Response to "Nit-Picking PLAID AS & ISO Project Editors Report into 'Unpicking Plaid' "

Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni,
Felix Günther, Giorgia Azzurra Marson, Arno Mittelbach, and Kenneth G. Paterson

Information Security Group, Royal Holloway, University of London, U.K.
Cryptoplexity, Technische Universität Darmstadt, Germany
{j.p.degabriele,kenny.paterson}@rhul.ac.uk, marc.fischlin@cryptoplexity.de,
{victoria.fehr,tommaso.gagliardoni,giorgia.marson,arno.mittelbach}@cased.de,
guenther@cs.tu-darmstadt.de

December 8, 2014

Abstract

This is a response to the document "Nit-Picking PLAID AS & ISO Project Editors Report into 'Unpicking Plaid' " [Fre14] on our paper "Unpicking PLAID – A Cryptographic Analysis of an ISO-standards-track Authentication Protocol" [DFF+14a, DFF+14b]. The project editor's report claims to reveal errors in our "Unpicking PLAID" paper that render the described attacks both mute and easily preventable. It also claims to identify mis-definitions and made-up privacy notions. This response expresses our viewpoint on that report, rectifying some misrepresented facts and countering false allegations.

1 General Remarks

The project editor's report often refers to the Australian standard AS 5185-2010 from 2010 [Aus10]. As stated clearly in Section 2 of our paper [DFF+14a, DFF+14b] we mainly refer to the ISO/IEC DIS 25185-1.2 version from 2014 [ISO14] and consulted other documents when appropriate. For us, this seems to be the logical choice when it comes to ISO standardization.

One of the important aspects of our work is to point out that one should have supporting evidence of the security of a protocol, and that the mere lack of known attacks is a dangerous path. This is why we also stress that some of the potential countermeasures we propose in our paper need to be checked thoroughly, before they should be considered for adoption.

2 On Section 4 ("History")

While the analyses by Watanabe [Wat13] and Sakurada [Sak13] in some sense confirm authentication and key secrecy properties of PLAID under the assumption of idealized cryptographic primitives, we—as already discussed in our paper—disagree with considering them as "cryptographic proofs" as the project editor's report does. In particular, these analyses do not consider privacy aspects.

3 On Section 6 ("Response to 'Unpicking PLAID', Primary attack.")

The project editor's report claims in Section 6.1 that the ShillKey fingerprinting attack from our paper can be easily prevented without changing the standard since

> "[t]he primary attack is against the 2010 version of the Reference Implementation that was written for the Australian Standard AS 5185-2010."

Let us stress again that our attack is based on the description of the ShillKey and its usage according to the ISO standard [ISO14].

We believe that a security-related standard should not introduce potential attack vectors by being ambiguous and leaving such important issues to developers. In contrast, the project editor's report further states in Section 6.1:

> "[A]ny change required to eliminate the attack (if desired) is solely up to the implementer/developer, since any implementation of ShillKey is interoperable with any other and the Standards are actually mute on how ShillKey is implemented and consequently how it is implemented is not an issue."

On this reading, an implementation could be correct according to the ISO standard, but vulnerable to the ShillKey fingerprinting attack from our paper.

Finally, Section 6.1 of the project editor's report states:

> "Out [sic] test harness shows the Researchers attacks can be completely prevent [sic] by simply 'adding entropy' and changing the ShillKey (fake key) for every single transaction. This has also been confirmed by the 'Unpicking Plaid [sic]' lead Professor Patterson [sic]."

Firstly, this description of the proposed countermeasure is potentially misleading to a reader who does not consult the source e-mail discussion in which the countermeasure was introduced and discussed. The proposed countermeasure involves setting the two most significant bytes of the ShillKey's RSA modulus to a random value, rather than properly generating a fresh ShillKey as a product of two random primes.

Secondly, Professor Paterson merely agreed that the proposed modification *might* work, but simultaneously pointed out that it would be an unusual approach to adopt, since the protocol would now be using RSA-style operations with a modulus that was not necessarily the product of two primes. It is therefore a misrepresentation to assert that the proposed countermeasure has been "confirmed" by Professor Paterson.

In Section 6.2, the project editor's report argues about a lack of a formal definition of privacy in our work, digresses into an Oxford dictionary definition of privacy, muses about it, and refers again to the Australian standard. Sections 3 and 4 of our paper, however, make it easy to infer what the attacks against the ISO standard achieve: tracing cards across executions, and identifying the supported key set of a card. Any decent notion of privacy in the cryptographic literature would be rendered insecure under the attacks. Also note that the ISO standard clearly states hiding of card and card holder identifying information as being a feature of the protocol:

> "This is done in such a way that strong authentication of the ICC and credentials is possible in a fast, highly secure and private fashion without the exposure of card or cardholder identifying information or any other information which is useful to an attacker." [ISO14, p. vi]

The project editor's report discusses the muteness of our attack in Section 6.3, according to our understanding due to the availability of CPLC data. First let us remark that there are card-based systems, especially in the area of sovereign documents, where the access to the CPLC is restricted because of privacy reasons. Secondly, let us quote from the ISO standard, Annex E:

> "In implementations where ID-leakage of any form cannot be tolerated, care may need to be taken to ensure the ATR/ATQ response does not contain unique per-card or per- scheme identifying data,..."
>
> and
>
> "Consider switching off access to administrative applications from contactless interfaces, particularly ones which store unique card identification information such as the GlobalPlatform Card Production Life Cycle (CPLC) data." [ISO14, p. 16]

Our attacks actually show that these countermeasures could be moot.

4 On Section 7 ("Response to "Unpicking PLAID', Section 5 comments")

The project editor's report states in Section 7.3, concerning our discussion about Bleichenbacher's attack:

> "As acknowledged by the authors of 'Unpicking PLAID', the usage of repeating RND1 in the Initial Authenticate Response is an effective mitigation against this class of attack even if the modulus becomes known."

This is clearly not what we state. We have never said that this completely prevents the attack, nor that other attacks don't apply. It is up to the PLAID authors to provide supporting evidence for this claim.

In Section 7 of the project editor's report, a recurring justification why the security concerns expressed in Section 5 of our paper do not have to be taken into account is that:

> "The Researchers have not presented any evidence of a security issue with this approach."

Let us stress again that we believe *supporting* evidence is needed to argue the security of a protocol and that the absence of known attacks should not be considered such.

5 Further Remarks

While we agree with the author of the project editor's report that the ShillKey fingerprinting attack from Section 3 of our paper is worth paying attention to, we note that the project editor's report does not mention at all the Keyset fingerprinting attack in Section 4 of our paper, which allows an attacker to reveal the exact set of keys a card knows, thereby determining its capabilities in terms of which terminals the card is able to authenticate to.

Finally, we wish to remark that the personal email correspondence with Professors Fischlin and Paterson, linked to in Annex A of the project editor's report, was published without their consent.

References

[Aus10] Standards Australia. *AS 5185-2010 Protocol for Lightweight Authentication of IDentity (PLAID)*. Standards Australia, 2010.

[DFF+14a] Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azzurra Marson, Arno Mittelbach, and Kenneth G. Paterson. Unpicking PLAID – A Cryptographic Analysis of an ISO-standards-track Authentication Protocol. In *1st International Conference on Research in Security Standardisation (SSR 2014)*, volume 8893 of *Lecture Notes in Computer Science*, pages 1–25. Springer, December 2014.

[DFF+14b] Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azzurra Marson, Arno Mittelbach, and Kenneth G. Paterson. Unpicking PLAID – A Cryptographic Analysis of an ISO-standards-track Authentication Protocol. Cryptology ePrint Archive, Report 2014/728, 2014. `http://eprint.iacr.org/`.

[Fre14] Graeme Freedman. Nit-Picking PLAID: AS & ISO Project Editors Report into "Unpicking Plaid". Cryptology ePrint Archive Forum, November 2014. `https://dl.dropboxusercontent.com/u/41736374/UnpickingReport%20V1.pdf`.

[ISO14] ISO. *DRAFT INTERNATIONAL STANDARD ISO/IEC DIS 25185-1.2 Identification cards — Integrated circuit card authentication protocols — Part 1: Protocol for Lightweight Authentication of Identity*. International Organization for Standardization, Geneva, Switzerland, 2014.

[Sak13] Hideki Sakurada. Security evaluation of the PLAID protocol using the ProVerif tool. `http://crypto-protocol.nict.go.jp/data/eng/ISOIEC_Protocols/25185-1/25185-1_ProVerif.pdf`, September 2013.

[Wat13] Dai Watanabe. Security analysis of PLAID. http://crypto-protocol.nict.go.jp/data/eng/ISOIEC_Protocols/25185-1/25185-1_Scyther.pdf, September 2013.