

SECURITY IN EMBEDDED SYSTEMS

Jesús Lizarraga, Roberto Uribeetxeberria, Urko Zurutuza, Miguel Fernández
Computer Science Department
Mondragon University, Spain
{jlizarraga,ruribeetxeberria,uzurutuza,mfernandez}@eps.mondragon.edu

1. Overview

An embedded system is a special-purpose computer system, which is completely encapsulated in the device it controls. An embedded system has specific requirements and performs pre-defined tasks, unlike a general-purpose personal computer.

The security of this type of systems is a pending subject and this can soon become a problem, even bigger than the lack of security of current desktop computers. A false sense of security on embedded systems exists as we are familiar with news about vulnerabilities and attacks on computer systems but there are still few reported attacks on embedded devices.

However, attacks and exploits on embedded systems are starting to get the attention of the hacker community. There are more and more exploits against PDAs and "mobile phone hacking tools" available on the net.

Table 1. Attack difficulty classification

Level	Name	Description
1	None	The attack can succeed by accident. No tools or skills are needed.
2	Intent	The attacker must have a clear intent in order to succeed. Universally available tools may be used (e.g., screwdriver).
3	Common tools	Commonly available tools and skills may be used (e.g., soldering iron).
4	Unusual tools	Uncommon tools and skills may be used, but they must be available to a substantial population (e.g., multimeter, oscilloscope).
5	Special tools	Highly specialised tools and expertise may be used, as might be found in the laboratories of universities, private companies, or government facilities.
6	In laboratory	A successful attack would require a major expenditure of time and effort and the resources needed are available only in a few facilities in the world.

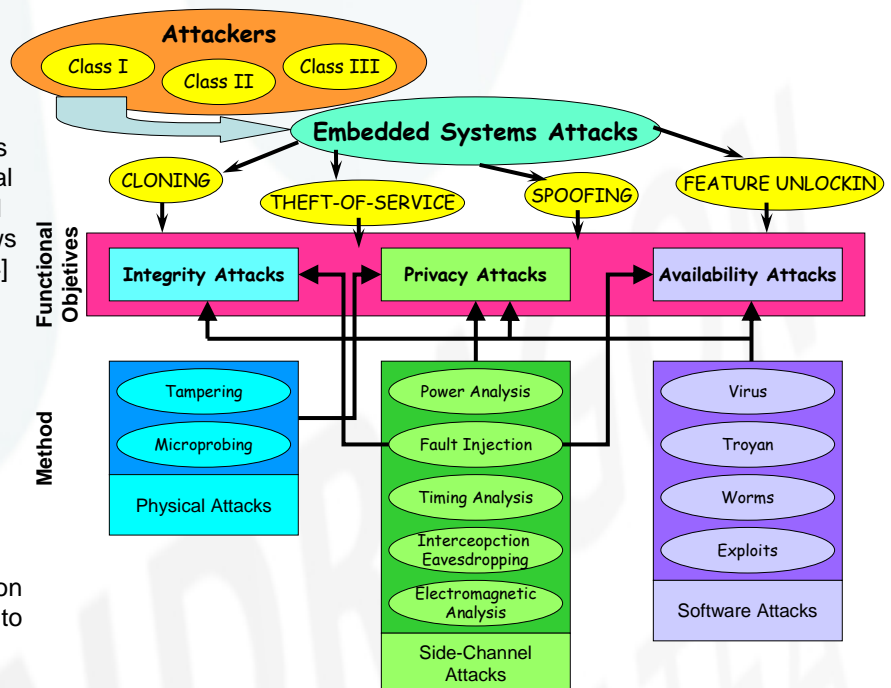
2. Attack Difficulty

Some embedded systems may incorporate security measures that will make more difficult to accomplish an attack. To classify the level of protection of a product Weinhart et al. [3] specified six levels of difficulty to succeed in attacks. Table 1 shows the description of those levels.

3. Attacks on embedded systems

It is possible to classify the attacks based on their final goal, functional objective and on the method used to execute them. The Figure shows a classification based on Ravi's [4] taxonomy of attacks.

- At the top level, attacks are classified into four main categories based on the final goal of the attack.
- The second level of classification is the functional objective of the attack.
- The third level of classification is based on the method used to execute the attack.



4. CONCLUSION AND FURTHER WORK

There is a lack of security on present embedded systems. Security is not usually taken into account during the design phase of the product and it is difficult to implement once the product is completed.

There is an increasing number of security threats over embedded systems and various hacker attacks that jeopardise the commercial viability of new products or that can endanger the correct operation of existing ones. For this reason, manufacturers must secure their products against specific threats trying to achieve a balance between the cost of security implementation and the benefits obtained.

However the implementation of security measures is not enough. It is also necessary to verify the effectiveness of these measures and even check for gaps or hidden threats. The product must be regularly monitored and updated in order to have the greatest effect possible against attacks. To accomplish this the definition of new security evaluation methodologies that take into consideration the changing nature of security and will assure that the product will remain secure is necessary.