Physical protection in mobile constrained devices

Benjamin Arazi

A fundamental problem

Mobile devices like wireless sensors or RFID tags can be physically accessed by any party, raising a particular need for physically protecting the secret key they use in secure communication.

This vulnerability should be treated while also considering the constrained conditions (cost, energy) under which such devices operate.

State of the art

Physical-security state of the art: Current physical security techniques resort to using special glue, coating methods, and the like. **No fundamental proofs are employed here, beside the 'good feeling' of the designers.**

Channel-security state of the art: **The security level of current channel security techniques is proved by mathematical theories**. Solutions must be accompanied with security modeling and proofs.

Motivation for physical security R&D

The security of a system is as strong as its weakest link.

The security of an entire RFID or mobile sensor system is currently based on `art' rather than science.

There is a need to devise physical security mechanisms whose strength can be evaluated and proved based on established theories from physics.

Suggested physical security R&D

Security strength is based on the extent of the inability of an adversary to perform an operation that is easily performed by valid users.
Two challenges:
- **devising means for executing this principle and**
- **devising means for accurately evaluating the adversary's inability.**

The possibility of **harnessing nanotechnology tools in satisfying secured memory execution and evaluation** should be considered.

Molecular memory

In nonvolatile molecular memory, a molecule is used to store a charge. Setting and resetting a memory cell is implemented by applying appropriate electric bias. Multilevel molecular memory involves nanowires whose electrical conductance is adjusted by molecules that accept or give electrons.

Such principles provide ample possibilities for preventing external probing, whereby the interaction between the probe and the molecule disrupts the stored charge or the electrons that control the conductance of nanowires.

More on probe interaction

The energy needed for reading a stored value by an external tampering probe, and the meaning of the interaction between the probe and the charge or electrons that support the memory, can be exactly evaluated using rules from classical physics.

A provably secure memory should be based on an approach whereby the mere attempt to read a stored value by resorting to illegal means would **provably** destroy the value attempted to be read.

Magnetic QCA

Special attention will be dedicated to the possibility of using here magnetic QCA. (Quantum Cellular Automata.) These nano-scale devices use **magnetic particles for both storage and processing.**

The integration of storage within the processor, in a nano-scale frame, opens new horizons in physical memory security. The extremely low power consumption of a magnetic processor is another advantage of this application when considering constrained components like RFID or wireless sensors.

Mechanical considerations

Secured memories based on established theories from mechanics should also be considered.

For example, possible implementation of electromechanical supports that would collapse when an outside probe approaches the structure.

Another aspect of physical security: Functionality obfuscation

<u>The problem:</u>

The possibility of hiding the functionality of a program or a logic circuit has major security implications. The hidden functionality can be regarded as a secret key, known only to the designer.

Trying to obfuscate the functioning of a CMOS logic circuit, it is obviously realized that an adversary can “shave” a circuit layer-by-layer and copy the fabrication masks. The circuit’s functionality can then be analyzed.

Static vs. dynamic ‘reverse engineering’

QCA circuitry lacks fabrication masks that can be shaved off-line, under static conditions, and optically copied. The circuit functionality is rather forced to be analyzed under dynamic conditions. That is, logic values actually have to be measured in order to realize the circuit functionality.

This observation is further enhanced when considering that in order to differentiate here between an AND and an OR gate, there is a need to measure the value of a fixed bit. This makes the problem similar to reading a stored value, making obfuscation similar to storage security.

Mixture of logic gates and conduction lines

In standard microelectronics, **the transistors and the conduction lines are made of different substances**, introduced into the process by different masks. As the masks can always be recovered by reversed engineering, the logic gates and the functionality of the circuit are recovered.

On the other hand, **QCA cells are the building blocks of logic gates as well as the conduction lines that join the gates when forming a logic circuit**. Having the gates and the conduction lines being made of the same cells obfuscates the discrete logic structure.

Hardware encryption based on controlled reversible computation

Traditionally, cryptographic transformations are based on a mathematical algorithm. The algorithm is first devised and analyzed, and then executed in a general CPU or by dedicated hardware. **This approach dictates hardware resources that cannot always be met by constrained components like RFID.**

The possible implementation, directly in hardware, of cryptographic transformations, where the cryptographic strength of the implementation is analyzed based on hardware/physical means should be investigated. This will facilitate the efficient implementation of cryptographic means in highly constrained environments.

Mobile devices raise a particular need for physically protecting a stored secret key

Current physical security solutions are more art than science

Nanotechnology can be possibly harnessed in satisfying secured memory execution and evaluation

The meaning of the interaction between a probe and a storage cell should be modeled under a variety of implementations

Storage security can be utilized in functionality obfuscation

Physical security mechanisms can be possibly utilized in devising hardware-based secured reversible transformations