Security in Embedded Networks

Elena Reshetova

Nokia Research Center Helsinki

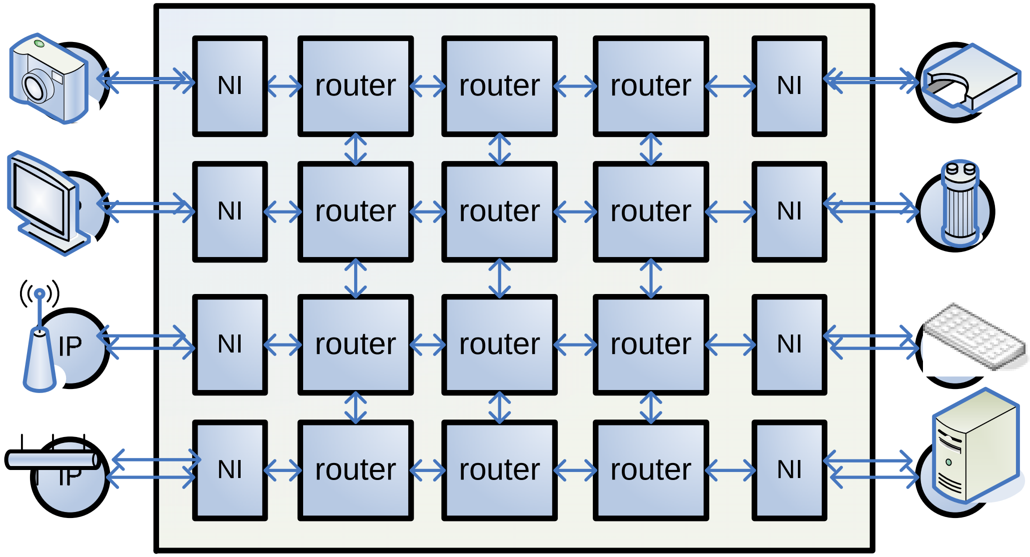
Michel Gillet

Nokia D R&D CT ASD PSD Connectivity SD

Finnish-Russian University Cooperation Program in
Telecommunications (FRUCT) seminar
Tampere, Finland, Oct-08

Background: Embedded Networks

- EN interconnects IPs
- IPs are low-level devices provided by different vendors
- Special IP – CCM
  - Initialization
  - Reconfiguration
- Expected EN configuration
  - IPs ~ 20, Routers ~ 8
  - ~ 4 ports per routers
  - Link speed ~ 1-5Gb/s



Summary of the previous report

- We made a literature study and analysis of current security situation in EN
- We identified the closest network types for EN and made an comparative analysis of their features
- We analyzed attacks and security solutions for these networks
- First thoughts were made about KM and Authentication
- We had an open question: Has EN the same vulnerabilities as considered networks?

Answering the question

Has Embedded Networks the same vulnerabilities?

- YES

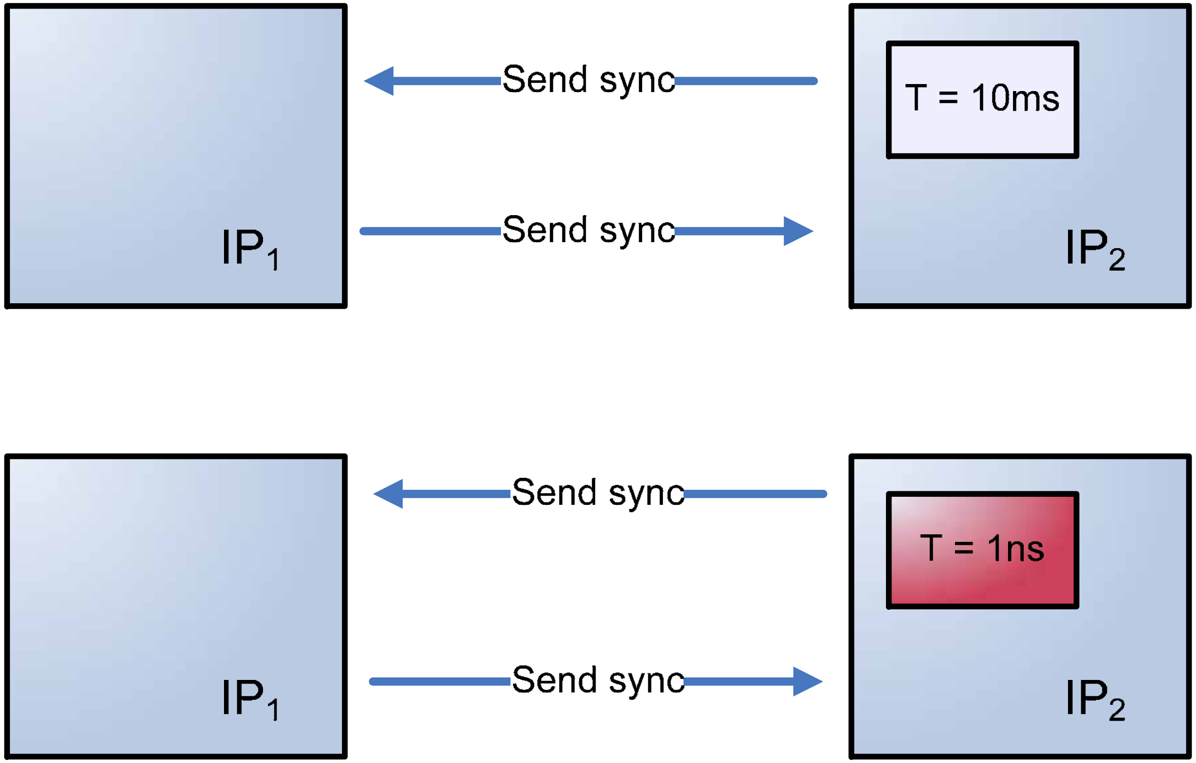
- Which vulnerabilities?
- What is need to be done to fix them?

- Cases
  - IP compromised
  - Router compromised

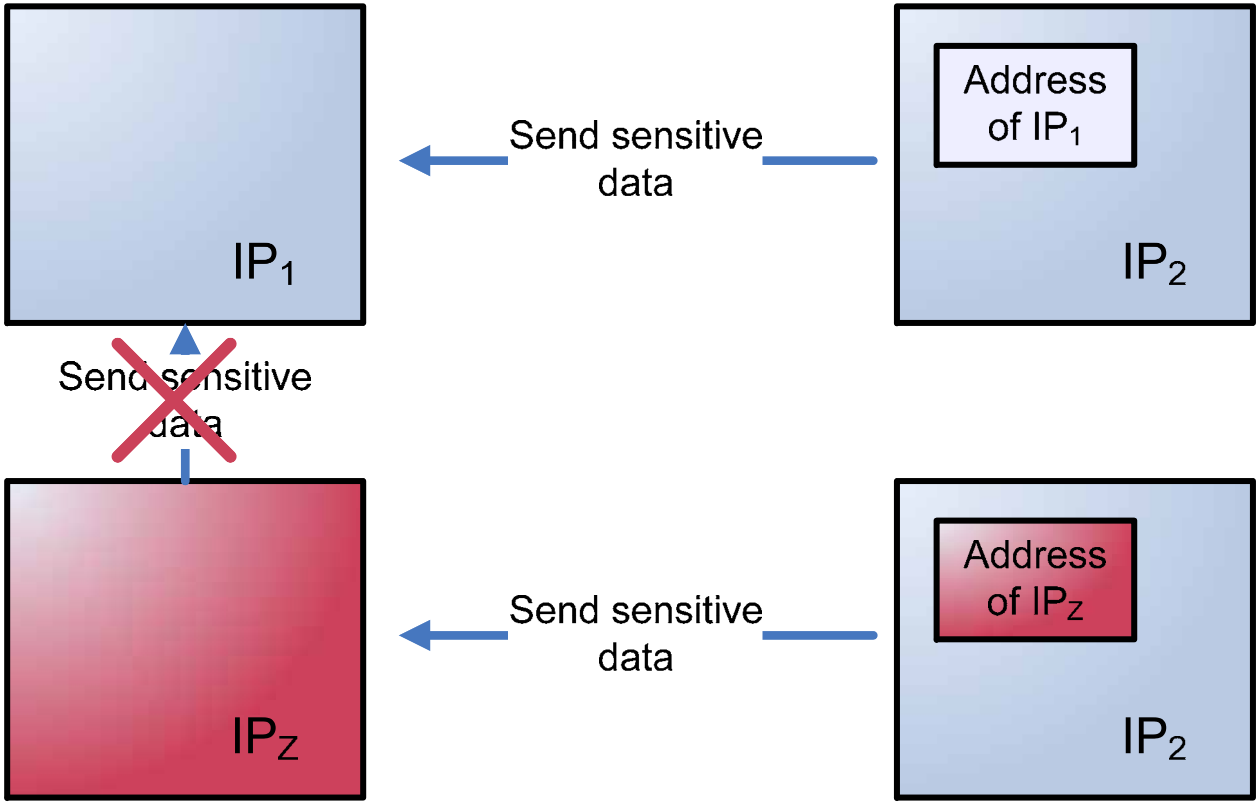
IP vulnerabilities

- IP contains software
  - uploading or fetching from central memory
  - interaction with other application level software
- IP is purely hardware
  - configuration protocol usage
- In case if IP is compromised
  - Misbehavior
  - M-i-t-M
  - DOS attacks
    - Livelocks, deadlocks, flooding

Example - flooding

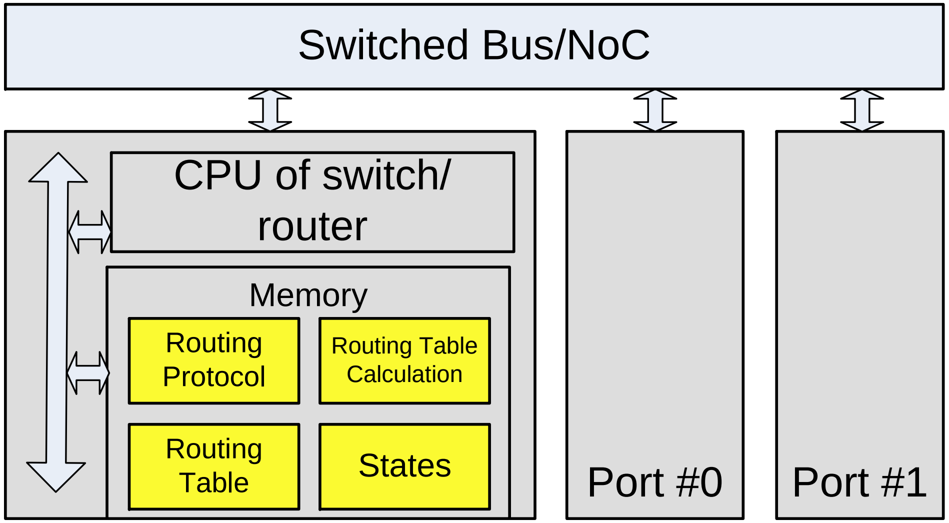


Example – Man in the Middle



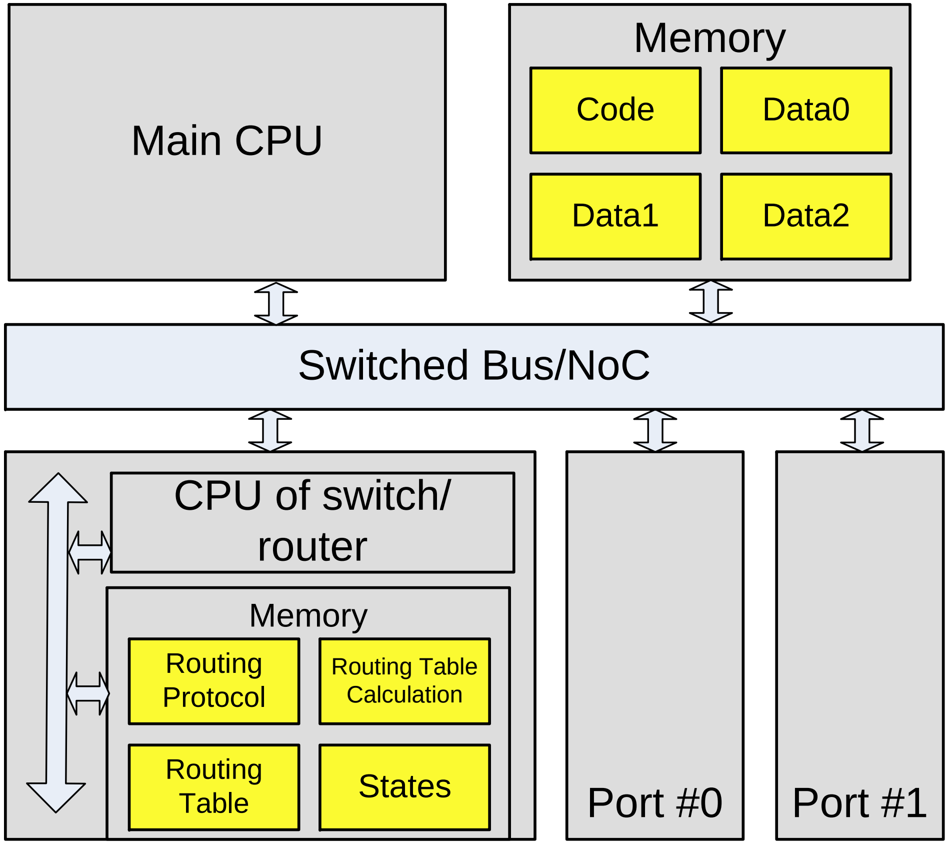
Compromised router

- By external protocols
  - configure protocol to set routing table
  - upload firmware protocol
  - upload some content in its execution memory



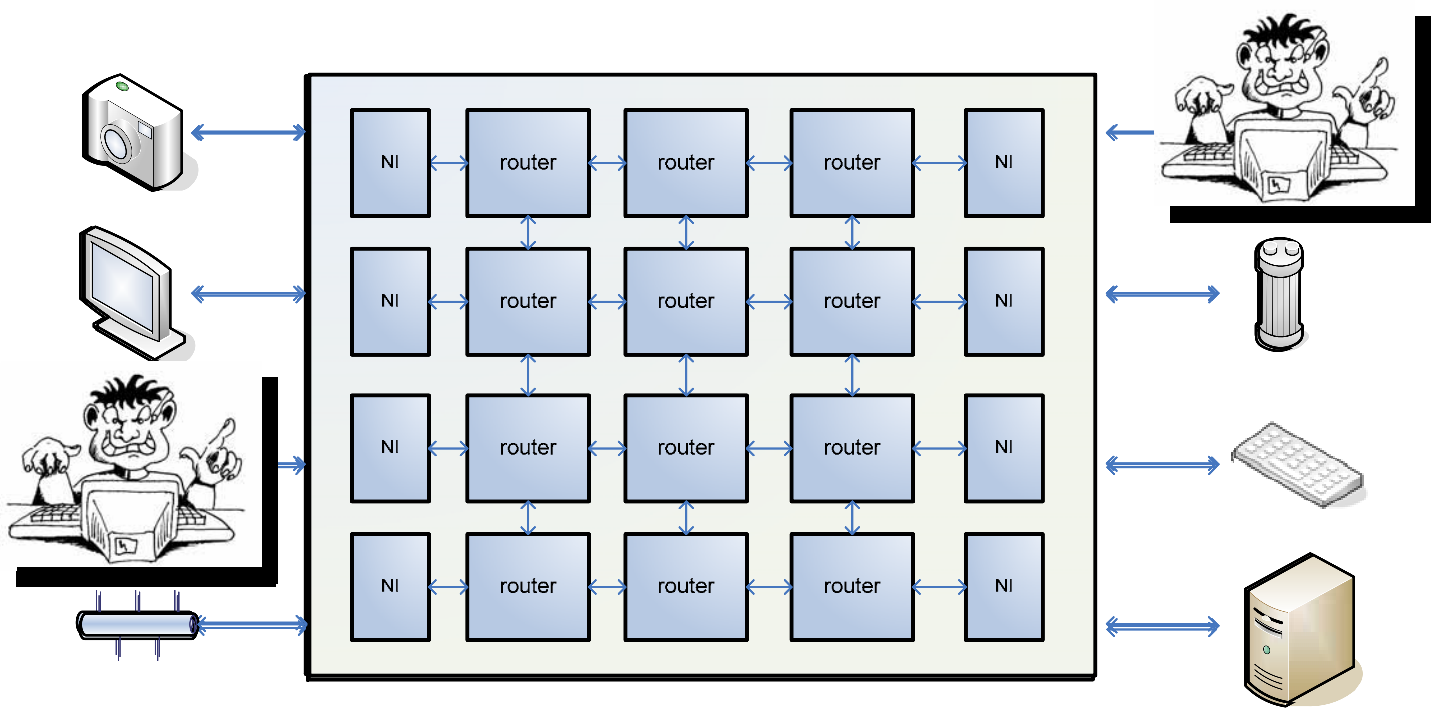
Compromised router - 2

- By internal software
  - gain access to some operation on the bus
  - change routing table, states
  - code executed by the CPU of the router



More possibilities for the attacks

- Some embedded networks have a link to the external word
  - USB-like connector going out of the mobile device
  - Wireless extension of the network



Message authentication

Message Authentication

- We need to authenticate about 128 bits
- Speed should be about 2-4Gbits/s
- Complexity of the hardware implementation should be reasonable

  - CBC-based MACs
  - HMACs
  - Carter-Wegman MACs
  - CRC-based MAC

- Block cipher encryption
  - AES
- SHA
- UMAC, PMAC
  - They all come to block encryption

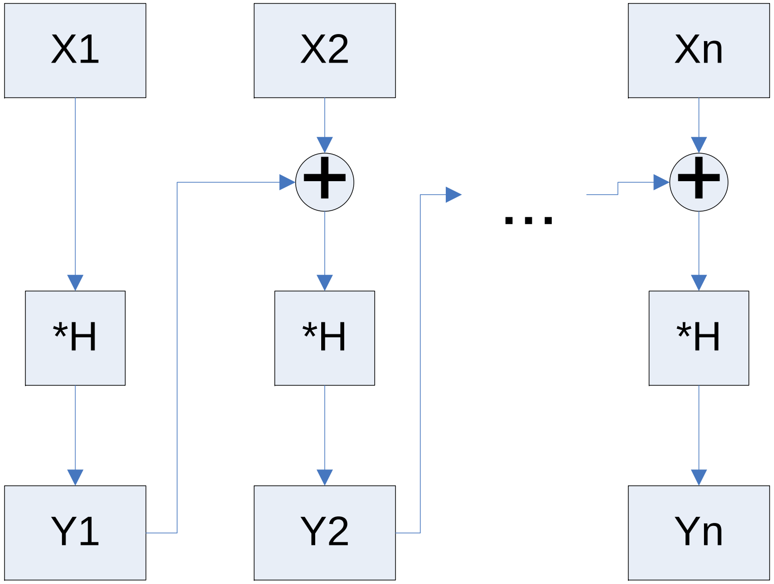
  - Well-known cipher
  - Block size and key size should be minimal

Message Authentication – 3

- GHASH

  by D.McGrew and J. Viega.

  - X + Y – addition over 2^w
  - X * Y – multiplication over 2^w



$$Y1 = X1 *H \bmod 2^w$$

$$Y1 = X1 *H \bmod 2^w \text{ xor } K$$

Conclusions

Conclusions

- Embedded network does have secure vulnerabilities
  - Parts of the network can be compromised
  - Compromised parts can make an successful attacks

- Security should be taken into account during the design phase
  - Proper security solutions should be found for
    - Message authentication
    - Key management
    - Encryption

Conclusions - 2

- Complex security analysis should be done for the network, but also for the endpoints

"*Using encryption on the Internet is the equivalent of arranging an armored car to deliver credit card information from someone living in a cardboard box to someone living on a park bench.*"

- Gene Spafford

NOKIA
Connecting People

Thank You & Questions

Contact information

Email: Elena.Reshetova@nokia.com