Network Working Group   J. Salowey
Internet Draft   Cisco Systems
Intended status: Informational   S. Hanna
Expires: April 2011   Juniper Networks
                                                     October 18, 2010

                        NEA Asokan Attack Analysis
                      draft-salowey-nea-asokan-00.txt

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 April 18, 2011.

Copyright Notice

Abstract

   The Network Endpoint Assessment 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.

Table of Contents

1. Introduction

   The Network Endpoint Assessment 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.

   This document is not intended to formally define a protocol but
   rather to explore the options for countering the Asokan attack. The
   NEA WG is expected to consider these options, decide which to
   select, and incorporate specific text defining that option into a
   Standards Track document. Then this document will be allowed to
   expire.

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
AAA server, which forwards the authentication protocol from one
tunnel to another, tricking a AAA server into believing these
messages came from the attacker and granting access to him.

```
                        +-------------+ ========= +----------+
                        |   Attacker  |-AuthProto--|AAA Server|
                        +-------------+ ========= +----------+
                              |
                          AuthProto
                              |
+--------------+ ========= +----------------+
|AuthorizedUser|-AuthProto--|Decoy AAA Server|
+--------------+ ========= +----------------+
```
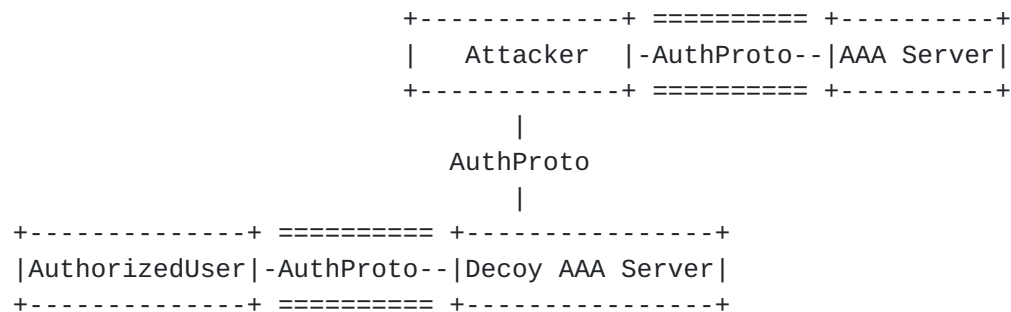
        Figure 1: One Example of Original Asokan Attack

As described in the NEA Overview [2], the NEA Reference Model is
composed of several nested protocols. The PA protocol is nested in
the PB protocol, which is nested in the PT protocol. When used
together successfully, these protocols allow a 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
for other purposes.

Figure 2 illustrates a NEA Asokan Attack. The attacker wants to
trick GoodServer into believing that DirtyEndpoint has good security
posture. This might allow the attacker to bring an infected machine
onto a network and infect others, for example. 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
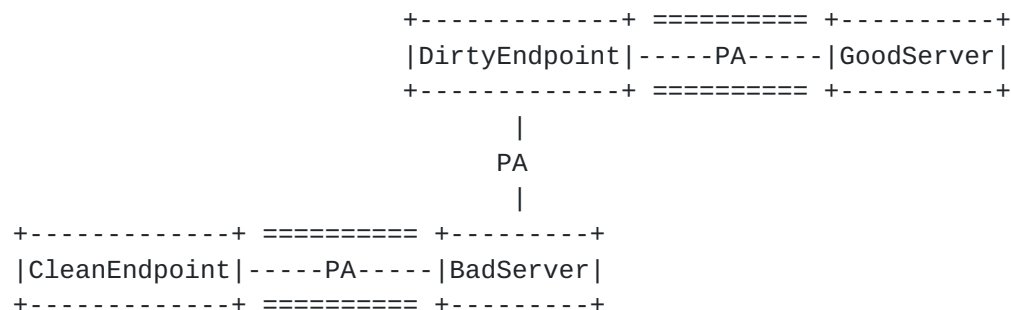DirtyEndpoint and therefore considers DirtyEndpoint to be clean.

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

        Figure 2: NEA Asokan Attack

Countermeasures against a 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 designed to accurately report on endpoint configuration but be especially secure and hard to compromise. The EMA observes and reports on critical aspects of endpoint posture such as which security-relevant firmware and software has 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. While the development of lying endpoint detection technologies is out of scope for NEA, these technologies must be supported by the NEA protocols.

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

   One 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 the proposals for both L2 and L3 PT
   involve TLS the 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 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 [5] 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 [6] 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 and
   thwart the Asokan attack 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 [7] 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 Asokan attack are as follows:

1. Make use of cryptographic binding, however binding identities of
   the tunnel endpoints in the EMA may be useful.
2. The same mechanism be used in L2 and L3 PT transports that make
   use of TLS.
3. Neither TLS endpoint can be in sole control of the TLS pre-master
   secret.
4. The preferred approach is to use secret key material exported from
   the TLS handshake using the mechanism defined in RFC 5705. The
   key material is exported using a standardized label and made
   available to the EMA that will use it.

6. IANA Considerations

This document has no actions for IANA.

7. 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], and PB-TNC [4].

8. References

8.1. Informative References

[1]   N. Asokan, Valtteri Niemi, Kaisa 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]   Rescorla, E., "Keying Material Exporters for Transport Layer
        Security (TLS)", RFC 5705, March 2010.

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

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

9. Acknowledgments

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