

# Advanced security methodologies - Secure coding practices

Pascal Steichen - M2SSIC-Metz

19/02/2010

# Contents

<b>1 Introduction</b>	<b>3</b>
<b>2 Architecture</b>	<b>3</b>
2.1 Architectural Document . . . . .	3
2.2 Principles of security architecture . . . . .	4
<b>3 Design</b>	<b>8</b>
3.1 Principles of security design . . . . .	8
3.2 Some special design issues . . . . .	11
<b>4 Implementation</b>	<b>11</b>
4.1 Principles of security implementation . . . . .	12
<b>5 Operation</b>	<b>13</b>
5.1 Principles of security operation . . . . .	13
<b>6 Testing</b>	<b>15</b>
<b>7 Bibliographic references</b>	<b>15</b>

# 1 Introduction

Secure coding is not simply getting behind it's keyboard and hack, it is real engineering.

Why do bridges support trains for hundreds of years ?

How could an Eiffel Tower swing several meters sideways in the wind and still welcome thousands of visitors per day, without harm ?

Well engineering is taken serious. First there is an **architectural** model, which will provide **design** plans (blueprints), only then construction (**implementation**) can start.

Why shouldn't we adopt this procedure too ?

Well we should !

# 2 Architecture

A *security architecture* is the process of selecting design elements and principles to match a defined security need. This implies to know how secure the program should become !

A good security architecture can be applied many times, to many applications and should serve as a framework for secure design decisions. A good advice is to work with an *architectural document*, where the different aspects are laid down.

## 2.1 Architectural Document

- Program organization
- Change strategy
- Buy versus build decisions
- Major data structures
- Key algorithms

- Major objects
- General functionality
- Error processing (corrective or detective)
- Active or passive robustness
- Fault tolerance

## 2.2 Principles of security architecture

- Ask questions

About what ? Some basic topics, are:

- About the worries
- About the resources
- About the software itself
- About the goals

And get answers before continuing the architecture process.

- Focus before leaping

It is important to know the destination before stepping on the gas. Engineers are problem solvers by nature, so first the problem should be well defined as well as the goals to reach.

- Define "just secure enough"

The idea is not to make an application *as secure as possible*, but *just secure enough*. Resources (of any type) are expensive so a precise definition on how secure an application should be, that is appropriate to the (business) context (it's environment), is crucial.

- Do engineering not prototyping

Employing standard engineering/construction techniques for software is critical for a good development process. Good security requires good design and good design techniques. This can avoid factors like :

- lack of any design
- simple human weakness
- poor coding practices

- Identify assumptions

Good engineers have in common the ability to look objectively at elements like mental models, system resources and process interruptibility and suspension. This enables clear identification of assumptions to be handled correctly.

E.g. *The users of this application will be human beings.*

- Get security in from day one

Research reveals that fixing a security bug in the design phase costs 1/60th of the cost for the same bug to be patched after the release. Planning with this in mind does save costs, maintenance and as such security of the application.

- Design with the enemy in mind

This is the *adversary principle*. It's important to try to anticipate how an attacker might approach solving the security puzzle of a specific application. This implies knowing a little of the usage environment of the application, to identify potential enemies.

- Work with the chain of trust

The chain of trust must be understood and respected, it's not save to invoke untrusted programs from within trusted ones. Secure applications should always validate what is presented to it, should not pass tasks to less-trusted entities and only emit valid and safe information.

- Be stingy with privileges

Sometimes called *principle of least privilege*, the idea is to limit privileges to it's uttermost needed.

- Always test against policy

Every attempted action must be tested against policy to get a stringent security, this is also called the *principle of complete meditation*.

- Build in fault tolerance

To build appropriate levels of fault tolerance, the 3 Rs, from the CERT-CC, come in the play:

- Resistance (deter attacks)
- Recognition (recognize attacks and potential impacts)
- Recovery (provide full service recovery after attacks)

- Address appropriate error-handling
 

This should indeed be considered at every stage of a software's life-cycle:

**Architect** Adopt a general plan for error handling, like stop on bizarre (unexpected) issues and log on all others.

**Designer** Devise rules on how to detect, discriminate and respond to errors.

**Coder** Capture the triggers and implement the design.

**Operator** Needs to check processes and if error handling is efficiently done.
- Degrade gracefully
 

Graceful degradation is the fact to continue operating in a restricted or degraded way, if something fishy happens, instead of simply stopping or failing.
- Fail safely
 

What should be the default fail behaviour of a given application ?
- Choose safe defaults
 

The "fail-safe" argument from before is somehow a sub-element of this: the need to provide safe default actions in general.
- KISS (Keep It Simple Stupid)
 

Simple systems are easier to design, implement and test well, moreover, features that don't exist can't be a security risk, nor can have bugs.

"A good theory should be as simple as possible - but not simpler."  
Albert Einstein
- Modularize
 

Modularize thoroughly and fully.
- Don't rely on obfuscation
 

Security through obscurity doesn't work ! Concealing how something works (like encryption algorithms) is in no sense an advantage, but can, in contrary, be dangerous. Security should be intrinsic.
- Seek statelessness
 

By state we think of the information a program retains while a transaction (or command) is executed. If a program retains minimal state, it's harder for it to get into a confused, disallowed state.

- Strive for practical measures and usability
 

In theory there should be no difference between theory and practice, but in practice, there is. That's why it's important to create a usable user environment (GUI, etc.) that makes it easy to do the right thing. This is also called the *principle of psychological acceptability*.
- Make accountability always possible
 

A good architecture must ensure that every action, as well as the responsibility of the assets, can be attribute to a specific individual.
- Limit resources consumption
 

A gentle resource usage contributes to the overall security of a system. Strange or seldom tested exceptions are often only detected when reaching the limits of resources exhaustion.

However, resource-consumption limitation, must also be combined with meaningful error recovery and handling to be really effective.
- Make event-reconstruction possible
 

It must be possible to track the exact sequence of events of key actions. This implies keeping audit-logs, it's the *principle of auditability*.
- Eliminate "weak links"
 

"A chain is only as strong as it's weakest link." Try to eliminate them. This implies planning the security as a whole, addressing the entire range of elements of a specific application.
- Use multiple layers of defence
 

In depth defence is the key, wear a belt *and* suspenders !
- View things in it's holistic whole
 

This goes even farer than eliminating "weak links", it's not enough to create a secure application by it's own. All it's interactions with the outside world must also be considered and from design on.
- Reuse secure code
 

Don't reinvent the wheel ! Make use of code, libraries or whole programs, that are known to be secure. It might even be interesting to have "code reuse" clauses in the policies.
- Don't rely on off-the-shelf software
 

However, despite the previous point, code reuse is not to be taken an easy task. For the sake of security issues off-the-shelf programs have to be treated very carefully, especially for mission critical operations.

Make sure to assess the security aspects of any solution intended for in-house usage.

- Don't forget democratic principles

Security should stay security. Don't implement security measures that mistreat individual privacy rights. In most countries there is a legal framework for this, regard it.

- What did I forget ?

Always ask yourself this question before moving along, humans forget things !

### 3 Design

Good design is the basis for an efficient software development process, as it not only enables to build a good defensive basis into the software from the beginning, but provides safe foundations for future extensions and maintenance.

Secure design has to be elaborated thoroughly, the following steps being typical efforts to perform.

#### 3.1 Principles of security design

- Risk assessment

Before starting to protect, one has to know and understand what is to be protected and from whom. This process is commonly called a risk analysis, trying to determine the threats, the vulnerabilities and their impacts.

It probably sounds a little strange to perform a risk analysis for the sole purpose of developing an application, as such an analysis normally includes the whole organisational aspects as well. Well that's exactly what is sought. The aim is to define all the implications the new element will have on the whole and vice-versa.

Despite the specific method chosen, be it OCTAVE, NIST SP800-30, EBIOS, ..., the following essential points should be addressed:

- How does the organization adopt the application ? Are there existing directives ?
- What influence will the application have on the organization ?
- What about the information manipulated by the application ?

- Risk mitigation

After the risks were assessed it is time to think about the management of those risks. Risk is good : *Having* risks is a sign that one's still in business, *managing* risks is a good way to stay in business.

Again dependant on the specific method chosen, this process might diverge slightly. Generally the options of risk management are:

- Risk assumption
- Risk avoidance
- Risk limitation
- Risk planning
- Risk acknowledgement and research
- Risk transference

- Work with a mental model

This practice might somehow look strange, but it is a nice way to get a global picture of the design. Trying to build a metaphor of the future application, can already show some potential issues and suggest solutions. Again, Albert Einstein, with his famous "Gedankenexperimente" can be taken as a prominent example of the effectiveness of such an approach.

- Define high-level techniques

Only now the more technical work can begin. Technical issues can be divided in 3 categories:

- those relating to the application's interaction with itself or other software ;
- those relating to network interaction:
- the specific defences against attack.

- Choose appropriate measures

It's not enough to cover, threats, vulnerabilities and attacks, implementation means more. Detailed and carefully chosen measures are the key for success. Various good practices exist, here some thoughts to consider.

- Background factors
  - Get the "big picture" of the environment and it's customs.
  - \* User "culture"
  - \* Technical traditions

- \* History of security issues (successful attacks, etc.)
- \* Potential targets

- Business issues

Address corporate culture and cost issues, important factors are:

- Maintenance
- Purchase cost
- Business efficiency
- Least noise technique
- False positives (negatives)

- Cost-benefit analysis

Implementing security measures is, of course, a crucial element, however, as with so many things in live, the cost/benefit ratio has to be coherent.

Pay attention to include all costs:

- training costs,
- maintenance costs,
- testing costs
- etc.

To determine benefits is harder, use the detailed risk analysis from before to get the picture.

- Methodologies

With large or long-term projects it is often difficult to keep all the information (collected until now) consistent. In that case a more stringent method can be used to rationalize the approach. This has the following advantages:

- Assumptions and decision become explicit
- Links between assumptions and decision become clear
- Changes can be automatically re-evaluated
- Investment versus risk expectation becomes visible
- Intuitions become explicit

- Evaluate the process

Far less evident yet, is the *principle of repeatable results*. The defined processes for security design decisions should yield consistent, coherent and reproducible results.

## 3.2 Some special design issues

Security design is an important part of software engineering, and the above practices cover the global picture well, or ? Well what about software you didn't design, third-party libraries, existing applications, that have to be secured ? The following three issues are good design practices for those kind of special issues.

- Retrofitting

Without access to the source code one isn't powerless, several significant security techniques exist to "retrofit" such applications:

- Wrappers
- Interposition

- Maintenance

Existing applications, for which access to source code is granted, needing a security maintenance to be up-to-date can be another source of vulnerabilities. Considering the following few advices can help to keep the global security safe.

- Handle with the same care and scrutiny as new code
- Understand the security design spirit in place and follow it
- Learn how the program works (don't trust the manuals)
- Don't introduce new trust relationships

- Compartmentalization

This concept approaches security issues the way that it places untrustworthy users, programs, objects in a kind of virtual box so that they can't do any harm. The three most compartmentalization techniques are:

- Jails
- Playpens
- Honey pots

## 4 Implementation

Unfortunately (already known since Morris's Internet Worm in early 1988) the most common implementation flaw is still the *buffer overflow*. Here some good implementation practices to fight them and others (of course).

## 4.1 Principles of security implementation

- Inform yourself

This might sound implicit, but it's always good to be reminded about.

- Follow vulnerability discussions
- Read books and papers
- Explore open source software

- Handle data with care

One of the central causes of those famous *buffer overflow* flaws is most probably lousy data input handling. The solution is simple: Verify carefully every piece of data input. Ways to do this includes practices like:

- Data cleansing
- Bounds checking
- Checking config files
- Checking command-line arguments
- Treating web content and URLs carefully
- Checking cookies
- Checking environment variables
- Checking all other data sources
- Setting valid initial values
- Handling file-name references carefully
- Storing sensitive data appropriately

- Reuse code

It always makes sense to reuse software or pieces of code that has been thoroughly reviewed and tested, and has withstood the tests of time and users.

- Thoroughly review

Some common review techniques:

- Peer review
- Independent Validation and Verification (IV&V)
- Use available security tools

- Use check-lists

As stated before check-lists are a good way to be sure to cover everything necessary (we're just humans). Some basic entries a good check-list should contain, are:

- Use at least passwords for user access
- User-IDs are unique
- Access control is role-based
- Passwords are not to be transferred in clear-text over the network
- Data transfer is encrypted between servers and clients
- ...

- Create maintainable code

In correspondence with the *Maintenance* section from the design chapter, where "we" were to maintain existing code. Here it's "our" job to be kind to the maintainers. For that task the following practices are useful:

- Use standards
- Remove obsolete code
- Test changes

## 5 Operation

Traditionally in many companies, the development staff and the operational staff are separate and even sometimes thorough competitors. As should have become clear till now this is a very bad approach. Development and operations are two sides of the same coin.

Security is everybody's problem !

The operational level security measures can be seen as a layered system of practices.

### 5.1 Principles of security operation

- Harden the network

Security most of the time begins on the network level, but one should not stop here.

- Allow only used services
- Use secure protocols
- Compartmentalize the network
- Monitor unauthorized traffic
- Deploy multiple layers of defence
- Log

- Secure the OS

The network and OS are the foundations on which the applications are build on, consider them deeply.

- Start with a secure installation
- Use good file access controlling
- Allow only used services
- Remove unused stuff
- Patch
- Log

- Deploy carefully

Now, with the network and the OS secured, comes the application.

- Consider file access controls
- If feasible, use compartmentalization
- Switch event logging on
- Apply same standards to third-party code

- Define sound operations practices

- Manage privileges
- Conduct operations tasks securely
- Manage configurations
- Keep patches up to date
- Manage users and accounts
- Treat temporary staff appropriately
- Test configurations
- Set up checks and balances
- Do backups, securely !
- Keep incident response plan (ready)

- Finally ...  
... keep in mind that security measures are a process not a one time work. Applications decay, by itself or via environment changes, maintain them !

## 6 Testing

About automation and testing, some useful automation tools to test the finalized applications.

- Libsafe (prevents BOs during execution)
- Immunix tools (runtime prevent BOs)
- Janus (does application "sandboxing")
- RATS (scans C, C++, Perl, Python and PHP for common security flaws)
- Splint (scans C for vulnerabilities and programming mistakes)
- UNO (detects : Uninitialized variables, Nil-pointer references and Out of bounds arrays, for C)
- whisker (cgi flaw scanner)
- Gprof (produces execution profiles)
- Nmap
- Nessus

## 7 Bibliographic references

- [Secure Coding - Principles & Practices, M. Graff & K. van Wyjk](#)
- [Code Complete 2, S. McConnell](#)
- [Secure Programming for Linux and Unix HOWTO, D. Wheeler](#)
- [Security Attribute Evaluation Method: A Cost Benefit Approach \(SAEM\)](#)
- [for bad practices: BOFH](#)