NIT-PICKING PLAID

AS & ISO Project Editors Report into "Unpicking Plaid"

AS & ISO/IEC Standard PLAID Project Editors report into Darmstadt University of Technology and Royal Holloway University of London Researchers Paper titled "Unpicking Plaid"

This discussion of "Unpicking Plaid" relates solely to the published "Standard" PLAID versions AS 5185-2010 including the related Reference Implementation as well as the incomplete and unpublished ISO/IEC 25185-1 (DIS1 Draft). The paper discusses errors in the researcher's definitions vs the Standards, the actual brilliance of the attack against RSA, and how the attack is both mute as well as easily prevented with zero technical change to the Standards. The discussion also identifies a number of errors in historical facts related to the development of PLAID as well as misunderstandings, mis-definitions and mis-characterisations as published by the group of self-stated "Independent Researchers".

Finally it identifies that the Researchers "Abstract" and privacy definitions were devised more for PRESS consumption than for consistency or technical accuracy to their own paper and research.

Version 1

November 2014

No wele is worth, that may no sorwe dryen.
And for-thy, who that hath an heed of verre,
Fro cast of stones war him in the werre!

Geoffrey Chaucer's 'Troilus and Criseyde, book II', circa 1385, (lines 866-868)

REVISION RECORD

This report is informative and is not maintained

Point of contact for any queries regarding this report is the ISO/IEC Project Editor.

Telephone: +61 403113624

E-mail: Graeme.Freedman@dotindot.com

Issue	Date	Description of revision
0.1	October 2014	Initial draft
0.2	November 2014	Draft for review
0.3	November 2014	Draft for review
1.0	November 19, 2014	First Public Draft

TABLE OF CONTENTS

1 Definition of Terms and Acronyms

- PLAID – Protocol for Lightweight Authentication of Identity
- PACS – Physical Access Control Systems
- LACS – Logical Access Control Systems
- ISO/IEC 14443 (all parts) – suite of low level standards defining "smart card" contactless interfaces and used widely for Transit, e-Passport, Contactless banking, NFC, High Frequency PACS and most other contactless use-cases requiring channel security.
- ISO/IEC 7816 (all parts) – suite of low level standards defining "smart card" contact interfaces and used widely for phone SIM, LACS, PKI, FIPS-201, EMV banking and many other use-cases involving smart cards.
- ICC – Integrated Circuit Card (Smartcard)
- IFD – InterFace Device (reader and/or seperate or integrated SAM)
- ID-Leakage – A constant subset of data that is static for each authentication exchange between a specific ICC and IFD.
- ShillKey – A Shill key is randomly generated by the ICC during PLAID instantiation but is only known to the ICC. A shill key is generated for both the Initial Authenticate (RSA) and the Final Authenticate (AES) commands. Shill key is used by the ICC in place of the actual key when an inconsistency is detected, thereby removing any indication to a potential attacker that an inconsistency has been detected.
- IP – Intelectual Property
- Commonwealth – The Australian Comonwealth Government
- COTS – Commercial Off The Shelf
- FIPS – US Government Federal Information Processing Standards
- ISO/IEC – International Standards Organisation/International Electrotechnical Comission
- Kerckhoffs principle - A cryptosystem should be secure even if everything about the system, except the key is public knowledge.
- Privacy – A state in which one is not observed or disturbed by other people
- SAM – Security Access Module – a smartcard format secure cryptographic hardware device which implements the IFD or back-office component of cryptographic transactions
- Researchers - Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azzurra Marson, Arno Mittelbach, Kenneth G. Paterson
- PICC - Proximity Integrated Circuit Card, logically equivalent to ICC

2 PLAID Licence

Since this paper discusses significant issues related to the design of PLAID readers should be aware of the licence offered by the Commonwealth of Australia, set out below:

All intellectual property rights in the Protocol for Lightweight Authentication of ID (PLAID) and/or its source code and/or its associated reference implementation (the Licenced Materials) are owned by the Commonwealth of Australia. The Licenced Materials are used, copied, accessed, downloaded or reproduced by you, as a User, under licence from the Commonwealth of Australia. The licence provided is perpetual, irrevocable, world-wide, non-exclusive, royalty free and no-charge, but all Users of the Licenced Materials or any product using or incorporating the Licenced Materials must include this statement in any reproduction of the Licenced Materials or in any product using or incorporating the Licenced Materials. Use of the Licenced Materials or any product incorporating the Licenced Materials is at the User's own risk, and the Commonwealth of Australia makes no warranties or representations about the Licenced Materials and/or any product using or incorporating the Licenced Materials, including about their quality or fitness for purpose.

The licence that applies to you as a User of the Licenced Materials can be found at http://www.plaid.gov.au/

3 Background

PLAID has been available for review in the public domain since 2008, and before that was privately reviewed within Government (US and AU) circles and by workshop attendees. Although the principle of its operation has not changed since 2006 when the use of a RSA/AES hybrid protocol was devised, various details of PLAIDs implementation and more recently the Standards have changed over time. Through that time a number of attacks or potential attacks have been put forward by various parties. These have been reviewed in every instance and in most cases "coded" in order to directly test their practicality. The results of these reviews have been fed back into the "Reference Implementation" or the "Standard"/s or both depending on the details of the particular attack.

From 2010, with the release of the Australian standard, PLAID is solely documented in the following places;

1. First standardized by the publication of AS 5185-2010, (see link)

2. The current "reference implementation" (version 8.04) was then published to match the AS 5185-2010 standard and provide a detailed example to commercial developers of both card and reader code. See www.plaid.gov.au. Note that the intention of the reference implementation is just to code just one example of an implementation of the protocol, not to fully implement every possible option or combination that is legitimate in a Standard. The idea is that developers can either modify a reference implementation or write their own code then test against the released version to determine the interoperability against a basic implementation the Standard. It should be noted that the Standards also include test vectors, which are the formal arbiter of interoperability, and therefore trump any reference implementation.

3. Older reference implementation versions (used during the industry public consultation and workshop process) are also available on the same site, but are purely historic artifacts in order to show the development of the IP should there ever be a challenge or attempt by any party to "commercialize: the IP (rather than make it publically and freely available).

4. A new ISO standard is currently under development based on AS 5185-2010. It is nominally called ISO/IEC 25185-1 and is currently only formally documented as draft DIS 2, it will not be completed before the presentation of the "Unpicking PLAID" paper in December 2014. It contains significant changes including alignment to post 2010 FIPS RSA bit length recommendations as well as alignment with other ISO standards, particularly ISO/IEC 7816. There are multiple different committee drafts of this which are available via each country's representatives. Once ISO/IEC 25185-1 is published (probably Q2-2015) a new "Reference Implementation" will be published, currently the un-finished code for this has been used to test a number of the security and denial of service issues, including those generated by

"Unpicking PLAID". The AU standard 5185-2010 will also be withdrawn at the same time, as is normal practice for any standard being upgraded to ISO.

This paper addresses and discusses the claims made in the "Unpicking PLAID" paper under the individual chapter references of that paper

3.1 Primary Reference

This paper is a response to a specific paper published by the self-styled "Independent Researchers" of Armstadt University of Technology and Royal Holloway University of London, called "Unpicking PLAID" The paper itself has been distributed in at least three versions and is not version controlled or dated within the document. This response is made against the version at: https://eprint.iacr.org/2014/728. Which is uncontrolled and therefore may or may not be a stable version.

3.2 Scope

The authors of "Unpicking PLAID" have expended significant energy in briefing Press. Some criticism generated because of these briefings and published by these journalists is not discussed in "Unpicking PLAID" but appears in various journalists articles specifically referencing "Unpicking PLAID". Much of this mis-represents both the Unpicking PLAID paper and the actual PLAID Standard itself. The huge potential scope of any such discussion means is not addressed in this discussion (it is out of scope).

4 History

PLAID was developed in 2006 to meet the Australian Government agency "Centrelink" internal staff security and privacy needs. Centrelink (now Human Services) has the 2nd largest staff in the Commonwealth after Defence. Unlike many agencies, these people have no barrier between them and the general public, and their offices are more like a coffee lounge with computers rather than being seperated from customers by a service counter. They are therefore more prone to personal privacy attacks.Their surnames and personal access records were consequently protected and treated as personal private data.

The Security Team was asked to develop an authentication protocol secure enough for LACS and fast and practical enough for PACS. It needed to permit single or multi factor authentication over a ISO/IEC 14443 (contactless) interface which does not leak any useable or personal information. The emphasis was on personal privacy of Centrelink staff details. It was well known at the time, although not generally publically known, that all existing PACS protocols were or would soon be publically compromised. Even on 2006 virtually all PACS protocls were "clonable" and leaked ID record data although the tools to do so were not widely available on EBay etc (as they are now). The master keys for several PACS "crypto based" protocols were known to be acquireable, but off-the-shelf tools were not avalilable as they now are, nor were the default manufacturers keys published on the internet.

At that time, as is still the case, it was also clear that there were no public or even industry Standard based options, every PACS protocol was either already broken, leaked personal private data, or was highly proprietary and/or un-published. The type of low cost cards in use by PACS vendors was also an issue, since it was clear that there were weaknesses in the low level silicone which is often no more than fixed gate arrays and fixed memory. It was necessary to design assuming high end cards with serious crypto co-processors and protected memory. It was clear that the vast majority of the PACS industy relied on "Security by Obscurity" and that the internet was quickly going to remove even that last obstacle from attackers. The major design considerations were:

- Use of existing standards and FIPS approved cryptographic algorithms
- Support COTS card interfaces (i.e. meeting both ISO/IEC 14443 and 7816) for PACS and LACS.

- Put the existing FIPS approved cryptographic algorithms together so as to ensure resistance to all known practical attacks.
- "ID-Leakage" free
- Entire exchange must complete in less than 500ms (due to tap-n-go PACS use-cases – this also eliminates traditional PKIs even to this day)
- Consistent with Kerckhoffs principle.
- If a single card is compromised then only that card needs revocation in the PACS system.
- Multiple keysets and "key rolling" needs to be supported.
- Multiple PACS record structures (ACSRecords) to support multiple proprietary back-offices.

Key dates and events were:

2006-2007 – Private reviews including comments and suggestions by:

- Defence Signals Directorate (Now Australian Signals Directorate), proposed the use of a hybrid protocol using both symmetric and asymetric AES and RSA ciphers as well as deemed the protocol fit for purpose.
- Commercial vendors in the PACS/LACS and security arena.
- NIST (US Government).

2007 -The IP for PLAID was locked down and published by the Commonwealth and was made available for use with an unrestricted and irrevocable licence to prevent proprietarisation of the IP by any one PACS player.

2008 - Reference implementation published on the GovDex website:

- Specifications for PLAID.
- Source code for the Javacard applet / cap file.
- GUI for communication with a PLAID enabled smartcard.

2009 - PLAID workshops conducted at:

- First workshop held in Canberra, hosted by Department of Human Services.
- Second workshop held in Washington D.C. (USA), hosted by NIST.
- Short Workshop - Microsoft Seattle – Full security team, led by Niels Ferguson

2010 - PLAID workshop conducted at:

- Third workshop held in Hong Kong (Hong Kong), hosted by APSCA.

2010 – PLAID standardised in Australia as AS 5185.

2010 – Reference implementation updated to match AS 5185 and dedicated PLAID website created (www.plaid.gov.au).

2011 – SAM reference implementation made available through the PLAID website.

2011 – Personalisation example implementation made available through the PLAID website

2011 – PLAID put forward for ISO/IEC standardisation as a fasttrack of AS 5185.

2011 – Pilot trails conducted by multiple Government departments using cross platform command line software

2013 – As part of the ISO/IEC Process - Japan publishes two Cryptographic proofs using two different programatic methods:

http://crypto-protocol.nict.go.jp/data/eng/ISOIEC_Protocols/25185-1/25185-1_Scyther.pdf

http://crypto-protocol.nict.go.jp/data/eng/ISOIEC_Protocols/25185-1/25185-1_ProVerif.pdf

2012-2014 – ISO Process gradually moves forward torwards publication of ISO/IEC 25185-1. ISO process generates many minor technical changes due to need to link and align to other ISO standards including and particularily the ISO/IEC 7816-4 command set as well as enhancements requested by various countries.

5 Errors in "Unpicking Plaid"

The following are factual and editorial errors in the document:

1. Abstract – States that for **AS 5185-2010** *"we show that the **privacy** properties of PLAID are significantly weaker than claimed"* but in fact the report shows that the privacy properties of PLAID are unbroken by the attack **and in fact unbreakable by the attack**. The report actually shows that the **"ID Leakage"** properties of the protocol (as defined in **AS 5185-2010**) could be better implemented in the 2010 version of the reference implementation by implementing the fake "ShillKey" better - see further discussion in section 6.2.

2. Abstract – states that it will be ...." reporting a number of undesirable cryptographic features of the protocol" This is however unargued and not actualised. The reference appears to logically means section 5.3 of the Unpicking PLAID paper however, as shown in section 7 of this discussion these are either not claims of the protocol or are not shown to be weaknesses by any argument presented by the Researchers - see further discussion in section 7.

3. History in Introduction is not 100% correct – the Public Consultation process included additional workshops and stages – see section 4 "History" above

4. P3, Last paragraph, the words "added for privacy reasons" is incorrect, the ShillKey was added to delay and distract an atacker, privacy was never an issue and is not stated as a design requirement.

5. P4, last paragraph, P5 first paragraph – Not clear what point is being made – OPACITY is a completely different protocol based on Eliptic Curve technology. Last sentence seems to mix this Paper on PLAID up with a completely seperate report on OPACITY.
6. P3 2nd last paragraph the Researchers state "Even though the encryption key in RSA is usually public, in PLAID it is kept secret to enhance privacy". This is an incorrect representation of PLAID, the reason for both keys being kept secret is in fact to prevent any leakage to an attacker of the AES diversification seed in order to enhance security. Note that PLAID is not a PKI, and the use of public and private key concepts is not relevant, ALL keys are secured in (preferably) hardware crypto devices.

6 Response to “Unpicking PLAID”, Primary attack.

The Primary atacks are set out in sections 3 and 4 of the "Unpicking PLAID" paper. The following responses in this section address those sections.

In this response it should clearly be noted that the following text is a direct quote from the following paragraphgraphs of the Australian Standard AS 5185-2010, the core source document upon which the Researchers base their paper.

---------- Quotes from Australian Standard AS 5185-2010 follow ----------

Section 2, Objectives of PLAID;

PLAID addresses the following objectives, and it should—
(a) be broadly suitable for PACS and LACS use-cases using COTS products;
……
(d) support interface neutrality for contact or contactless usage;
……
(f) not expose any individually identifiable, unique or determinable data or characteristic of the ICC or cardholder during authentication;
(g) not expose private data in the clear at any interface;
……..

Section 4, Terms and definitions:

> 4.4 ID-Leakage
> A constant subset of data that is static for each authentication exchange between a specific ICC and IFD.
> NOTE: This subset (even when encrypted) could allow for identification of an individual smartcard, and therefore indirectly the cardholder.

---------- Quotes from Australian Standard AS 5185-2010 end ----------

6.1 A brilliant attack against RSA but easily prevented in PLAID

The attack is quite brilliant, and is very interesting in its potential against RSA generically, but is easy to prevent without changing Standards.

We have coded the primary attack against our test harnesses. Out tests show that the primary attack can in theory approximate the value of the ShillKey as set out in sections 3 and 4 of the Unpicking PLAID Paper when applied against the 2010 version of the PLAID Reference Implementation (version 8.04). We have not determined how many samples would be needed for a full complement of cards; however the number and logistics required to actually mount a live attack is likely to be completely impractical, and more easily done other ways as discussed below.

The primary attack is against the 2010 version of the Reference Implementation that was written for the Australian Standard AS 5185-2010. This version of the various reference implementations can be better coded. You will note that some early reference implementation versions did not use a ShillKey at all (follow link).

Reference implementations are easily and regularly changed since they generally only implement a sub-set of the standard, just enough to be able to assist developers test interoperability between differing implementations of the same standard. They are not a formal part of the Standard, just guidance for developers.

Unlike the various (8) PLAID reference implementations, the standard itself includes absolute normative (compulsory) test vectors which are included as "Appendix A, Test Vectors" These are the critical tests which determine compliance with the standard.

For AS-5185-2010 the Test Vectors do not define ShillKey at all, since it is left up to the developer to implement. The same is true of all versions of the Draft ISO/IEC Standard 25185-1;

How the ShillKey is practically implemented is not defined in test vectors in ANY version of any of the Standards involved, and therefore any change has zero impact on interoperability.

The above means that any 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. (ShillKey is - after all - just a fake error response mechanism, to avoid any error code).

Out test harness shows the Researchers attacks can be completely prevent by simply “adding entropy” and changing the ShillKey (fake key) for every single transaction. This has also been confirmed by the "Unpicking Plaid" lead Professor Patterson, – see email in Annex A.

Why this was not reported in the "Unpicking PLAID" paper is unclear, we would normally expect academic reports to include the results of third parties (negative or positive) particularly when they selectively report other correspondence with those parties. It does however make the press story significantly less entertaining.

The full details of the changes required to prevent the attack, whilst only costing a few milliseconds in transaction time are include in the email trail to/from Professor Patterson in Annex A.

These will be included in the ISO/IEC 25185-1 version of the Reference Implementation once ISO/IEC 25185-1 is published in 2015 as well as a transitional update in version 8.04.X

6.2 Researchers assign Privacy to Inanimate objects

The paper starts out in its Abstract stating *"we show that the privacy properties of PLAID are significantly weaker than claimed*" and goes on to state that *"we describe and evaluate a suite of attacks that break the privacy goals of PLAID."* Along with, many other similar references and claims,

The context, lack of definition and the many references to the term "privacy" in the paper lead the reader to believe that the term is used in the normal English sense. This is defined in the Oxford dictionary as: "*A state in which one is not observed or disturbed by other people*". Other dictionaries contain very similar definitions related to "people", and the Researchers do not define their technical meaning or in fact their plurality of meanings of "Privacy".

At section 4.4 Australian Standard AS 5185-2010 specifically defines ID-Leakage (see quote above), and clearly defines that via a definition which is quite different to the dictionary definition of "Privacy".

The Researchers paper makes many claims against "privacy goals", but does not reference the formal source document Australian Standard AS 5185-2010 for the PLAID "privacy goals".

In fact the Researchers attack is a clear "ID-Leakage attack" under the Definition of ID-Leakage in AS 5185, and their use of the term "privacy" is clearly misleading, particularily in context of the Standard.

A review of the actual Standard – AS 5185-2010 shows that the term "privacy" only occurs twice, in an Annex in relation to the protection of key diversification data or seed (DivData) and most importantly in section 2 (g) under "Objectives of PLAID", which looks very much like the Researchers "privacy goal".

Section 2 (g), "Objectives of PLAID", clearly states;

- *"(g) not expose private data in the clear at any interface;"*

Given that it is clear according to virtually any English definition that there is a very significant "privacy" difference between;

1. "Personal private data", (like the user's personal PACS Wiegand Record, held in the ACSRecord), and

2. "Card fixed data" (like the card serial number) which is easily and precisely available to an attacker but not used in PLAID, and
3. "Card statistical data" (like the Researchers ShillKey approximations) that is potentially exposing random data used only on error conditions.

It would seem that the Researchers have **personified** the physical card and their definition of the "privacy goal" to the point where both "Card fixed data" and "Card statistical data" are now parts of their definition of "Personal Private Data", or simply merged into their exceptionally broad definition of "Privacy". This is clearly inconsistent with a normal English language definition of Privacy, which involves the person, not the inanimate, virtual, or statistical object.

This is like saying that if you take a photo of a person wearing a Batman mask and cape as they scale a tall building and the photo includes a crowd of various masked wrestlers watching, you can then prove Batman is Bruce Wayne by photo-analyzing their masks.

The Researchers have in fact NOT shown that any real or useful "private data" is exposed in the clear at any interface" and have in fact confirmed that exposure of actual PRIVATE data it is not possible under this attack or any attack referenced. Batman's real identity is safe! The bold statement that "the privacy properties of PLAID are significantly weaker than claimed" and that their attacks "break the privacy goals of PLAID" is a very long way from the facts, and conceivably both misleading and deceptive.

The Researchers have in fact shown that there is a potential for ID-leakage as defined in AS 5185-2010 and as implemented in version 8.04 of the reference implementation.

Further; readers should be aware that, in the case of a PACS system, the critical "Personal Private Data" is in fact the "Wiegand" number (or other stored credential strings) associated with one or more of the PLAID "ACSRecord" values secured in the PLAID on-card JavaCard applet. If these records were exposed then an attack could be mounted on two exposed building signal wires against most existing PACS systems doors simply using a laptop and a wired in Wiegand emulator and the Wiegand record binary value. Most other card protocols hold these values in the clear, and/or use the card serial number as this record.

It is therefore clear that both "card fixed data" and "card statistical data" can be determined, and that this is a very interesting, but completely mute fact.

The ShillKey itself is in fact a fake key designed to confuse and mis-direct the resources of an attacker and is random for that purpose, which in fact seems to have been served.

Finally - "card fixed data" is explicitly called out as normally available in the clear with an explicit warning in annex E of Australian Standard AS 5185-2010. Those involved in the practical issues of PACS and LACS cards will know that this is completely unsurprising.

The argument about Privacy is therefore both mute and is conceivably devised to "beat up" a press story. It seems that "Privacy Goals" and "Privacy" definitions are being "made up" by the Researchers on-the fly to support their agenda, rather than common-sense or even English.

6.3 Attack is Mute

The actual attack is a remarkable and very smart phenomenon, but is mute because it never obtains “personal identification” data in any form and only obtains a statistical approximation of random data (not private data) in the form of a “fake” ShillKey set up by PLAID to deflect an attacker.

More accurate, non-statistical, per-card identification data is much more easily obtained in the clear, the ShillKey is not "Personal Private Data", but is just random data generated by the card itself.

With COTS cards, it is practically very difficult to remove all unique per-card electronic identification, so an attacker will virtually always be able to obtain a "card serial number" which is also commonly

printed on the card (check your ID Cards). (I.e. the electronic equivalent of the Batman or Robin outfits.)

Below see two reports generated from the contactless interface of two cards (in the clear). These reports are from two of the most common dual interface cards used in US FIPS-201 Government ID implementations worldwide (the Oberthur ID-One Cosmo V7.0.1. card).


eg contactless card1.html


eg contactless card2.html

NB – If Links above do not work, go to Annex B

You will notice that the IC Serial Numbers for these two cards (separate reports) are 00 00 05 91 and 00 00 07 11 respectively, available in the clear, these are also physically printed on the cards. You will also be interested in the wealth of other information included in the reports which is also in the clear. This is all inside a Card Production Life Cycle (CPLC) structure which is used for the full life of the card to register each card uniquely using the GlobalPlatform lifecycle management Standards (which are also partially mirrored in ISO standards, and use the key standards including the ISO/IEC 7816 series)

The same is true of most existing PACS cards since most only supply an IC Serial Number with no authentication protocol (zero crypto). Many low end un-managed cards (all MiFare cards) embed the IC Serial Number in either the Historical Bytes (see in report above) or in the cards Answer To Reset/Query (also see the structure in the report above) or occasionally in other responses.

The reason the IC Serial Number is universally available in the clear is because most if not all other (NON PLAID) crypto based protocols use the IC Serial Number either for lifecycle management or as the seed for the cards symmetric key diversification algorithm or both. It is also used in GlobalPlatform secure channel protocols for card application management, diversification and application secure load.

So the IC Serial number is commonly used in the clear for both the symmetric key diversification seed and for stock control purposes and for card management and update. Finally - manufacturers commonly need the batch and IC Serial Number to make their print personalisation systems work.

The first version we saw of the Researchers paper did not point this out. The Unpicking PLAID researcher's team were clearly surprised when told about the above (see email in annex), even though this fact was clearly stated in Annex E of Australian Standard AS 5185-2010 (their reference document). They immediately added the page 5 paragraph "Reaction by Responsible Authorities" into the next version to explain the work-around from Annex E everyone else needed to do to ensure the "unpicking PLAID" attack remained relevant and not mute.

As per the objectives of PLAID set out at the start of this section, it needs to be practically implementable on COTS cards. The response on page 5 is clearly an academic response since the CPLC data is fundamental to card lifecycle management and smartcards are even moving away from supporting dual interfaces in favour of just a single contactless interfaces. This has already happened for NFC phones. How do the Researchers plan to implement without a contact interface?

Finally you would need both very large quantities and accept limitations on COTS availability and when and where you could manage cards to justify the very academic changes suggested. It is much easier to make minor changes the code in the reference implementation as set out earlier in this discussion, and assume that there is significant but useless ID-Leakage from CPLC data.

7 Response to “Unpicking PLAID”, Section 5 comments

A number of comments are made in section 5 of the "Unpicking PLAID" paper.

7.1 "Forward (In) security" (5.1)

The Researchers use the term "Forward security" which is undefined. We assume, but it is not clear, that the authors are referring to the concept of "Forward Secrecy" and "Perfect Forward Secrecy" as defined by Diffie, Oorschot and Wiener. This appears reasonable since their own reference [BPR00] uses the assumed term rather than the specified "Forward Security"

Response

"Unpicking PLAID" has correctly identified that the PLAID protocol does not provide the security characteristic of "Forward Secrecy" or "Perfect Forward Secrecy". As stated in "Unpicking PLAID", if the IFD is fully compromised then it would be possible to access all past and future sessions where the entire exchange has been captured.

The claim that "*The loss of keys of either party immediately reveals all past session keys, and also future sessions…*" is however inaccurate.

In the event that an individual ICC is compromised, then only sessions using **that ICC** can be compromised because only that single ICC holds the diversification seed "DivData" for itself.

Due to the key diversification utilised in the symmetric cipher, a single ICC compromise will not allow an adversary to decrypt or complete the session for any other ICC.

In other words, for any ICC other than the one compromised, an adversary will be unable to complete the transaction, decrypt the IA Response/FA Response or retrieve the KeysHash value.

Finally – the Researchers have not described a method to obtain the keys in the first place, PLAID is implemented in smartcard and SAM hardware devices with highly accredited secure key storage capability, and includes reference implementation examples for SAM hardware devices.

Further - It remains unclear if this section is the subject of the reference in the Abstract to *" …a number of undesirable cryptographic features of the protocol".* The Researchers should explain this statement so it can be reviewed in the public domain.

7.2 "Key (In) security in the Bellare-Rogaway Model" (5.2)

Response

No concerns or inaccuracies noted. The point seems to be that the particular Bellare-Rogaway model is not met, but no claim in that regard is made, and the Researchers have failed to describe any possible attack.

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

Further - It remains unclear if this section is the subject of the reference in the Abstract to *" …a number of undesirable cryptographic features of the protocol".* The Researchers should explain this statement so it can be reviewed in the public domain.

7.3 "On the Applicability of Bleichenbacher's Attack" (5.3)

Response

The practicality of an attack of this nature is predicated on obtaining the values of an RSA public key (that is, the modulus and the public exponent). Section 3 of "Unpicking PLAID" provides the specifics of a valid attack which could provide approximations for these values.

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.

Additionally the version of the reference implementation (Targeted for release with the publication of ISO/IEC 25185-1) varies the value of the ShillKey slightly on each usage thereby as discussed earlier defeats the proposed statistical attack introduced in Section 3.

Further - It remains unclear if this section is the subject of the reference in the Abstract to *" …a number of undesirable cryptographic features of the protocol".* The Researchers should explain this statement so it can be reviewed in the public domain.

7.4 "CBC-mode encryption" (5.4)

Response

Contactless protocols such as PLAID need to optimise every possible operation in order to achieve practical tap-n-go performance.

The authors of "Unpicking PLAID" have correctly noted that hardcoding the Initialisation Vector (IV) to an all zero string when using CBC mode "….*does not conform with standard practice, which demands the use of random IVs to achieve security against chosen plaintext attacks*". This is usually true, however in the case of PLAID there is no opportunity to perform a plaintext attack since each symmetric cipher operation occurs only after verification of the previous step. Additionally, the first block of the FA Command is comprised of 14 random values unique per session, further reducing the requirement for strong IVs which would unnecessarily complicate the protocol.

The authors have correctly stated that draft ISO/IEC 25185-1 is inconsistent with ISO/IEC 9797-1 padding method 2 as this standard states that padding is always applied (even if the cipher operation is being performed on a complete block). In the interest of optimising the runtime required, PLAID was designed so that, a complete block was used thereby eliminating the need for padding.

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

Further - It remains unclear if this section is the subject of the reference in the Abstract to *" …a number of undesirable cryptographic features of the protocol".* The Researchers should explain this statement so it can be reviewed in the public domain.

7.5 "Entity Authentication" (5.5)

Response

No concerns or inaccuracies noted. In general, the concerns regarding PKCS#1.5 and AES-CBC have been articulated in 5.3 and 5.4 respectively.

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

Further - It remains unclear if this section is the subject of the reference in the Abstract to *" …a number of undesirable cryptographic features of the protocol".* The Researchers should explain this statement so it can be reviewed in the public domain.

7.6 "Payload Insecurity" (5.6)

Response

The "Payload" has been removed from current versions of ISO/IEC 25185-1

The comment clearly includes the assumption that a card has been broken, but does not described a method to obtain the keys in the first place, PLAID is implemented in smartcard and SAM hardware devices with highly accredited secure key storage capability, and includes reference implementation examples for SAM hardware devices.

Further - It remains unclear if this section is the subject of the reference in the Abstract to *" …a number of undesirable cryptographic features of the protocol".* The Researchers should explain this statement so it can be reviewed in the public domain.

7.7 "On the Impossibility of Key Revocation" (5.7)

Response

Physical Access control systems currently, universally, only support credentials (ACS Records) in the clear, typically over very slow Wiegand or slightly faster RS-485 cabling. Some "new" systems support symmetric encryption at the session layer over RS485. These systems, unlike PKI systems, can only revoke the customer record (typically the Wiegand or card serial number). They have no concept of asymmetric cryptography or the possibility of key revocation, and the vast majority use the Wiegand Wire Data analogue protocol over two signal wires which cannot support any form of session security nor support any form of digital data (Key Revocation) transmission.

Per-Card revocation is therefore limited to the capability of existing PACS systems, which is practically limited to revocation of the (typically 26 bit) ACSRecord. These systems typically have no concept of key management at all, and therefore PLAID is very much a transition strategy whilst the PACS industry modernises.

Like most large scale contactless symmetric key systems, (Transit systems being the best example), PLAID supports key roll by supporting multiple on-card keysets – once one is out-of-date or compromised then the terminals are instructed to use a new one – and the cards can be updated from the terminals or desktop readers using secure hardware SAMS.

Further - It remains unclear if this section is the subject of the reference in the Abstract to *" …a number of undesirable cryptographic features of the protocol".* The Researchers should explain this statement so it can be reviewed in the public domain.

7.8 "Key Legacy Attack" (5.8)

Response

Kerckhoffs principle applies here - PLAID does not make use-case related decisions based on the particular keyset used; this is the purpose of the OPModeID record. It does not matter which keyset is used, as long as one is valid, the perimeter security decisions are made based on the authenticated OPModeID record sent to the card, and the card responding with a specific ACSRecord based on that. In most real cases the actual keyset (version) will be obvious from the building owner, and is effectively public data as per Kerckhoffs principle.

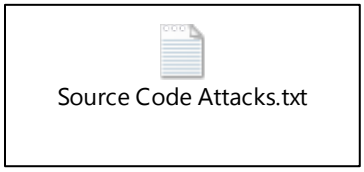
The Researchers have not described a method to obtain the keys in the first place, which would be necessary to actually mount any actual attack.

Further - It remains unclear if this section is the subject of the reference in the Abstract to *" …a number of undesirable cryptographic features of the protocol".* The Researchers should explain this statement so it can be reviewed in the public domain.

8 Annex A – Correspondence with Marc Fischlin and Ken Paterson

As referenced elsewhere – see full text of correspondence with Marc Fischlin and Ken Paterson, best read "bottom to top" and particularly note the second last email correspondence.

https://dl.dropboxusercontent.com/u/41736374/Source%20Code%20Attacks.txt



9 Annex B – Example Data in the clear from GlobalPlatform JavaCard Cards

See reports on following pages:

Date: 2014-11-11
Time: 16:34:25
Version: 3.0.1

JLoad Report

Content:

1. General Card Information

Card Type:	ID-One Cosmo V7.0.1

Back to Content

2. Reset Information

Cold ATR

```
3B 8F 80 01 80 73 CC 91 CB F9 A0 00 00 03 08 00 00 10 00 29
```

Interface Characters

TS	3B	Convention	direct
T0	8F	Number of historical bytes	15
TD1	80	Protocol type	T=0
TD2	01	Protocol type	T=1

Default Values

Clock rate conversion integer	372
Baud rate adjustment integer	1
Maximum frequency supported	5000000 Hz
Programming current factor	50
Programming voltage	5000 mV
Extra guard time integer	0
T=0 work waiting time integer	10
T=1 information field size IFSC	32
T=1 character waiting time integer	13

T=1 block waiting time integer	4
T=1 error detection code	LRC
Clock stop	not supported
Operating condition classes	A only
SPU	not used

Historical Bytes

80 73 CC 91 CB F9 A0 00 00 03 08 00 00 10 00

Category indicator	status indicator in compact TLV object	
Card capabilities	DF selection	by full DF name by partial DF name implicit
	EF access	short EF identifier supported
	EFs of TLV structure	supported
	Behaviour of write functions	one-time write
	Value FF for first byte of TLV tags	valid (long private tags, constructed encoding)
	Data unit size	2 nibble(s)
	Command chaining	supported
	Extended Lc and Le fields	supported
	Logical channel assignment	by interface device
	Maximum number of logical channels	4
Application identifier	AID of impl. selected application	A0 00 00 03 08 00 00 10 00

Warm ATR

3B 8F 80 01 80 73 CC 91 CB F9 A0 00 00 03 08 00 00 10 00 29

Interface Characters

TS	3B	Convention	direct
T0	8F	Number of historical bytes	15
TD1	80	Protocol type	T=0
TD2	01	Protocol type	T=1

Default Values

Clock rate conversion integer	372
Baud rate adjustment integer	1
Maximum frequency supported	5000000 Hz
Programming current factor	50
Programming voltage	5000 mV

Extra guard time integer	0
T=0 work waiting time integer	10
T=1 information field size IFSC	32
T=1 character waiting time integer	13
T=1 block waiting time integer	4
T=1 error detection code	LRC
Clock stop	not supported
Operating condition classes	A only
SPU	not used

Historical Bytes

80 73 CC 91 CB F9 A0 00 00 03 08 00 00 10 00

Category indicator	status indicator in compact TLV object	
Card capabilities	DF selection	by full DF name by partial DF name implicit
	EF access	short EF identifier supported
	EFs of TLV structure	supported
	Behaviour of write functions	one-time write
	Value FF for first byte of TLV tags	valid (long private tags, constructed encoding)
	Data unit size	2 nibble(s)
	Command chaining	supported
	Extended Lc and Le fields	supported
	Logical channel assignment	by interface device
	Maximum number of logical channels	4
Application identifier	AID of impl. selected application	A0 00 00 03 08 00 00 10 00

Back to Content

3. CPLC Data

48 20 50 2B 82 31 80 30 00 63 02 91 00 00 07 11 20 06 11 42 10 12 11
43 10 12 11 44 10 12 13 03 00 00 00 00 00 00 00 00 00 00

ROM Part

48 20 50 2B 82 31 80 30 00 63

IC Fabricator	48 20	
IC Type	50 2B	
Operating System Identifier	82 31	
Operating System Release Date	80 30	2008-01-30

Operating System Release Level	00 63	

EEPROM Part

02 91 00 00 07 11 20 06 11 42 10 12 11 43 10 12 11 44 10 12 13 03 00 00 00 00 00 00 00 00 00 00

IC Fabrication Date	02 91	2010-10-18
IC Serial Number	00 00 07 11	
IC Batch Identifier	20 06	
IC Module Fabricator	11 42	
IC Module Packaging Date	10 12	2011-01-12
ICC Manufacturer	11 43	
IC Embedding Date	10 12	2011-01-12

Pre-Personalization Data

11 44 10 12 13 03 00 00

IC Pre-Personalizer	11 44	
IC Pre-Personalization Date	10 12	2011-01-12
IC Pre-Personalization Equipment Identifier	13 03 00 00	

Personalization Data

00 00 00 00 00 00 00 00

IC Personalizer	00 00
IC Personalization Date	00 00
IC Personalization Equipment Identifier	00 00 00 00

Back to Content

4. Card Manager / Issuer Security Domain

A0 00 00 01 51 00 00

Key Set

Version	01	
Key	ID: 01	Length:16 Type:AES (16, 24, or 32 long keys) '88'
Key	ID: 02	Length:16 Type:AES (16, 24, or 32 long keys) '88'
Key	ID: 03	Length:16 Type:AES (16, 24, or 32 long keys) '88'

Properties

AID	A0 00 00 01 51 00 00	A0 00 00 01 51 00 00

FCI	6F 6D 84 07 A0 00 00 01 51 00 00 A5 62 73 2F 06 07 2A 86 48 86 FC 6B 01 60 0C 06 0A 2A 86 48 86 FC 6B 02 02 01 01 63 09 06 07 2A 86 48 86 FC 6B 03 64 0B 06 09 2A 86 48 86 FC 6B 04 03 15 9F 6E 2A 48 20 50 2B 82 31 80 30 00 63 02 91 00 00 07 11 20 06 11 42 10 12 11 43 10 12 11 44 10 12 13 03 00 00 00 00 00 00 00 00 00 00 9F 65 01 FF	
KeyDiversificationData	45 52 54 48 55 52 00 00 07 11	
IIN	4F 42 45 52 54 48 55 52	
CIN	48 20 50 2B 20 06 00 00 07 11	
Card recognition data	GlobalPlatform 1	
Card management type/version	GlobalPlatform 2 / 2.1.1	
Card identification scheme	GlobalPlatform 3	
Secure channel protocol	GlobalPlatform 4 SCP03 i=15	
Confirmation counter	0	

Back to Content

5. Security Domains

Back to Content

6. Applets

Back to Content

7. Packages

Back to Content

Date: 2014-11-11
Time: 16:31:15
Version: 3.0.1

JLoad Report

Content:

1. General Card Information

Card Type:	ID-One Cosmo V7.0.1

Back to Content

2. Reset Information

Cold ATR

```
3B 8F 80 01 80 73 CC 91 CB F9 A0 00 00 03 08 00 00 10 00 29
```

Interface Characters

TS	3B	Convention	direct
T0	8F	Number of historical bytes	15
TD1	80	Protocol type	T=0
TD2	01	Protocol type	T=1

Default Values

Clock rate conversion integer	372
Baud rate adjustment integer	1
Maximum frequency supported	5000000 Hz
Programming current factor	50
Programming voltage	5000 mV
Extra guard time integer	0
T=0 work waiting time integer	10
T=1 information field size IFSC	32
T=1 character waiting time integer	13

T=1 block waiting time integer	4
T=1 error detection code	LRC
Clock stop	not supported
Operating condition classes	A only
SPU	not used

Historical Bytes

80 73 CC 91 CB F9 A0 00 00 03 08 00 00 10 00

Category indicator	status indicator in compact TLV object	
Card capabilities	DF selection	by full DF name by partial DF name implicit
	EF access	short EF identifier supported
	EFs of TLV structure	supported
	Behaviour of write functions	one-time write
	Value FF for first byte of TLV tags	valid (long private tags, constructed encoding)
	Data unit size	2 nibble(s)
	Command chaining	supported
	Extended Lc and Le fields	supported
	Logical channel assignment	by interface device
	Maximum number of logical channels	4
Application identifier	AID of impl. selected application	A0 00 00 03 08 00 00 10 00

Warm ATR

3B 8F 80 01 80 73 CC 91 CB F9 A0 00 00 03 08 00 00 10 00 29

Interface Characters

TS	3B	Convention	direct
T0	8F	Number of historical bytes	15
TD1	80	Protocol type	T=0
TD2	01	Protocol type	T=1

Default Values

Clock rate conversion integer	372
Baud rate adjustment integer	1
Maximum frequency supported	5000000 Hz
Programming current factor	50
Programming voltage	5000 mV

Extra guard time integer	0
T=0 work waiting time integer	10
T=1 information field size IFSC	32
T=1 character waiting time integer	13
T=1 block waiting time integer	4
T=1 error detection code	LRC
Clock stop	not supported
Operating condition classes	A only
SPU	not used

Historical Bytes

80 73 CC 91 CB F9 A0 00 00 03 08 00 00 10 00

Category indicator	status indicator in compact TLV object	
Card capabilities	DF selection	by full DF name by partial DF name implicit
	EF access	short EF identifier supported
	EFs of TLV structure	supported
	Behaviour of write functions	one-time write
	Value FF for first byte of TLV tags	valid (long private tags, constructed encoding)
	Data unit size	2 nibble(s)
	Command chaining	supported
	Extended Lc and Le fields	supported
	Logical channel assignment	by interface device
	Maximum number of logical channels	4
Application identifier	AID of impl. selected application	A0 00 00 03 08 00 00 10 00

Back to Content

3. CPLC Data

48 20 50 2B 82 31 80 30 00 63 02 91 00 00 05 91 20 06 11 42 10 12 11
43 10 12 11 44 10 12 13 03 00 00 00 00 00 00 00 00 00 00

ROM Part

48 20 50 2B 82 31 80 30 00 63

IC Fabricator	48 20	
IC Type	50 2B	
Operating System Identifier	82 31	
Operating System Release Date	80 30	2008-01-30

Operating System Release Level	00 63	

EEPROM Part

02 91 00 00 05 91 20 06 11 42 10 12 11 43 10 12 11 44 10 12 13 03 00 00 00 00 00 00 00 00 00 00

IC Fabrication Date	02 91	2010-10-18
IC Serial Number	00 00 05 91	
IC Batch Identifier	20 06	
IC Module Fabricator	11 42	
IC Module Packaging Date	10 12	2011-01-12
ICC Manufacturer	11 43	
IC Embedding Date	10 12	2011-01-12

Pre-Personalization Data

11 44 10 12 13 03 00 00

IC Pre-Personalizer	11 44	
IC Pre-Personalization Date	10 12	2011-01-12
IC Pre-Personalization Equipment Identifier	13 03 00 00	

Personalization Data

00 00 00 00 00 00 00 00

IC Personalizer	00 00
IC Personalization Date	00 00
IC Personalization Equipment Identifier	00 00 00 00

Back to Content

4. Card Manager / Issuer Security Domain

A0 00 00 01 51 00 00

Key Set

Version	01	
Key	ID: 01	Length:16 Type:AES (16, 24, or 32 long keys) '88'
Key	ID: 02	Length:16 Type:AES (16, 24, or 32 long keys) '88'
Key	ID: 03	Length:16 Type:AES (16, 24, or 32 long keys) '88'

Properties

AID	A0 00 00 01 51 00 00	A0 00 00 01 51 00 00

FCI	6F 6D 84 07 A0 00 00 01 51 00 00 A5 62 73 2F 06 07 2A 86 48 86 FC 6B 01 60 0C 06 0A 2A 86 48 86 FC 6B 02 02 01 01 63 09 06 07 2A 86 48 86 FC 6B 03 64 0B 06 09 2A 86 48 86 FC 6B 04 03 15 9F 6E 2A 48 20 50 2B 82 31 80 30 00 63 02 91 00 00 05 91 20 06 11 42 10 12 11 43 10 12 11 44 10 12 13 03 00 00 00 00 00 00 00 00 00 00 9F 65 01 FF	
KeyDiversificationData	45 52 54 48 55 52 00 00 05 91	
IIN	4F 42 45 52 54 48 55 52	
CIN	48 20 50 2B 20 06 00 00 05 91	
Card recognition data	GlobalPlatform 1	
Card management type/version	GlobalPlatform 2 / 2.1.1	
Card identification scheme	GlobalPlatform 3	
Secure channel protocol	GlobalPlatform 4 SCP03 i=15	
Confirmation counter	0	

Back to Content

5. Security Domains

Back to Content

6. Applets

Back to Content

7. Packages

Back to Content
