

The Basic Problem



There's an axiom in security that "*Any engineer can design a product that he himself can't break.*" There was once a man back in the 60s who bought a new Corvette and had a large, custom stereo unit installed. The unit was so large that the dashboard had to be removed to mount the unit properly, so the man felt quite confident that the stereo wouldn't be stolen. The thieves who quickly stole his stereo used a hatchet to cut the center out of his dashboard.

He had neglected to ask a thief how they would evade his security measures.

Many security projects are approached the same way—the focus is on functionality with security tacked on at the last moment with little thought to the actual threat environment or the resources that might be brought to bear in order to attack the system.

Other projects may include excessive security features from the standpoint of design and consulting costs, but are not necessarily more secure. Many dollars can be spent on technical security with robust and redundant systems that resist the kinds of penetrations that they were designed to thwart. Yet the security features can be circumvented by unusual attacks which may involve simple field modifications that are not detectable by the configuration control system.

The Basic Solution

Just like our friend with the Corvette, it's best to get a thief's advice when designing an information assurance (IA) product—not just once at the beginning but periodically along the design and evaluation timeline.

Consultants who provide the thief's experience are about four times as expensive as the engineers who are designing the product, so in order to be cost-effective the consultant should save four hours of engineering time for each hour the consultant charges. In a product designed for high-risk situations, even more consultant hours may be necessary since the cost of failure can be added to the cost of the engineering time saved.

This paper presents a life-cycle approach to the development of custom, secure systems. History has shown that independent security and risk analyses during the concept-development and system-design phases avoids the excessive loss of time and money, and possible product rejection, during the security certification and approval processes.

This paper presents a life-cycle approach to the development of custom, secure systems. History has shown that independent security and risk analyses during the concept-development and system-design phases avoids the excessive loss of time and money during the security certification and approval processes.

If the accrediting authority is involved at the preliminary design review and presented with the threat and risk assessment, and if the risk mitigations are documented throughout the life-cycle of system development, then there are no surprises during the certification or approval processes.

The products designed and built with this life-cycle approach tend to be certified and approved for field use with a minimum of redesign and rework. Short-term budget constraints may force a reduction in the scope of the life-cycle security analyses, but there are some subtasks that cannot be ignored, especially security risk assessment and risk mitigation which should be part of every progress review since they are critical to final accreditation.

History has shown that when a product or system is developed without the life-cycle security analyses, the accreditation process is often quite stressful for the customer's management. Rather than approving a product that meets all the operational and security requirements, they are forced to deal with the security problems identified during the certification step which either must be ignored,

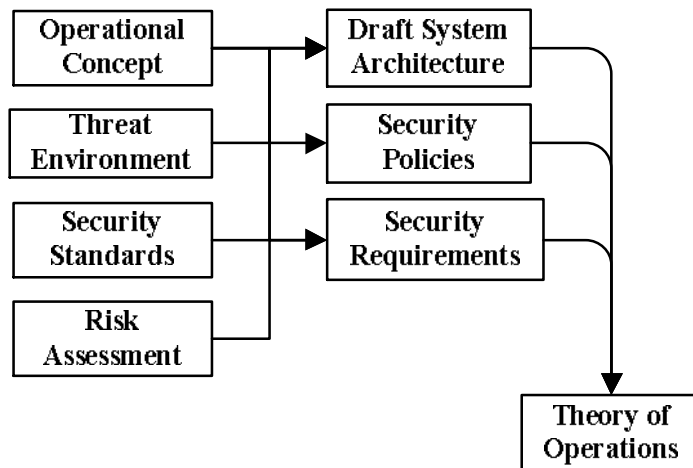
patched or solved with security policies that are hard to enforce.

Let's look at the various stages of IA projects and identify the most cost-effective places to involve the consultant.

The Concept Stage

At the very beginning of a project, after the preliminary feasibility studies but before design actually commences, it's necessary to determine if a product can be created with the resources available to meet the information assurance demands. There are a number of inputs to this part of the process.

A Theory of Operations combines the basic architecture of the product, the security requirements that it has to meet, and the Security Policies that will protect the information.



The *Operational Concept* is how the product will actually be used in daily use including the information inputs and outputs. The *Threat Environment* and a *Risk Assessment* have to be considered in order to determine the selection and strength of the IA features.

The value of an information loss should be considered along with the embarrassment and legal consequences to the information owner. This is a complex, multi-dimensional problem which should not be left to mere assumptions if you want to minimize the combined cost of producing the product and of future information loss.

The *Risk Assessment* is often neglected but can reduce costs by focusing the security features on the anticipated threats. The risk assessment should consider not only the likely actions of the attackers but their motivation, and resources. The value of an information loss should be considered along with the embarrassment and legal consequences to the information owner. This is a complex, multi-dimensional problem which should not be left to mere assumptions if you

want to minimize the combined cost of producing the product and of future information loss.

The output of this stage is a *Theory of Operations* document which combines the *Draft Security Architecture* of the product, the *Security Requirements* that it has to meet, and the *Security Policies* that will protect the information in areas where the product can not. There is always some security-relevant issue that is beyond the control of the product.

For instance, consider a case where the product must use a password that was created in another system so the new product cannot enforce the requirements for password quality. There would have to be a security policy that passwords created in the other system would have to be of a certain quality.



This stage in the design is the most critical and cost-effective point to involve security consultants. Every aspect of the design at this point is merely words on paper and easily changed. From this point on the engineers will start charging hours and making the design increasingly expensive to alter.

The largest cost savings occur at this stage by minimizing the security requirements which contribute to high design and operations costs later on. Some costs, such as the length of a cryptographic key have no effect on costs in modern systems; a 256 bit key has the same cost as a 40 bit key. Other security requirements, such as encrypting all files in storage on hard disks, will produce millions of dollars of ongoing costs even in small organizations. The cost of such an extreme security requirement is almost impossible to justify. A more moderate requirement that identified a smaller class of files to be encrypted may be justified once the risk assessment is completed. The consultants must be experienced enough to match the security requirements to the threats and risks.

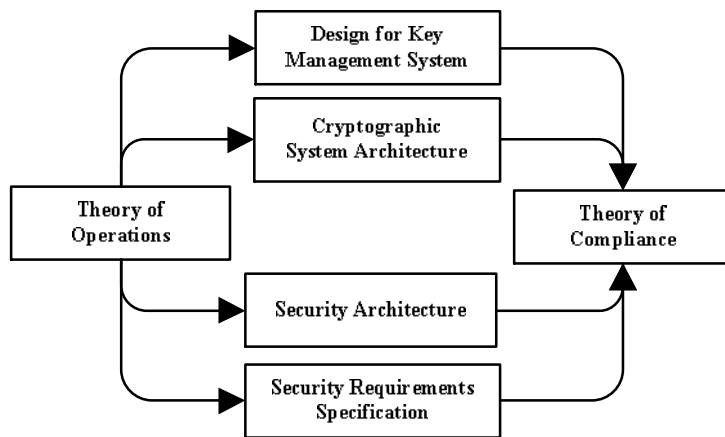
The Design Stage

There are two critical steps during the design process that involve consultants; the preliminary design review (PDR) and the critical design review (CDR). From the consultant's point of view, the design stage is focused on the *Theory of Compliance*. They continually ask themselves questions like: Is the design compliant with the security requirements

document? Do the preliminary and final designs counter the threats identified in the risk and threat assessment documents?

There's a feedback process at PDR. Now that the design has started to take shape, it's a good time to question and alter, if necessary the original assumptions and perhaps the requirements. This feedback has been omitted from the drawings for clarity.

Security consultants must be involved in the preliminary and critic design reviews in order to insure that security deficiencies are removed before the product goes further into the design process where errors are more expensive to correct.



Of these two design reviews, the PDR is the most important from the consultant's viewpoint because from that point on, the cost of changes increases dramatically. The CDR should include just a quick check by the consultant to see if the final design matched the preliminary design from a security standpoint.

The period between the CDR and PDR involves consultants only sporadically to answer questions about the details of the design. If the design involves cryptography, the designers should check with the consultants to insure that opportunities for attack aren't being opened up through poor key management choices or through the modes chosen for the cryptographic algorithm.

The Certification Stage

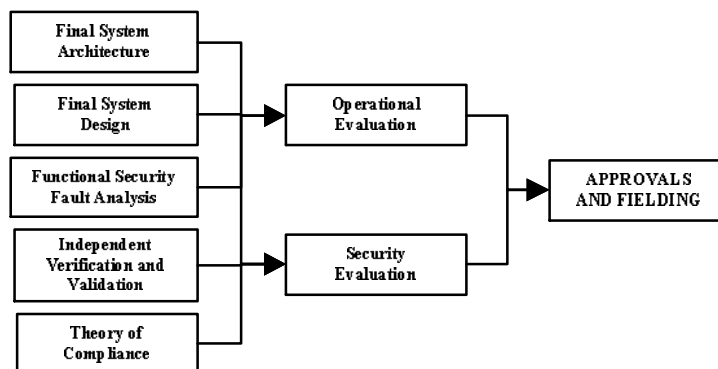
The final stage in the process is getting the product certified for use. The analysis must be carried out from both perspectives—operations and security.

There will be the obvious checks to insure that the product matches the design and that the design matches the purposes for which it is intended. Depending on the amount of risk involved, there may be a place for consultants at this stage.

An independent verification and validation (IV&V) study, which might include a security fault analysis, will physically test the product to determine if the security works. The system will be attacked and attempts made to circumvent or neutralize the security measures. This can be an expensive process depending on the threat environment to which the product will be exposed.

If an attacker is expected to spend \$1 million to break the system, a few hundred thousand dollars spent at this point may be justified. If the system only has to ward off hacker-hobbyists then the IV&V study might be abbreviated or omitted.

The final stage insures that the product is right for the environment. An Independent Verification and Validation study may be necessary when the risks and threats are substantial.



Depending on the future use of the product, the security evaluation might be done by a consultant—generally not the same consultant that was involved in the design stage. In US government systems, the security evaluation is often done by the National Security Agency, or a group internal to the agency that is procuring the product.

Choosing the Right Consultants

Security consultants are paid to assist in the design and later to attack the design. Doing either efficiently so as to minimize cost requires a consultant with enough experience to quickly identify problems.

How much experience is required?

The answer depends on your initial assessment of the threat environment. If your primary threats are from hacker-hobbyists, then any consultant with a few years of experience can help you. If you need to protect your systems against organized crime or foreign governments, then you'll need someone who has experience spending large amounts of time and money attacking systems in unusual ways.

Remember our friend with the Corvette, information thieves will use methods that may be beyond the experience of a well-educated engineer who only thinks of the security mechanisms in the environment for which he designed them. The successful thief is familiar with the average threat environment so he just attacks the product from another direction.

Is ISSI the Right Consultant for You?

Our people have several hundred years of combined experience—in designing secure systems, in evaluating secure systems, and of course, in attacking secure systems.

We think so—we've worked with small startup companies with simple access control problems, and government agencies with extraordinary threats and dramatic consequences of failure.

Our people have several hundred years of combined experience—in designing secure systems, in evaluating secure systems, and of course, in attacking secure systems. Each of our consultants has over 30 years of experience. We usually form teams of people with different backgrounds to insure that each problem is viewed from the widest possible perspective.

We always find flaws in designs. We'll tell you how to fix the flaws; we'll tell you the consequences if you don't. At every step we'll try to help you make cost-effective decisions for your organization, your product and your customers.

Find ISSI on the web at <http://www.infosecsys.com>.

Let's talk about your upcoming project; call Ron Frazer, president of ISSI, at 850.543.2129 or email him at ron@infosecsys.com.