depending of the business criticality of the process it will help to support.

Technological context: an application running on a Windows environment has different risks than if the same application is running under Linux or Unix. Other factors are network infrastructure, services oriented architecture (SOA) or the need to connect the application to the Internet.

Legal context: an organisation using its application in Singapore and in Canada may have to support different risks from these different countries legislations. For example, in some countries there exist some laws where a manager can be held personally responsible for a security breach of an application under his responsibility, if he cannot prove that all the adequate security risks were identified, measures implemented and periodically controlled.

Application characteristics: All data needed by the application including user data, application configuration data and infrastructure and services configuration data. All user types including end-users, administrators and managers. All application main functionalities such as online banking, LDAP authentication, logging, managing customer information, etc.

Targeted application level of trust: a label associated to a specific list of security requirements that the application has to meet.

Actual application level of trust: the result of a verification that all required security processes and functionalities are working as expected.

5 The Application Security Risk Analysis

One of the main steps for implementing application security at minimal cost is using application security risk analysis. The organisation must predetermine if an application (existing or future) is worth protecting and how much the organisation is willing to pay for that protection. The application risk analysis is a good tool for finding answers to these questions.

At the beginning of an application project (whether the application will be developed, acquired or supplied by an external developer) an application risk analysis must be performed.

From its own contexts, an organisation may define the three contexts where the specific application will be running. Usually, the organisation already has a good idea about what characteristics the application will have to offer, such as what kind of data to be stored or computed, the functionalities to be provided, the type of users who will use and support it, etc.

From those four elements (Figure 1), the organisation will have to derive corresponding risks, which will determine security concerns that may be or must be addressed by this application and the application project.

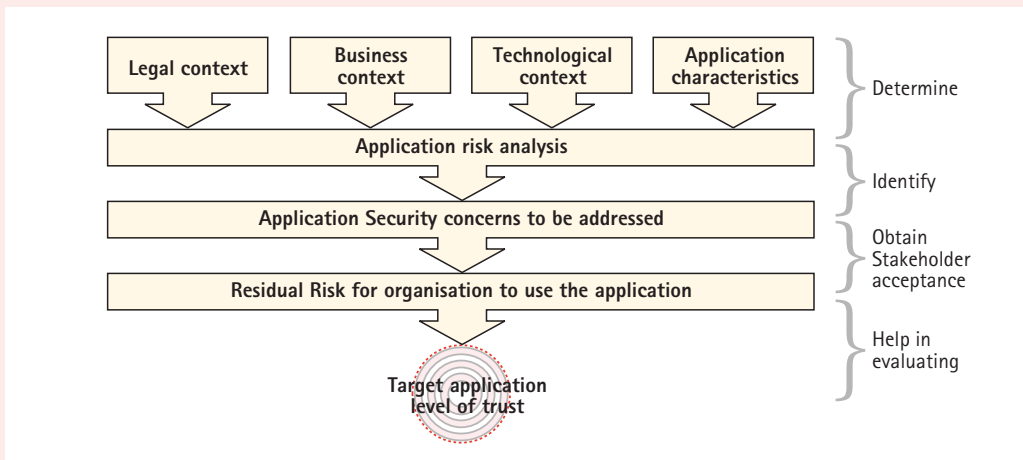


Figure 1: Application security risk analysis process simplified overview

Some security measures may be implemented at project management level, while others will be implemented inside the application itself, such as the secure application architecture, secure functionalities or security services. Specific actors' qualifications may be required on critical tasks and security technological infrastructure enhancements or product replacements may have to be performed to minimise the risk to an acceptable level for the organisation.

Once these application security measures are identified, the organisation will have to decide what will be an acceptable solution for each of them, based on its user-friendliness, its effectiveness and its cost.

When, at the end of the process, the organisation receives assurance that the solutions from all selected application security measures have been verified and controlled, it will then know that the application can be used safely in its specific contexts.

The need for security doesn't end when the application goes into production. The real application life cycle ends only when it is put into retirement, which can happen several years later (up to 25 years is frequent in big organisations). It must maintain the same level of trust for all this time. Periodic verification and control of application security measures should be performed to ensure this.

Roughly, as soon as contexts or application characteristics change, the application level of trust should be verified.

A secure application is an application that properly covers security needs from the management, IT, development and audit organisation teams, according to the target application level of trust, taking into account the application characteristics and the target execution contexts (legal, business and technological). It must be possible to prove on demand that the target application level of trust was attained and maintained.

CRIM Website: <http://www.crim.ca>

ISIQ Website: <http://www.isiq.ca>