

# Security analysis of the Digital Transmission Copy Protection Specification

**Haibo Tian**

National Key Lab. on ISN  
Xidian University  
Xi'an, China

**Yumin Wang**

National Key Lab. on ISN  
Xidian University  
Xi'an, China

**Abstract** - This paper analyzes the secure protocols in the digital transmission copy protection (DTCP) specification. The full authentication protocol in the specification is a combination of the Diffie-Hellman (DH) key exchange algorithm and the digital signature technique. It is claimed that the protocol can prevent “man in the middle” attacks. However, we can apply at least three classical attacks to the protocol. All of them can overthrow the authentication objective. Further, a sender or receiver mismatching is discovered. The receiver mismatching threatens the system integrity property of the DTCP specification.

**Keywords:** DTCP; secure protocols; image communication; digital right management.

## 1 Introduction

The digital transmission content protection (DTCP) specification defines a cryptographic protocol for protecting entertainment content from unauthorized copying, intercepting, and tampering as it traverses digital transmission mechanisms such as a high-performance serial bus that conforms to the IEEE 1394-1995 standard [1]. Authenticated key exchange is a main component of the specification. Two authentication levels are defined, namely full authentication and restricted authentication. The full authentication is expected to be a more secure method for a connected device to verify that another connected device is authentic. Since the full authentication employs the digital signature technique and DH key exchange algorithm, it is claimed that “the DH algorithm is considered secure when combined with digital signatures to prevent a so-called ‘man-in-the-middle’ attack” in the white paper of the DTCP specification [2]. The device authentication is described as “mutual between source and sink” when the DTCP specification is discussed in [3]. A brief description of the specification [4] says that “the source device and the sink device authenticate each other, and establish shared secrets.”

However, we show that when a source or sink device completes an execution of the full authentication, the device can not confirm the identity of the counterpart. Hence the mutual authentication claim is failed. A further analysis shows that there is sender or receiver mismatching

even in the content transmission phase. The receiver mismatching threatens the system integrity property, which is one of the three main design goals of the DTCP specification.

## 2 The Full Authentication

We first review the full authentication protocol briefly. The protocol employs a signature algorithm and a DH (Diffie-Hellman) key exchange algorithm. The signature algorithm is a method for digitally signing and verifying the signatures of digital content to verify the integrity of the data. The DH key exchange is used during full authentication to establish control channel symmetric cipher keys, allowing two or more parties to generate a shared key.

1.  $A \xleftarrow{r_B, Cert_B} B$
2.  $A \xrightarrow{r_A, Cert_A} B$
- 3.1  $A \xleftarrow{yG, Text_B, Sig_B(r_A, yG, Text_B)} B$
- 3.2  $A \xrightarrow{xG, Text_A, Sig_A(r_B, xG, Text_A)} B$

Fig. 1. The full authentication protocol in the DTCP specification

As shown in Fig.1, the full authentication protocol consists of two roles: a source device A and a sink device B. At first, the device B initiates the full authentication, and sends a random challenge  $r_B$  and its device certificate  $Cert_B$  to the device A. Secondly, the device A returns a random challenge  $r_A$  and its device certificate  $Cert_A$  to the device B. After the random challenge and device certificate exchange, each device verifies the integrity and revocation status of the other device’s certificate, and then calculates a DH first-phase value. Then the sink device B sends its DH key  $yG$ , the renewability message version number and generation of the system renewability message  $Text_B$ , and a message signature containing the other device’s random challenge  $r_A$  concatenated to the preceding components. At the same time, the device A sends its  $xG$ ,  $Text_A$  and a message signature to the device B. After the DH key and signature exchange, each device verifies the received

signature. If the verification is successful, each device computes an authentication key used for a key derivation procedure.

### 3 Classical Attacks

We consider “man in the middle” attacks. A malice device M is assumed to exist between two honest devices logically. The device M can intercept, modify, and insert messages in a serial bus linked network. The device may be a modified normal device, which enjoys some powerful but not good features. Considering such an attacker, there are at least three classical attacks against the full authentication. The three attacks can be found in many literatures, and are documented in the chapter eleven of reference [5]. The first one is called reflection attack. The reflection attack uses the message symmetric property of the full authentication. The second is Wiener’s attack. This attack comes from the lack of sender’s random challenge in the signatures. The third attack is Lowe’s attack. The attack is workable because there is no identity in the signatures. These all attacks cause authentication failure, which differs from the common knowledge about the DTCP specification.

#### 3.1 Reflection Attack

Suppose a malice device M. The device intercepts messages sent by a legitimate sink device, says B, and replays these messages directly to the device.

$$\begin{aligned}
1. & M \leftarrow \frac{r_B, Cert_B}{B} \\
2. & M \xrightarrow{r_B, Cert_B} B \\
3.1 & M \leftarrow \frac{yG, Text_B, Sig_B(r_A, yG, Text_B)}{B} \\
3.2 & M \xrightarrow{yG, Text_B, Sig_B(r_A, yG, Text_B)} B
\end{aligned}$$

Fig. 2. Applying the reflection attack to the full authentication protocol

Since the device B’s certificate is licensed, the certificate checked by B is a good certificate. Since B’s signature is created legitimately, when device B uses the public key in the received certificate to verify the received signature, the verification procedure will report that the signature is good. When the device B completes the full authentication, it believes that it is talking with another device B and shares an agreed key with that device. However, device B only serves as an initiator, and there is no legitimate responder.

This attack shows that it is important for a device to check the communication peer’s random number with the device’s local random number. If a sink device checks whether the random number in the received message is the same as its local random number, the reflection attack will not work. The effect of the attack is authentication failure. The following communication does not exist since no

source device appears and the device M does not know the agreed key of the sink device. The entertainment content remains secure.

#### 3.2 Wiener’s Attack

Suppose that a malice device M has obtained certificates of two legitimate devices B and C by eavesdropping. Then the device M initiates a run with a source device A, and initiates a run with another source device B.

$$\begin{aligned}
1.1 & M(B) \xrightarrow{r_M, Cert_B} A \\
1.2 & A \xrightarrow{r_A, Cert_A} M(B) \\
2.1 & M(C) \xrightarrow{r_A, Cert_C} B \\
2.2 & B \xrightarrow{r_B, Cert_B} M(C) \\
2.3.1 & B \xrightarrow{yG, Text_B, Sig_B(r_A, yG, Text_B)} M(C) \\
1.3.1 & M(B) \xrightarrow{yG, Text_B, Sig_B(r_A, yG, Text_B)} A \\
1.3.2 & A \xrightarrow{xG, Text_A, Sig_A(r_M, xG, Text_A)} M(B)
\end{aligned}$$

Fig. 3. Applying the Wiener’s attack to the full authentication protocol

In the first run, the device M sends a random value  $r_M$  and the device B’s certificate to the device A. When the device A replies with a random value  $r_A$  and its certificate, the device M uses the device C’s certificate and the device A’s random value to initiate the second run with another source device B. The device B replies with its certificate and a random value  $r_B$ . The device B will then be voluntary to send the last message since there is no sequence relation between the last two messages in the full authentication. When the device M receives the last message, the device M sends this message to the device A. Then the device A replies with a message in step 1.3.2 and completes the full authentication. The result is that the device A believes that the device B initiates this run and that it shares an agreed key with the device B. However, the device B has never initiated such a run, and it is waiting for the device C’s last message.

The attack shows the importance of including one device’s own random challenge in its signature. If the signature in step 2.3 contains the random challenge of the device B, the device M can not directly replay the message without detection. The effect of the attack is authentication failure. The following communication does not exist since no sink device appears and the device M does not know the agreed key of the device A. The entertainment content remains secure.

### 3.3 Lowe's attack

Suppose a device M. The device has a licensed certificate. Then the device can use a source device A as an oracle to cheat a sink device B.

$$\begin{aligned}
 1.1 \quad & B \xrightarrow{r_B, Cert_B} M(A) \\
 2.1 \quad & M \xrightarrow{r_B, Cert_M} A \\
 2.2 \quad & A \xrightarrow{r_A, Cert_A} M \\
 1.2 \quad & M(A) \xrightarrow{r_A, Cert_A} B \\
 1.3.1 \quad & B \xrightarrow{y_B G, Text_B, Sig_B(r_A, y_B G, Text_B)} M(A) \\
 2.3.1 \quad & M \xrightarrow{y_M G, Text_B, Sig_M(r_A, y_M G, Text_B)} A \\
 2.3.2 \quad & A \xrightarrow{xG, Text_A, Sig_A(r_B, xG, Text_A)} M \\
 1.3.2 \quad & M(A) \xrightarrow{xG, Text_A, Sig_A(r_B, xG, Text_A)} B
 \end{aligned}$$

Fig. 4. Applying the Lowe's attack to the full authentication

When a sink device B initiates the first run with a source device A, the device M intercepts the first message  $r_B$ ,  $Cert_B$ , and replaces  $Cert_B$  by M's certificate  $Cert_M$ . The replaced message is sent to the source device A in the second run. The response message of A is replayed directly to the sink device B. The device M then intercepts the device B's last message, and replaces the device B's DH key  $y_B G$  and the signature of B by its own DH key  $y_M G$  and the signature of M. The device A's last message is replayed directly to the device B. Now the device A and B complete the full authentication. The device B believes that it is talking with the device A and that it shares an agreed key with A. However the device A believes that it is talking with the device M and that it shares an agreed key with M.

The attack shows the importance of including the communicating peer's identity in one device's signature. If the signature in step 2.3.2 contains the identity of the device M, the device M can not directly replay the message to the device B without detection. The effect of the attack is authentication failure of the device B. Since the agreed key of the device B is not the same as that of the device A, there is no content transmission phase between the device A and the device B.

Similarly, the device M can use the device B as an oracle to cheat the device A. The result is that the device A believes that it is talking with the device B and that it shares an agreed key with B, whereas the device B believes that it is talking with the device M and that it shares an agreed key with M. The effect of the attack is authentication failure of the device A. When the device A continues to send entertainment content, there is no device which can receive it.

## 4 Mismatching

Attacks in the section 3 cause authentication failure, which identifies the vulnerability of the DTCP specification. But none of them threat the entertainment content transmission phase. In this section, a sender or receiver mismatching is identified, which does affect the content transmission phase. While the sender mismatching only has potential limitation to the applicable scenarios of the DTCP specification, the receiver mismatching directly threatens the system integrity property.

### 4.1 The attack

A receiver mismatching is presented in Fig.5.

$$\begin{aligned}
 1.1 \quad & B \xrightarrow{r_B, Cert_B} M(A) \\
 2.1 \quad & M \xrightarrow{r_B, Cert_M} A \\
 2.2 \quad & A \xrightarrow{r_A, Cert_A} M \\
 1.2 \quad & M(A) \xrightarrow{r_A, Cert_A} B \\
 1.3.1 \quad & B \xrightarrow{y_B G, Text_B, Sig_B(r_A, y_B G, Text_B)} M(A) \\
 2.3.1 \quad & M \xrightarrow{y_M G, Text_B, Sig_M(r_A, y_B G, Text_B)} A \\
 2.3.2 \quad & A \xrightarrow{xG, Text_A, Sig_A(r_B, xG, Text_A)} M \\
 1.3.2 \quad & M(A) \xrightarrow{xG, Text_A, Sig_A(r_B, xG, Text_A)} B
 \end{aligned}$$

Fig. 5. The receiver mismatching attack

This attack differs from the Lowe's attack in the step 2.3.1. The signature content of step 2.3.1 is  $y_B G$  instead of  $y_M G$ . After this replacement, the attack result is different. When the device A and B complete the full authentication, the device A indeed shares an agreed key with the device B. If the device M continue to replay directly all messages between the device A and the device B, the device B can receive the entertainment content from A. The device A believes that it is sending entertainment content to the device M, whereas the device A is sending the content to the device B. We call this attack as receiver mismatching.

Similarly, there is a corresponding sender mismatching, i.e. a sink device B believes that it is receiving entertainment content from the device M, whereas it is receiving the content from a source device A. This happens when the device M uses the device B as an oracle to cheat the device A, and signs the DH public key of device A directly.

### 4.2 The effect of the attack

We explain the effect of the receiver mismatching and the sender mismatching attack to the DTCP specification. The first is the effect of the receiver mismatching attack.

According to the DTCP specification, after the full authentication and key exchange, a system renewability procedure is executed. The main function of the renewability procedure is to update the SRMs (system renewability messages) of a device. The main content in the SRM is the CRL (certificate revocation list), where identities of unauthorized devices are included. Before content transmission, a device should check the latest SRM to exclude unauthorized devices. In this way, the high quality entertainment content will be transmitted and stored only in authorized device, and the long term integrity of the system is guaranteed. This integrity property is one of the three design goals of the DTCP specification.

But now, the malice device M can make any revoked devices receive high quality entertainment contents again. Suppose that the device M has a licensed certificate, which is a modified normal device. Suppose a sink device B that has been revoked. As a specially designed device, the device M will not check the revocation status of the device B. The device M executes the receiver mismatching attack. Then the device M replays all messages between the device B and the device A. Now the revoked device B can receive the protected entertainment content. Hence, there is a malice device M which can renew any revoked devices. This status illustrates a threat to the system integrity of the DTCP specification technically.

The effect of the sender mismatching is not so directly, but is related to some application scenarios. Suppose that the sender's identity is crucial for a receiver to deal with the fee of receiving the high quality entertainment content. Then the sender mismatching attack may provide a way for an attacker to collect filthy lucre. So the sender mismatching is a potential limitation to the application scenarios of the DTCP specification.

## 5 Conclusion

We have presented three classical attacks. Each attack shows a design weakness of the full authentication protocol. The mismatching attacks are identified, and the effect of this attack is analyzed. The weaknesses of DTCP, especially the mismatching attacks, urge a technical improvement of the DTCP specification.

## 6 References

- [1] 5C. Digital transmission content protection specification volume 1 (Informational version). Revision 1.4, 2005.2, Available: <http://www.dtcp.com>.
- [2] 5C. Digital transmission content protection white paper. Revision 1.0, 1998.7, <http://www.dtcp.com>.
- [3] Eugene T. Lin, Ahmet M. Eskicioglu, Reginald L. Lagendijk, and Edward J. Delp. Advances in digital video

content protection. Proceedings of the IEEE. 2005, Vol. (93): 171-183.

[4] A. M. Eskicioglu, J. Town, E. J. Delp. Security of digital entertainment content from creation to consumption. Elsevier Signal Processing: Image Communication, 2003, vol.(18): 237-262.

[5] Wen B. Mao. Modern Cryptography: Theory and Practice. NJ: Prentice Hall PTR, 2003. Nobel Laureate, His book, Publisher, Location, Year.