Internet Engineering Task Force (IETF)
Request for Comments: 6813
Category: Informational
ISSN: 2070-1721
J. Salowey
Cisco Systems
S. Hanna
Juniper Networks
December 2012

The Network Endpoint Assessment (NEA) Asokan Attack Analysis

Abstract

The Network Endpoint Assessment (NEA) protocols are subject to a subtle forwarding attack that has become known as the NEA Asokan Attack. This document describes the attack and countermeasures that may be mounted.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Network Endpoint Assessment (NEA) [2] protocols are subject to a subtle forwarding attack that has become known as the NEA Asokan Attack. This document describes the attack and countermeasures that may be mounted. The Posture Transport (PT) protocols developed by the NEA working group, PT-TLS [5] and PT-EAP [6], include mechanisms that can provide cryptographic-binding and identity-binding countermeasures.

2. NEA Asokan Attack Explained

The NEA Asokan Attack is a variation on an attack described in a 2002 paper written by Asokan, Niemi, and Nyberg [1]. Figure 1 depicts one version of the original Asokan attack. This attack involves tricking an authorized user into authenticating to a decoy Authentication, Authorization, and Accounting (AAA) server, which forwards the authentication protocol from one tunnel to another, tricking the real AAA server into believing these messages originated from the attacker-controlled machine. As a result, the real AAA server grants access to the attacker-controlled machine.

```
                         +-------------+ ========== +----------+
                         |   Attacker  |-AuthProto--|AAA Server|
                         +-------------+ ========== +----------+
                                |
                            AuthProto
                                |
+--------------+ ========== +----------------+
|AuthorizedUser|-AuthProto--|Decoy AAA Server|
+--------------+ ========== +----------------+
```

Figure 1: One Example of Original Asokan Attack

As described in the NEA Overview [2], the NEA Reference Model is composed of several nested protocols. The Posture Attribute (PA) protocol is nested in the Posture Broker (PB) protocol, which is nested in the PT protocol. When used together successfully, these protocols allow an NEA Server to assess the security posture of an endpoint. The NEA Server may use this information to decide whether network access should be granted, or it may use this information for other purposes.

Figure 2 illustrates an NEA Asokan Attack. The attacker wants to trick GoodServer into believing that DirtyEndpoint has good security posture. This might allow, for example, the attacker to bring an infected machine onto a network and infect others. To accomplish this goal, the attacker forwards PA messages from CleanEndpoint through BadServer to DirtyEndpoint, which sends them on to GoodServer. GoodServer is tricked into thinking that the PA messages came from DirtyEndpoint and therefore considers DirtyEndpoint to be clean.

```
                         +-------------+ ========== +----------+
                         |DirtyEndpoint|-----PA-----|GoodServer|
                         +-------------+ ========== +----------+
                                |
                               PA
                                |
+-------------+ ========== +---------+
|CleanEndpoint|-----PA-----|BadServer|
+-------------+ ========== +---------+
```

Figure 2: NEA Asokan Attack

Countermeasures against an NEA Asokan Attack are described in Section 4.

3. Lying Endpoints

Some may argue that there are other attacks against NEA systems that are simpler than the Asokan attack, such as lying endpoint attacks. That is true. It's easy for an endpoint to simply lie about its posture. But, there are defenses against lying endpoint attacks, such as using an External Measurement Agent (EMA).

An EMA is hardware, software, or firmware that is especially secure, hard to compromise, and designed to accurately report on endpoint configuration. The EMA observes and reports on critical aspects of endpoint posture, such as which security-relevant firmware and software have been loaded.

When an EMA is used for NEA, the PA messages that reliably and securely establish endpoint posture are exchanged between the EMA itself and a Posture Validator on the NEA Server. The Posture Collector on the endpoint and any other intermediaries between the EMA and the Posture Validator on the NEA Server are not trusted. They just pass messages along as untrusted intermediaries.

To ensure that the EMA's messages are accurately conveyed to the Posture Validator, even if the Posture Collector or other intermediaries have been compromised, these PA messages must provide integrity protection, replay protection, and source authentication between the EMA and the Posture Validator. Confidentiality protection is not needed, at least with respect to the software on the endpoint, but integrity protection should include protection against message deletion and session truncation. Organizations that have developed EMAs have typically developed remote attestation protocols that provide these properties (e.g., the Trusted Computing Group's (TCG's) Platform Trust Service (PTS) Protocol Binding to IF-M [7]). While the development of lying endpoint detection technologies is out of scope for NEA, these technologies must be supported by the NEA protocols. Therefore, the NEA protocols must support countermeasures against the NEA Asokan Attack.

4. Countermeasures against the NEA Asokan Attack

4.1. Identity Binding

One way to mitigate the Asokan attack is to bind the identities used in tunnel establishment into a cryptographic exchange at the PA layer. While this can go a long way to preventing the attack, it does not bind the exchange to a specific TLS exchange, which is desirable. In addition, there is no standard way to extract an identity from a TLS session, which could make implementation difficult.

4.2. Cryptographic Binding

Another way to thwart the NEA Asokan Attack is for the PA exchange to be cryptographically bound to the PT exchange and to any keying material or privileges granted as a result of these two exchanges. This allows the NEA Server to ensure that the PA messages pertain to the same endpoint as the party terminating the PT exchange and that no other party gains any access or advantage from this exchange.

4.2.1. Binding Options

This section discusses binding protocol solution options and provides analysis. Since PT-TLS and PT-EAP involve TLS, this document focuses on TLS-based solutions that can work with either transport.

4.2.1.1. Information from the TLS Tunnel

The TLS handshake establishes a cryptographic state between the TLS client and TLS server. There are several mechanisms that can be used to export information derived from this state. The client and server independently include this information in calculations to bind the instance of the tunnel into the PA protocol.

Keying Material Export - RFC 5705 [8] defines Keying Material Exporters for TLS that allow additional secret key material to be extracted from the TLS master secret.

tls-unique Channel Binding Data - RFC 5929 [9] defines several quantities that can be extracted from the TLS session to bind the TLS session to other protocols. The tls-unique binding consists of data extracted from the TLS handshake finished message.

4.2.1.2. TLS Cipher Suites

In order to eliminate the possibility of a man-in-the-middle attack and thwart the Asokan attack when using the keying material export binding export mechanism, it is important that neither TLS endpoint be in sole control of the TLS pre-master secret. Cipher suites based on key transport, such as RSA cipher suites, do not meet this requirement; instead, Diffie-Hellman Cipher Suites, such as RSA-DHE, are required when this mechanism is employed.

4.2.1.3. Using Additional Key Material from TLS

In some cases, key material is extracted from the TLS tunnel and used to derive ciphering keys used in another protocol. For example, EAP-TLS [10] uses key material extracted from TLS in lower-layer ciphering. In this case, the extracted keys must not be under the control of a single party, so the considerations in the previous section are important.

4.2.1.4. EMA Assumptions

The EMA needs to obtain the binding data from the TLS exchange and prove knowledge of the binding data in an exchange that has integrity protection, source authentication, and replay protection.

5. Conclusions

The recommendations for addressing the NEA Asokan Attack are as follows:

1. Protocols should make use of cryptographic binding; in addition, binding identities of the tunnel endpoints in the EMA may be useful.

2. In particular, L2 and L3 TLS-based PT transports (e.g., PT-TLS and PT-EAP) should use the same cryptographic binding mechanism.

3. The preferred approach is to use the tls-unique channel binding data from [9]. The tls-unique value will be made available to the EMA that will use it. This approach can utilize any TLS cipher suite based on a strong cipher algorithm.

6. Security Considerations

This document is primarily concerned with analyzing and proposing countermeasures for the NEA Asokan Attack. That does not mean that it covers all the possible attacks against the NEA protocols or against the NEA Reference Model. For a broader security analysis, see the Security Considerations section of the NEA Overview [2], PA-TNC [3], PB-TNC [4], PT-TLS [5], and PT-EAP [6].

7. Informative References

[1] Asokan, N., Niemi, V., and K. Nyberg, "Man-in-the-Middle Attacks in Tunneled Authentication Protocols", Nokia Research Center, Finland, Nov. 11, 2002, http://eprint.iacr.org/2002/163.pdf.

[2] Sangster, P., Khosravi, H., Mani, M., Narayan, K., and J. Tardo, "Network Endpoint Assessment (NEA): Overview and Requirements", RFC 5209, June 2008.

[3] Sangster, P. and K. Narayan, "PA-TNC: A Posture Attribute (PA) Protocol Compatible with Trusted Network Connect (TNC)", RFC 5792, March 2010.

[4] Sahita, R., Hanna, S., Hurst, R., and K. Narayan, "PB-TNC: A Posture Broker (PB) Protocol Compatible with Trusted Network Connect (TNC)", RFC 5793, March 2010.

[5] Sangster, P., N. Cam-Winget, and J. Salowey, "PT-TLS: A TCP-based Posture Transport (PT) Protocol", Work in Progress, October 2012.

[6] Cam-Winget, N. and P. Sangster, "PT-EAP: Posture Transport (PT) Protocol For EAP Tunnel Methods", Work in Progress, July 2012.

[7] Trusted Computing Group, "TCG Attestation PTS Protocol: Binding to TNC IF-M", Version 1.0, Revision 27, August 2011.

[8] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", RFC 5705, March 2010.

[9] Altman, J., Williams, N., and L. Zhu, "Channel Bindings for TLS", RFC 5929, July 2010.

[10] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, March 2008.

8. Acknowledgments

The members of the NEA Asokan Design Team were critical to the development of this document: Nancy Cam-Winget, Steve Hanna, Joe Salowey, and Paul Sangster.

The authors would also like to recognize N. Asokan, Valtteri Niemi, and Kaisa Nyberg who published the original paper on this type of attack and Pasi Eronen who extended this attack to NEA protocols.

Authors' Addresses

Joseph Salowey
Cisco Systems, Inc.
2901 3rd. Ave
Seattle, WA 98121
USA
EMail: jsalowey@cisco.com

Steve Hanna
Juniper Networks, Inc.
79 Parsons Street
Brighton, MA 02135
USA
EMail: shanna@juniper.net