Modern age burglary

Jeroen Klaver & Kevin de Kok

University of Amsterdam
System & Network Engineering

Outline

- Introduction
- Research question
- Approach
- Analysis
- Attack vectors
- Impact
- Conclusion

Introduction

- Old setup
  - Alarm systems over PSTN
  - Secure
- New setup
  - Alarm systems over IP
  - Secure?

Research question (1)

- Main question:

”Is it possible to perform a burglary without getting noticed by influencing the communication between the alarm system and the control room?”

Research question (2)

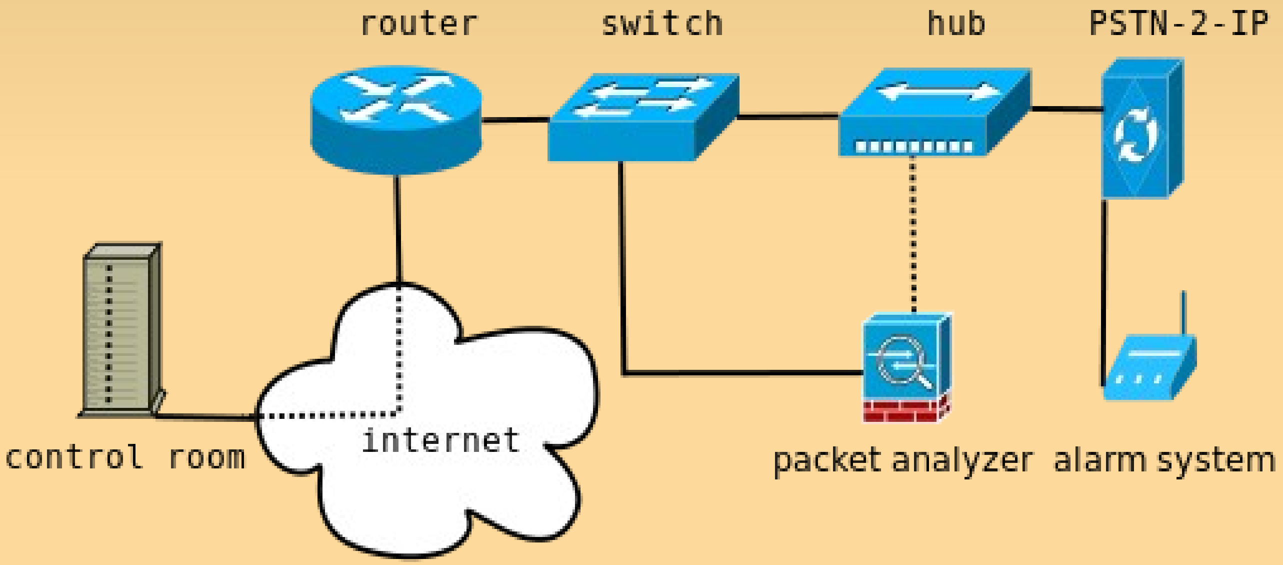
- Sub questions:
  - Which attack vectors that targets communication can be used to bypass the alarm system?
  - What could be the impact if alarm systems over IP-based networks are vulnerable for different attack vectors?
  - Which improvements can be made if alarm systems over IP-based networks are vulnerable for different attack vectors?

Approach

- Traffic capturing part 1
  - Blackbox approach
  - Getting familiarized with the data
  - Recognising information
- Traffic capturing part 2
  - Greybox approach
  - Different events

Network setup

- Hub or bridge



Traffic analysis

- Same packets used every time
  - Registration
  - Activating
  - Deactivating
  - Heartbeat
  - Alarm trigger
- Dedicated ports used for each account
- Each packet is acknowledged

Packet analysis (1)

- Two parts
  - Header
  - Event specific
- Acknowledgement from control room
  - Two versions
  - No repeating pattern

Packet analysis (2)

- Different account code
  - 4 digit number
- Two differences
  - Specific part
  - Header

Packet analysis (3)

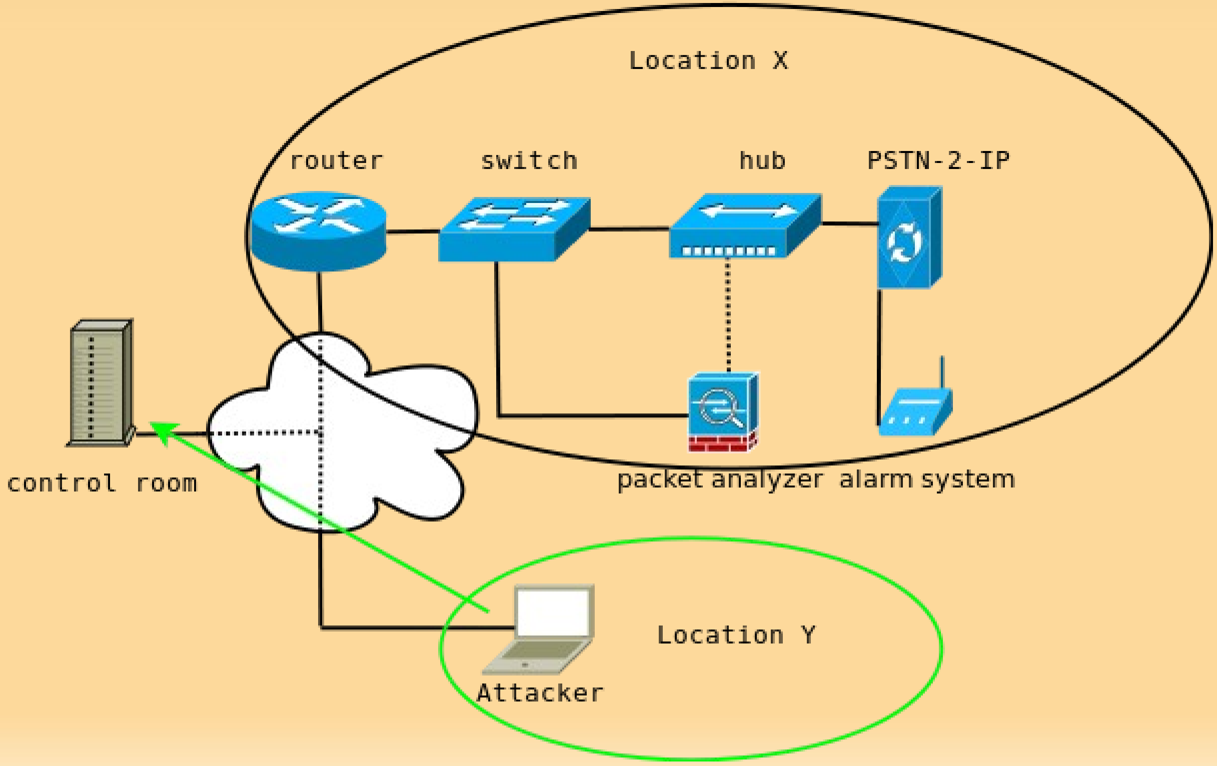
- Specific part
  - 4 bytes differ
- Encryption
  - Hex values compared to account code
  - XOR
  - Key = 0xB5
- UDP port number
  - Acknowlegdement of registration packet
  - Same encryption as account code

Packet analysis (4)

- Header
  - 2 bytes differ
- Must be account code
- Example encryption
  - Account code: 0011
  - Bytes: 0x00 and 0x11
  - XOR
  - Key = 0x85

Think as a burglar

- Activate alarm on location X, deactivate from location Y.
- Trigger alarms from different accounts.



Attack vectors

- Replay attack
  - Disable / enable alarm
  - Trigger alarm sensors
  - DoS (system and human)
- Brute force attack

Replay attack

- Capturing network traffic
- Working data sets
    - Disabling alarm
    - Triggering sensors

DoS attack

- Overloading control room with fake alarms
  - Impact on availability security guards
- Requirements
  - Data set from a real alarm
  - Port numbers
  - Account code
  - Checksum

Brute force attack

- Control room ”coorporates”
  - Static registration port used
- Account code + checksum = brute force
  - Account code: 4 digits(0-9) == 10.000 posibilities
  - Checksum: 1 byte == 256 posiblities
  - Total: 10000*256 = 2.560.000 posibilites
  - Total time needed:

    (2560000/2)/60/60/24) ≈ 15 days

Impact

- PSTN-2-IP sold by different security company's
  - Therefore PSTN-2-IP is actively used
- Newer systems available:
  - Strong encryption
  - Seperate vpn routers
  - QoS

Improvements

- Rewrite protocol
- Protection against replay attacks
- Improve confidentiality
  - Avoid replay attacks with account information
- Improve integrity
  - Avoid decrypting payload from packets
- Improve availability
  - Avoid DoS possibilities

Conclusions

”Is it possible to perform a burglary without getting noticed by influencing the communication between the alarm system and the control room?”

- Protocol vulnerable for replay attacks
- No advanced crypto is used
- DoS
- A burglar needs technical knowledge and resources.

On a side note

”It takes 1,5 hours before a line failure is detected by the control room”

Questions?

- Report soon available at:

  https://www.os3.nl/2009-2010/students/kevin_de_kok/rp1