ACE Working Group
Internet Draft
Interned status: Standards Track
Expires: August 26, 2017

Q. Huang
M. Wei
H. Wang
S. Li
P. Wang
Y. Li
Chongqing University of
Posts and Telecommunications

February 22, 2017

Subliminal Channel Hiding Communication for Constrained-Node Networks
draft-huang-ace-hiding-communication-00

Abstract

Due to the computation and storage limitations of constrained-node networks, it is costly to apply those security mechanisms based on public key algorithm. This document proposed a subliminal channel hiding communication method, which can provide message authentication service and protect the transmission of the sensitive data.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on August 26, 2017.

Table of Contents

1. Introduction

In the existing networks, the processing of the sensitive data has mainly used a variety of encryption technologies, and the sensitive data is transmitted through the public channel. The attacker could easily detect the communication process, hence, the man-in-middle attack, the DoS attack or the Sybil attack can be applied to interfere the communication, which makes the legal receiver cannot obtain the encrypted sensitive data, and leads to the failure of the communication process eventually.

The subliminal channel hiding communication is to hide the sensitive data into the ordinary data. The attacker is hard to analyze whether there is any sensitive data in the ordinary data. In this way, the transmitted ordinary data would not cause attacker's attentions and doubts. The subliminal channel hiding communication decreased the

intercept rate of the sensitive data and guaranteed the security of the sensitive data fundamentally.

The traditional subliminal channel hiding communication is not suitable for the constrained-node networks due to its high computational overhead. Many existing subliminal channel communications are based on public key mechanisms, such as: Scheme of subliminal channel based on Schnorr digital signature and analysis, and the Subliminal Channel Protocol based on Elliptic Curve Digital Signature Algorithm, both of them hides the sensitive data into the digital signature by using embedding algorithm. Although the message authentication mechanism is introduced in the communication process, the asymmetric encryption technology is adopted in the existing embedding algorithm, which increases the calculation costs of the node, and makes the distribution of the public key and the private key very complex.

The purpose of this document is to solve the problems of low security and high energy consumption in constrained-node networks communication process. A subliminal channel hiding communication method based on Message Authentication Code (MAC) has been put forward. By using the data hiding technology, the confidentiality and integrity of the sensitive data can be protected, where the sensitive data is less vulnerable to be attacked in the communication process.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]

1.2. Terms Used

MAC: Message Authentication Code.

Ordinary data: The data is divided into different grades according to its importance, the ordinary data is low-grade.

Sensitive data: The data is divided into different grades according to its importance, the sensitive data is high-grade. Such as the key update messages, time synchronization messages, etc.

Broadcast packet: A 2-tuple packets contains the ordinary data and MAC.

Cluster head node: Resource-rich node with high computation and storage capacity.

Cluster node: Constrained node with constrained computation and storage capacity.

2. Subliminal Channel Hiding Communication

2.1. Overview of the scheme

There are two types of nodes in this document, the cluster head node which is a resource-rich node, and the cluster node which is a constrained-node. The topology of the network is shown in Figure 1. Node A is cluster head node, node B, C and N etc. are cluster nodes.

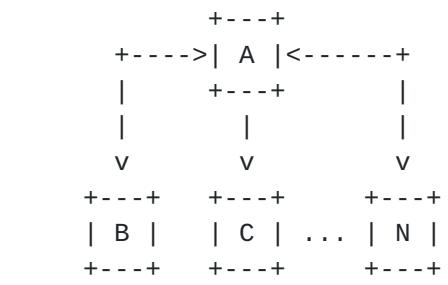

Figure 1. The network topology

There is a trust third party with high computation and storage capacity in the network used to distribute the key materials and other necessary materials to the cluster head node and the cluster nodes at the initialization phase. The mode of the third party is shown in Figure 2.

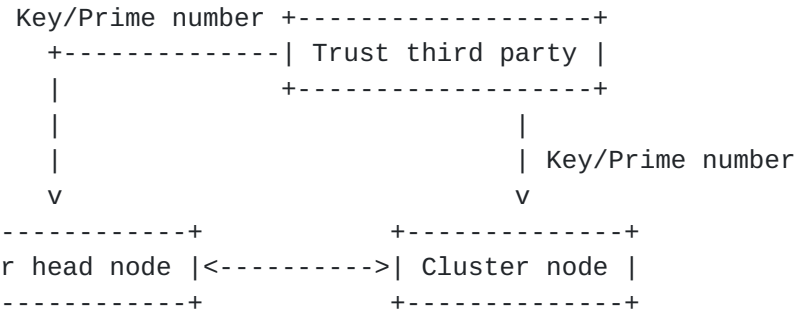

Figure 2. The third-party mode

The cluster head node hides the sensitive data into MAC and constructs a broadcast packet by using Chinese Remainder Theorem (CRT). Then the cluster head node sends the broadcast packet to the

cluster nodes. While the cluster nodes receive the broadcast packet it SHOULD have the message authenticated before, and then it can extract the sensitive data from the MAC if the message is certified. The attacker cannot know whether the MAC contains a sensitive data and cannot get any data from the MAC. This method increased the difficulty of decoding the sensitive data.

2.2. The implementation of the scheme

The communication process is divided into several steps: (1) Initialization phase; (2) Preprocessing phase; (3) Constructing broadcast packets; (4) Message authentication; (5) Recovering the sensitive data.

(1) Initialization phase: In order to realize authentication and information hiding, the trust third party needs to generate the key parameters. The trust third party generates a key k shared by the whole network nodes, and a series keysrespectively shared by the cluster nodes and the cluster head node. The trust third party also generates a large prime number m shared by the whole network nodes, and a series of large prime numberrespectively shared by the cluster node and the cluster head nodes.

(2) Preprocessing phase: when the cluster head node broadcasts the ordinary data v, it utilizes hash algorithm and key k to generate a preprocessed data b.

If the cluster head node wants to send a sensitive data u to the cluster node A, it utilizes the individual key KA and the identity of the receiving node A through a symmetric encryption algorithm to generate an encrypted sensitive data U.

(3) Constructing broadcast packets phase: the cluster head node utilizes the preprocessed data b, the prime number m, the encrypted sensitive data U and the prime number mA which is shared by the cluster node A and the cluster head node to calculate the congruence equation according to the Chinese Remainder Theorem algorithm.

The cluster head node calculates the solution of the congruence equation as the MAC which is embedded the sensitive data. Then the cluster head node constructs a 2-tuple packets P and broadcasts to the cluster nodes.

(4) Message authentication phase: when the cluster node A received the 2-tuple packets P, it SHOULD first authenticate the packet. If

the packet P is certified, which means the packet p is credible; otherwise, it will discard the packet.

(5) Recovering the sensitive data phase: If the packet P passed the verification, the cluster node A will calculate the encrypted sensitive data U by using its prime number mA from the MAC, then it uses key KA to decrypt the data U, and finally obtains the sensitive data u.

3. Security Considerations

TBD.

4. IANA Considerations

This memo includes no request to IANA.

5. References

5.1. Normative References

5.2. Informative References

[RFC2119]
Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119,DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7228]
Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228,DOI 10.17487/RFC7228, May 2014, <http://www.rfc-editor.org/info/rfc7228>.

Authors' Addresses

QingQing Huang
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: huangqq@cqupt.edu.cn

Min Wei
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: weimin@cqupt.edu.cn

Hao Wang
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: wanghao@cqupt.edu.cn

Shuaiyong Li
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: lishuaiyong@cqupt.edu.cn

Ping Wang
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road

Chongqing, 400065
China

Phone: (86)-23-6246-1061
Email: wangping@cqupt.edu.cn

Yong Li
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: 13101279737@126.com