Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Volume 21, No. 1, ISSN 1726-9679
ISBN 978-3-901509-73-5, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2010
Make Harmony Between Technology and Nature, and Your Mind will Fly Free as a Bird
DAAAM Symposium

BUILDING SAFE REALTIME CHANNEL FOR MOBILE TELEOPERATED ROBOTS

BURIAN, F[rantisek]; VESELY, M[ilos] & ZALUD, L[udek]

Abstract: *One of the main problems in secure wireless communication of mobile robots with operator stations is to maintain sufficient security to transmitted data. Real-time behavior of communication with unpredictable and uncorrectable packet losses due to signal fluctuations makes situation difficult. Current secure implementations of mobile robot protocols have some vulnerability that can help attacker to partially decode the stream. With this information attacker can broke the transmission keys. Novel variant of standard protocol that makes some specific attacks more difficult is described in this paper.*
Key words: *mobile robots, communication, cryptography, system security*

1. INTRODUCTION

Teleoperated mobile robots can be described as robots controlled remotely by human operator through communication link. On the operator's station the collected data (from joystick and controls) is packed into simple UDP datagrams, and sent through communication link to robot. The robot is controlled by this data. Status of the robot and video signal are collected and packed into the same stream and sent back to the operator's station using same UDP datagrams. Computer in operator's station decodes current robot data and shows it on the displays (see Fig. 1). This communication link shoul be ciphered.

2. COMMUNICATION DESCRIPTION

Real-time control of the robot is needed although link speed is very low. Any packet-negotiation in protocol must be avoided. Packet negotiation would cause unpredictible delays, dead lock and dangerous buffering. This buffering and delays are huge problem and operator would be unable to control the robot. No packet negotiation and bad reception would cause lower framerate and flickering of the video. Operator is able to deal with this situation. Therefore none of the negotiation schemes can be performed.

Real robotic applications have some specific properties (Solc & Zalud, 2000) (Zalud et al., 2009). The download from the robot consist video signal and is about ten times bigger then upload. Considering features and problems mentioned in previous paragraphs none of the comperession techniques that benefits from interframe prediction can be used.

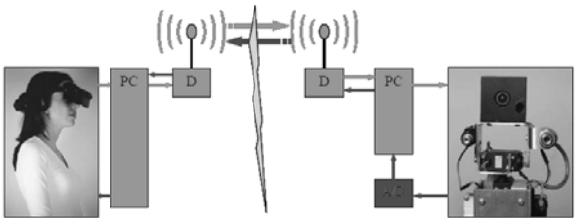

Fig. 1. Telepresently operated robot

In practical application, protocol in which one transmitted packet carries one JPEG compressed block of video stream is used. The packet loss will create blocky image, but image of the robot exterior remains on the screen.

The robot uses small, working boards with low computational power which comply with military standards. Because of this limitation these boards are unable to apply any high-level ciphering, which can achieve good security for all transmitted data. There must be done a compromise between computational requirement and system security.

The main problem in this scenario is that all packets have same structure and are sent unencrypted in simple static protocol. Using static data on same places creates potential risk of compromising the packet.

3. ADAPTED PROTOCOL DESCRIPTION

Communication strategy was described in previous paragraph. From this strategy, following constraints emerge:

- one packet cannot depend on another,
- loss of single packet must not break the stream,
- the key bit stream must be different for each packet (initialization vector),
- by experience the ciphering must not load the communication link more than 1%.

From those points we can conclude that simple stream cipher (Menezes et al., 1997) cannot be used for its simplicity. The AES cipher (Menezes et al., 1997) (Atasu, 2004) (Daemen & Rijmen, 2002) is too computing power consuming to be used on our robot's microcontroller system. One easy way how to overcome this problem is to use a symmetric Block cipher with some modifications. These are described in forthcomming sections.

3.1 Ciphering every packet

An easy way to do ciphering on each packet is to crypt every incoming data block in packet, and chain results in to output packet. This mode is well known as Cipher-block mode "CBC" described in (Knudsen, 2000). The main principle of encryption and decryption is shown in the Fig. 2 and Fig 3.

Each packet in this scenario must obtain different initialization vector (IV). The IV vector must be the same length as the encrypted block, and must be transferred in the channel. For example, for 256-bit blocks and 1500-byte packets sending IV will raise data communication by 2%. This additional load can be lowered by transmission of IV index into IV table instead of full length IV (see Fig. 2 and Fig. 3).

As can be seen from these figures, the initialization vector is transferred in unciphered format. It does not represent any security risk, it is a property of CBC ciphering scheme. Follow the Fig. 2: The IV vector for block 3 is previous ciphered block 2, which is visible in the link for the attacker. This means the IV table (and translation from IV index to table) doesn´t need to be secret (ciphered).

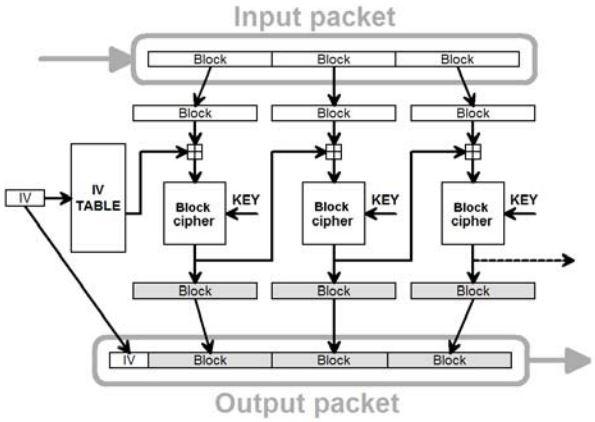

Fig. 2. Ciphering a packet

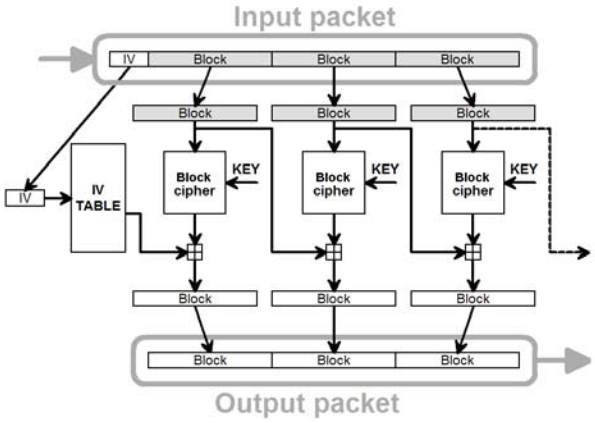

Fig. 3. Deciphering a packet

Security of the protocol is limited by IV repetition statistics and the initial guess of the attacker in original packet. The classical packet contains header in the first few bytes that controls the rest of the packet. The headers are statistically very similar, and are positioned on the same location in each packet. To make attacker's life more difficult, protocol must be designed for floating position of the header. In this situation, attacker can be confused by changing the entire message, and he/she cannot record more starts of header (SOH) in the same place.

3.2 Design of the protocol of the packet

As the previous chapter says, the protocol must be adapted to sustain maximum security of data. The protocol supposes that all transferred data is binary and compressed. This implies that data entropy of the packet is near to 1 Shannon/bit. This means, that data has small redundancy, and ciphering is very effective, due to small distance between two valid messages.

The first few bytes of the packet are obviously treated as a header. For the maximum security in the designed protocol, these bytes (called P) have been filled by a random number. The rest of this buffer is reserved to carry the data in the form of circular buffer (See Fig. 4).

We can define algorithm, which converts P into a number, identifying position of the starting point in data buffer (SOH). The algorithm can use modulus arithmetic, using some prime number as a base of division (for example 1493). Algorithm is mathematically described in equation 1:

$$SOH = (PK_1 + K_2)\ mod\ r \qquad (1)$$

On the transmitting side, there is no additional overhead except single modulus division and storing data to circular

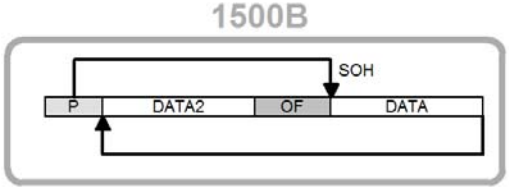

Fig. 4. Circular buffer with defined start of header (SOH)

buffer. It is fast and additional cryptographic processor is not needed. Plaintext data is never visible outside of the device on the bus. On the receiving side, there is same overhead as well as on the transmitting one.

On the attacker side, there are some garbage bytes on the beginning of packet. Stochastic analysis of those bytes over IV gives no results, because it is compressed random number. Stochastic analysis of any block over IV gives no result, because the data position changes inside every block. Stochastic analysis of entire packet gives no results because of different IV in every block (the CBC mode helps there). The only way to get the decoded data is to know the keying scheme and know the keys K1 and K2.

4. CONCLUSION

Current secure implementations of mobile robot protocols have some vulnerability that can help attacker to partially decode the stream and break the transmission keys.

In this article we described our mutation of standard protocol which makes some specific attacks more difficult. Proposed modification uses Block ciphering chained with CBC scheme and proprietary protocol with floating header position. Floating position is based on random number.

The designed communication scheme will be in the future used to securely transport data via unsafe link between mobile robot and operator's station.

5. ACKNOWLEDGEMENTS

This work has been supported in part by Ministry of Education, Youth and Sports of the Czech Republic (Research Intent MSM0021630529 Intelligent systems in automation), Grant Agency of the Czech Republic (102/09/H081 SYNERGY - Mobile Sensoric Systems and Network) and by Brno University of Technology. Without kind support of the above-mentioned agencies and institutions the presented research and development would not be possible.

6. REFERENCES

Atasu, K. (2004). Efficient aes implementations for arm based platforms, *In SAC 04: Proceedings of the 2004 ACM symposium on Applied computing*, 841-845, ACM Press

Daemen, J. & Rijmen, V. (2002). *The design of Rijndael: AES--the advanced encryption standard*, 3-540-42580-2, Springler-Verlag, New York

Knudsen, L.R. (2000). Block chaining modes of operation, *Report in Informatics*, 0333-3590, University of Bergen, Norway

Menezes, A. J.; Oorschot, P. C. V.; Vanstone, S. A. & Rivest, R. L. (1997). *Handbook of applied cryptography*, 0-8493-8523-7, CRC Press, New York.

Solc, F. & Zalud, L. (2000). *Utar - universal telepresence and autonomous robot*, 141-146, 80-214-1641-6, Brno university of technology, Faculty of Electrical Engineering

Zalud, L.; Kopecny, L. & Burian, F. (2009). Robotic systems for special reconnaissance, *ICMT09 International Conference on Military Technologies 2009*, 532-541, 978-80-7231-649-6, Akademie obrany