



# Hardware Protection Against Software Piracy


Published 1984

Tim Maude and Derwent Maude

Presented by Mark Noble



## Introduction(1)

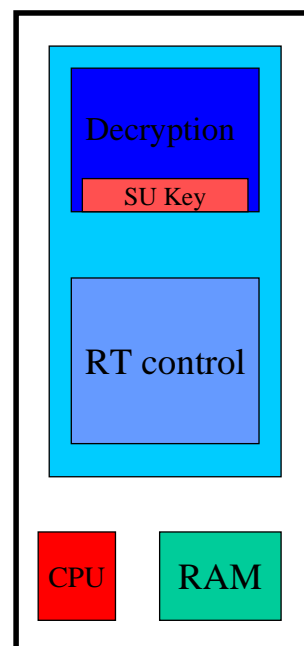
- Author's intent is to discourage piracy by making it more effort than it's worth
  - Pirates might
    - 1 Duplicate for friends (copying)
    - 2 Copy for resale (counterfeiting)
    - 3 Discover algorithms (reverse engineering)
  - Proposed System designed for protection against (1) and to a degree (2)
- 

## Introduction (2)

- The authors give details on the
  - Hardware aspect of the security unit
  - Software aspect of the security unit
  - Encryption algorithm for protecting the software
  - Execution of the protected software ←
  - Possible methods of attack

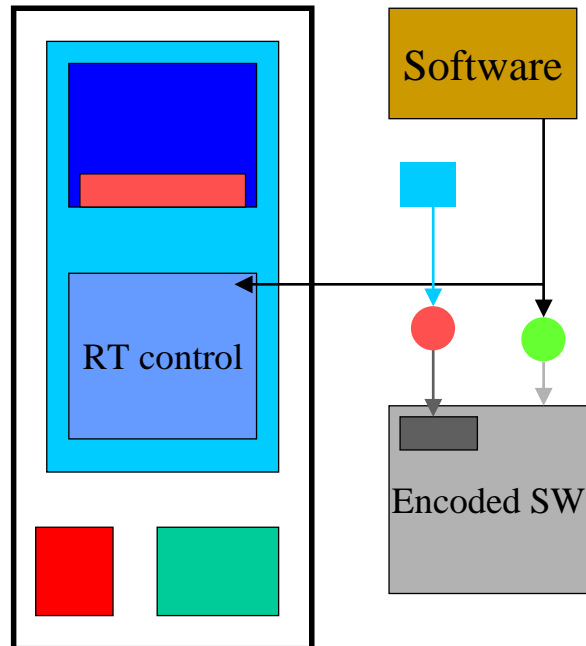
## Security Unit

- Consists of RAM, ROM and a CPU
- Functions are decryption, runtime instruction execution and runtime control
- Security Unit's Private Key is coded into the ROM



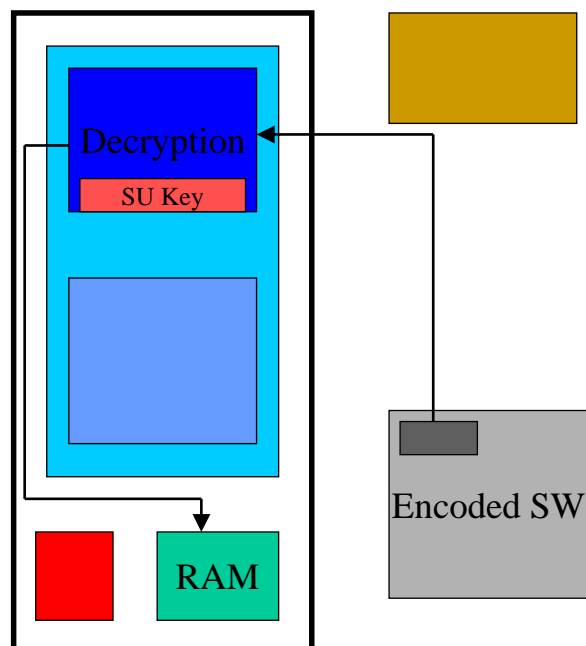
# Software Preparation

- **Software** is protected by
  - Segmenting the code
  - Randomly reordering the segments
  - Move **Runtime path control** into the Security Unit
  - Encrypt **software** with **vendor's public key**
  - Encrypt **Vendor's Private Key** with **Security Unit's public key**



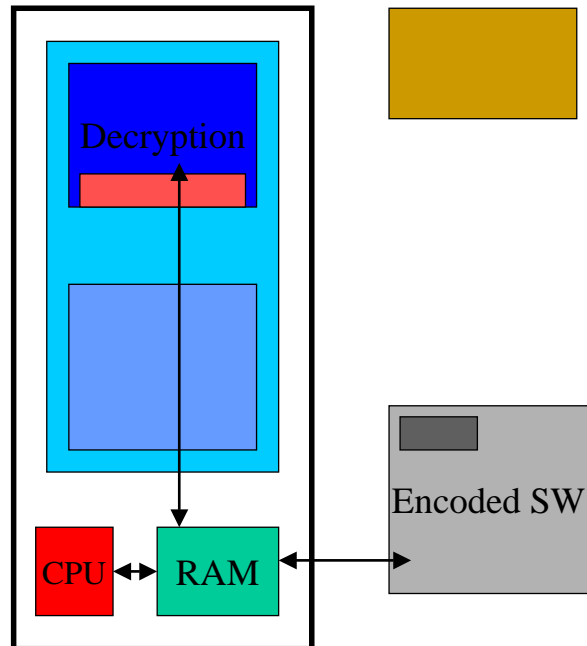
# Software Startup

- On Startup, Vendor's Private Key is decrypted using the **Security Unit's private key**
- Decoded Key moved to **RAM**



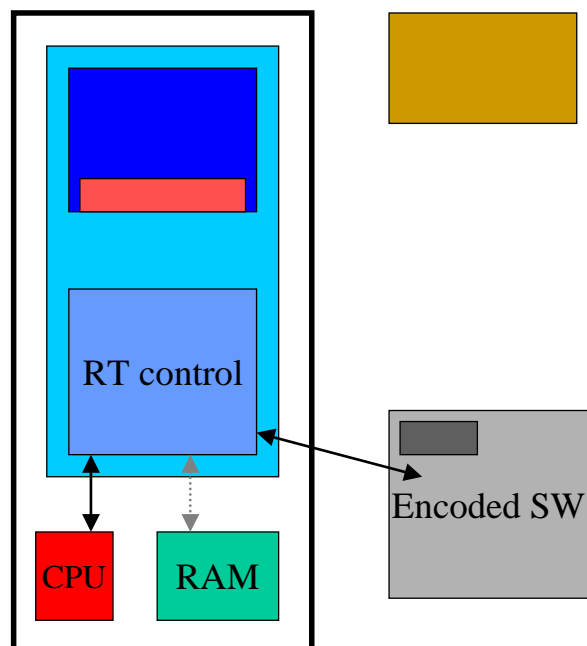
# Runtime Execution

- During runtime, instructions are passed to the Security Unit, **decrypted** using the Vendor's Private Key and then executed
- If required, results are passed back



# Runtime Control

- Branch and case statement decisions are made in the **runtime controller**
- At the end of each code segment, the Security Unit's **runtime controller** is called to determine which segment is executed next





# Conclusion

- Basic ideas of the paper are good but the hardware, software and cryptography need to be updated
- Hardware protection makes hacking an order of magnitude more difficult
- The protection suggested in this paper is adequate for an average person (“Duplicating for a friend” and possibly “Copy for Resale” ), but, in my opinion, it will not stop a determined hacker

Q How much more secure is a hardware and software combination compared with software only?

