

Security Engineering: Science or Art?

Dave Hays, SSE, CM, MA

ITT industries

(321) 494-4757

Security Engineering, for the longest time, has been an area that only became an issue if a system was penetrated or a virus detected. Security Engineering was viewed as a feature to add on after the "real" engineering was done (the design and production of the system completed). As a result security has been a patchwork of add-on applications instead of being integrated into the design.

Security Engineering has become a recognized need in today's global marketplace. Organizations, both in DoD support and the private sector have realized that the practice of adding security as an afterthought is too costly and security must be part of the system design from the start.

Unfortunately, the design effort sometimes still suffers from our engineering roots. The tendency is to design in all the newest and latest whistles and gadgets. "See how well we protect your system from intruders and insiders?" This can have its own pitfalls as hackers rise to the challenge of systems with better security controls by inventing new methods or finding areas to exploit, leading to the cycle of challenge - exploitation. Additionally the newest bells and whistles may not be the best method to protect the system, sometimes simpler is best. The most expensive solution may not offer the protection to the needs of the system or users.

Security Engineering must first start with an analysis of the system requirements. Security analysis should include such questions as:

- 1) What is the purpose of this system?
- 2) What type(s) of data will it store or process?
- 3) How critical is the data or its accuracy?
- 4) Does the security of the information warrant the cost?

5) Where is the true threat likely to come from?

Security Engineering is another piece of the overall puzzle and must be considered when a project is first conceived and then continue throughout the development of a system to ensure effective measures are implemented.

Let's look at the impact of the five (5) questions asked above.

What is the purpose of this system? The focus here should be will the system be used to process or store financial information, will it be used to for research? Is there a requirement for the system to interconnect with other systems or will it be a closed system? Who will have access to the system and it's data, do all the individuals need access to all of the data on the system or will individuals require different levels of access?

What type(s) of data will it store or process? Will it process or store information such as credit card numbers, security numbers, bank account information or other personnel information? Is the data company proprietary?

How critical is the data or it's accuracy? Here you must consider the effect that loss or contamination/corruption of the information will have. Financial information transferred between banks or stock transfer information are examples of data where accuracy is critical.

Does the security of the information warrant the cost? The tendency is to either over protect the system with expensive measures that can affect the performance of the system, or to implement minimal measures that leave the system open to either outside intrusion or internal attack. Without a proper evaluation either path can have expensive consequences.

Where is the true threat likely to come from? Here's the final evaluation.

After considering the system purpose, data type and information critically you must determine the amount of effort required to properly protect the system.

Studies have shown that while the media reporting concentrates on the outsider threat, these intrusions make up only a small portion of the actual penetrations. The trusted insider has proven to be the largest threat faced by companies today. The insider who has access due to his position or job description can cause more damage than dozens of external hackers either by purpose or by accident.

How do you defend? Monitoring of system activity by the System Administrator is a start. Giving employees only access to the files and directories they need to do their job is another. It's not possible to always spot the disgruntled employee before he acts but by being vigilant you can detect his activity and minimize the effect.

Passwords and permissions can be effective in protecting a system or information from being accessed by personnel who do not have a reason to see the information. Employees should be trusted, they have to be given access to the data and tools needed to perform their jobs but the information must also be protected.

The Security Engineer must give the System Administrator the tools necessary to operate their system in a safe and secure manner. If the security tools are integrated properly then the Administrator will be more comfortable using them and less likely to disable the security features.

System Security doesn't need to be a mystery. Education and experience are needed to give the Engineer the knowledge to do his job. By developing the security architecture from the system requirements, and focusing on system purpose, data storage

or use and information criticality an Engineer can help design an efficient system with security built in without adding applications that have not been integrated. If the Security Engineer does his job, then the System Administrator and users will utilize the security features and thus protect the system as much as possible.