Superdistribution
--- The Concept and the Architecture

Ryoichi Mori and Masaji Kawahara

presented by Ping Xu

1. Introduction to Superdistribution
2. Protect Module
3. Conclusion

1. Introduction to superdistribution

- ***Superdistribution*** --- an approach to distributing software, so that:
  - software is available freely and without restriction, but in encrypted form
  - users pay for the use of the software product, not for possessing it
  - software is protected from modifications
  - the software's using terms, conditions and fees are set by the owner
  - this approach relies neither on law nor ethics, instead through the ***Superdistribution Architecture*** --- a combination of electronic devices, software, and administrative arrangements

1. Introduction to superdistribution

- ***S-box ---*** every computer must be equipped with an ***S-box*** (**S**uperdistribution **box**) --- which is the very heart of the ***Superdistribution Architecture*** --- a hardware device which contains microprocessors, RAM, ROM, and a real-time clock. The S-box preserves secret information (such as a deciphering key), and it is implemented as a ***protected module.***

2. Protected Module

- a ***protected module*** is an information container that defends the contained information from attacks.
- There are two kinds of ***protected module***s:

  analogue --- for example,by monitoring the changing of resistance

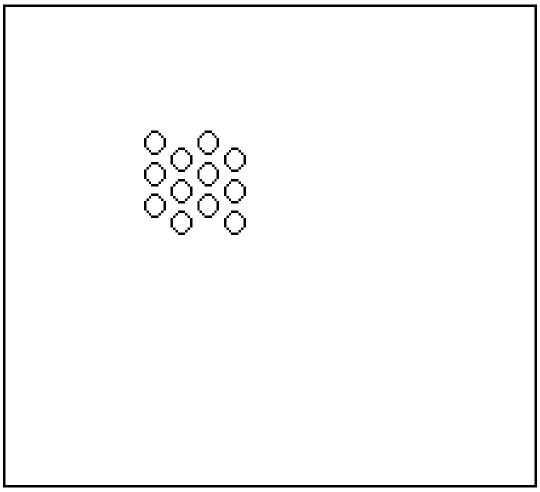
  digital --- I will discuss this one next

2. Protected Module --- digital

- **Tactic** --- by closely spaced detectors and wiring between two layers
  - A detector is an RAM cell. The detectors are individually addressable, and each one can be read or written.
  - A protected layer consists of a great number of detectors, closely spaced.
  - Layers of detectors can be staggered so as to increase the effective density.

    With closely spaced and staggered, the center-to-center distance of adjacent detectors can be made as small as 3 * 10 ^ -6 meter.

2. Protected Module --- digital

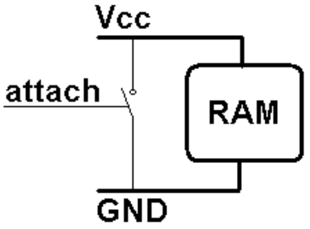


detectors closely spaced in a layer

2. Protected Module --- digital

- Wiring between two layers not only provides signal paths but also provides an additional level of protection.

- If an attack is detected:



secret information stays in RAM. grounping the power supply results in the vanishing of info.

2. Protected Module --- digital

- **<u>Attack detect</u>** --- the procedure is as follows:

  write a random value into the detector and read it back

  write the complement of that value into the detector and read it back

  if retrieved value != written value, a possible attack is indicated

  repeat the test several more times to make sure not a transient error

  test other detectors in the physical vicinity of the erroneous one

  if number of faulty detectors > a threshold, an attack happens!

3. Conclusion

- In my presentation:
  - First, I introduce the ***superdistribution*** --- an approach to distributing software.
  - Then, I mainly specify the digital ***protected module*** --- which uses the detectors to ensure that nobody can physically invade the protected region without destroying one of the detectors.

3. Conclusion

- Today, encryption algorithms trend to not expose the algorithms themselves, but are put in some hardware devices. Clipper is such an example. This paper has similar idea to this trend, it concentrates on the whole, involving hardware and software architecture, to guarantee the whole system’s security. It is worth a careful reading.

QUESTION(discussion)

- If such a protected module must be equipped when you run software or encryption algorithms(in other words, no such a module exists, they cannot execute.), what are the advantages? the disadvantages? What if you are the developer(producer)? What if you are a user?