Direct Debit Transactions: a comprehensive analysis of emerging attack patterns

Luigi Coppolino†, Salvatore D'Antonio†, Luigi Romano†, Gaetano Papale†, Luigi Sgaglione†
†University of Naples "Parthenope"
{luigi.coppolino, salvatore.dantonio, luigi.romano, gaetano.papale, luigi.sgaglione}@uniparthenope.it
and
Ferdinando Campanile†
†Sync Lab S.r.l
{f.campanile}@synclab.it

***Abstract*—In the recent years payment systems in Europe are evolved to a new scenario where transactions and retail payments take place according to the SEPA (Single Euro Payments Area) Regulation. SEPA is an initiative of the European banking industry aiming at making all electronic payments across the Euro area – e.g. by credit card, debit card, bank transfer or direct debit – as easy as domestic payments currently are. One of the payment schemes defined by the SEPA mandate is the SEPA Direct Debit (SDD) that allows a creditor (biller) to collect funds from a debtor's (payer's) account, provided that a signed mandate has been granted by the payer to the biller. Thanks to SDD consumers can make and receive no-cash euro payments with a single set of instructions and a single bank account. It is apparent that the use of this standard scheme facilitates the access to new markets by enterprises and public administrations and allows for a substantial cost reduction. However, the other side of the coin is represented by the security issues concerning this type of electronic payments. A study conducted by Center of Economics and Business Research (CEBR) of Britain, on behalf of Liverpool Insurance Company, showed that from 2006 to 2010 the Direct Debit frauds have increased of 288%. In this paper a comprehensive analysis of real SDD data provided by the EU FP7 LeanBigData project is performed in order to identify and classify emerging and sophisticated attack patterns that can be executed against an SDD service. The results of this data analysis will be used to inspire the design of a security system supporting analysts to detect Direct Debit frauds.**

I. Introduction

Payment systems are in rapidly evolution. And so is for the payment frauds. Whenever a new payment method is introduced, the fraudsters try to take advantage from loopholes and security weaknesses that each novel system brings with it. In this scenario the European Union has developed the Single Euro Payment Area (SEPA), where 500 million of citizens, businesses and the European Public Authorities can make and receive over 100 billion no-cash payments every year [1]. SEPA Direct Debit (SDD) is a service that allows consumers to make in euro payments using a single bank account and a single set of instructions. A common standard, if on one hand translates into efficiency gains for businesses and public administrations, facilitating access to new markets and reducing costs, on the other hand, the simplification of the payment process increases the risks for the users. The SDD service is not free from cybercrime attacks. A study conducted by Center of Economics and Business Research (CEBR) of Britain, on behalf of Liverpool Insurance Company, showed that from 2006 to 2010 the Direct Debit frauds have increased of 288%, with an expected growth of 57% for the next three years [2]. The magnitude of these evidences is related to the lack of knowledge on the part of financial institutions with respect to the types of threats that an attacker can put in place. The research presented in this paper have as goal the analysis and identification of emerging attack patterns against the Direct Debit transactions. Our work is been driven from the study of real SDDs provided by an Italian bank. This data are properly filtered and anonymized by the fraud analyst of the institute. The paper is organized as follows. Section II presents the works found in literature that approached to the issues in SDD payments and electronics ones. In the Section III an in-depth analysis of the SEPA standard and an accurate description of the phases to set-up a Direct Debit transaction is presented. Particular emphasis is given to the almost absence of security mechanisms that a financial institution puts in place to protect his/hers users due to unauthorized or fraudulent SDDs. Section IV, starting from the information reported in the previous sections, analyzes the hazards of the SDD process due to the adoption of Creditor Mandate Flow Model (CMF). Section V proposes a categorization, in four misuse cases, of attacks that a fraudster can put in place against an unaware SDD's user. To this aim, we have analyzed a huge amount of real SDD data, over than 2TB of real data, provided by SincLab S.r.l within the European LeanBigData project. Finally, Section VI concludes the work showing future research directions.

II. Related work

The Direct Debit frauds are a modern topic in the scientific community and, at the beginning of our work, we were aware that no literature concerning this argument was available. However, several are the publications relating the detection of threats against other forms of electronic payment. In [3] [4] the authors describe the advanced cyber threats, specifically targeted to financial institutions and propose an approach based on combining multiple and heterogeneous data to detect frauds against a Mobile Money Transfer (MMT). The research presented in [5], denotes that in real life fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. The work present a survey of various techniques (Data mining, Fuzzy logic, Machine learning...) used in credit card fraud detection. In [6] is showed that the frauds tend to be perpetrated to certain patterns and the

use of Neural Network to detect fraudulent transactions is presented. The paper [7] suggests a novel combination of the two well known meta-heuristic approaches, namely the genetic algorithms and the scatter search to detecting credit card frauds. The method is applied to real data and very successful results are obtained compared to current practice. The research presented in [8] proposes an analysis of the identity theft and the related crimes. In the SDDs analysis are been fundamental many publications of European Payment Council (EPC). In particular [9] defines the SEPA Direct Debit Scheme (SDD-Core), rules and the obligations. The work [10] presents a review of the SEPA evolution and a discussion on the ISO-20022 XML standard, the types of national or regional Additional Optional Service and the different clearing practices associated with these. Finally, for the future developments of this work, very interesting are the results presented in [11] where the authors propose and demonstrate the applicability of a visualization support in a Big Data banking use case.

III. SEPA Direct-Debit transactions

SEPA is the area where citizens, businesses, governments and other economic actors can make and receive in euro payments [12]. The jurisdictional of the SEPA scope currently consists of the 28 EU Member States [13], the members of European Free Trade Association-EFTA (Iceland, Liechtenstein, Norway and Switzerland), plus Monaco and San Marino. The goal of the SEPA project includes the development of financial instruments, standards, procedures and infrastructures to enable economies of scale. This paper is focused on SEPA Direct Debit transactions (SDDs), one of the services provided by SEPA. Typical examples of SDD transactions are services that require recursive payments such as pay per view TV, gym subscription and energy distribution. The actors involved in an SDD transaction are:

- **Creditor**
  In the SEPA Direct Debit (SDD) schema is the person or company who has a credit that will be satisfied by collecting funds from the Debtor's bank account through an SDD transaction.
- **Debtor**
  In the SEPA Direct Debit (SDD) schema is the person or company who has a debit that satisfies by providing funds from his/her bank account to the Creditor's bank account by means of an SDD transaction.
- **Creditor's and Debtor's banks**
  Represent the respective banks of Creditor and Debtor.

When a Creditor must draw funds from another person's bank account, to set up the process, he/she has to acquire an SDD mandate from Debtor and advise his/her bank about it. During each transaction, the Creditor sends a direct debit request (with information about the amount of the transaction) to his/her bank that will start the process to request the specified amount from Debtor's bank account. The Debtor must provide only the signature of the mandate, but has no prior acknowledgement about the direct debit being in charge to his/her bank account. Usually, the Creditor send a receipt to the Debtor by using a best effort service, so no guarantee about delivery time and delivery itself is provided. In this process, the Debtor will have knowledge

[scale=0.28]SDD2.eps

Fig. 1: **SEPA Direct Debit process**

of an unauthorized direct debit only when the funds have already been withdrawn and after reception of his/her bank statement. This of course exposes the Debtor to a large number of possible frauds. For these reasons, with SEPA, in case of unauthorized transactions due to errors or frauds, a Debtor can request refund until 8 weeks from the SDD deadline or 13 months in case of an unauthorized SDD. The SDD process (figure 1) is characterized by the following steps:

- **Acquisition**

1) The mandate is signed by the Debtor and is notified to the Creditor Bank.

- **Validation**

1) The Creditor Bank sends a validation request for the received mandate to the Debtor Bank.
2) The Debtor Bank receives the validation request and returns its validation.

During this step is checked the validity of Debtor Bank coordinates.

- **SDD Request**

1) The Creditor generates a receipt at least 14 working days before its deadline.
2) The Creditor sends an SDD request to its bank (at least 11 working days before in case of first SDD request, 9 for subsequent requests).
3) The Creditor Bank sends an SDD request to the Debtor Bank which checks the correctness of the request and if no problem occurred, the bank debits the SDD on Debtor's account.

- **Interbank clearing**

1) The Debtor Bank communicates the result of SDD request to the Creditor Bank.
2) In case of positive response, the Creditor Bank credits the amount of the transaction on Creditor's account.

The standard adopted by SEPA to compose SDD requests is the ISO 20022 [14] [15], a multi-part International Standard performed by ISO Technical Committee TC68 Financial Services. It defines a modelling methodology to capture in a syntax-independent way financial business areas, business transactions, and associated message flows. Also, it sets a central dictionary of business items used in financial communications and fixes a set of XML and ASN.1 design rules to convert the message models into XML or ASN.1 schemas, whenever the use of ISO 20022 XML or ASN.1-based syntax is preferred. In Italy, from the 1st of February 2014, domestic credit transfers, banking and postal direct debits (RIDs) were replaced by the corresponding SEPA instruments. The SEPA standard adopted by Italy is slightly different from the canonical one (ISO 20022). In particular, for the SDD request, the "CBIBdySDDReq.00.01.00" standard which is provided by

the Interbank Corporate Banking (CBI) consortium, is used. In listing 1 an excerpt of real SDD's data is shown. It contains the information of the Creditor. The "Id" field represents the Creditor Identifier [16] on 23 digits. In particular, from digit 8 to digit 23 is defined the VAT number of the company.

```
<Cdtr>
 <Nm>xxx yyyyy</Nm>
  <PstlAdr>
        <TwnNm>xxxxx yyyyy zz</TwnNm>
        <Ctry>Italia</Ctry>
        <AdrLine>via numero xx</AdrLine>
  </PstlAdr>
        <Id>
          <PrvtId>
            <Othr>
               <Id>ITXXX100000008570720YYY</Id>
            </Othr>
          </PrvtId>
        </Id>
</Cdtr>
   <CdtrAcct>
     <Id>
       <IBAN>ITXXX000000000200000YYY</IBAN>
     </Id>
   </CdtrAcct>
```

Listing 1: **Excerpt of Creditor's data in ISO 20022 format**

An analogous structure is used to the Debtor, but the "Id" field is on 16 digits and represents the fiscal code of the user. In the real data that we have analyzed, every ISO 20022 xml file contains a trace of purpose of the transaction (i.e gym or pay-tv subscription) within the field "Ustrd".

IV. Issues in SEPA transactions

The SEPA Direct Debit transactions, as any other form of electronic payment, are not immune from attacks of fraudsters. At the basis of each SDD fraud there is an "Identity Theft", either the Debtor's identity or the Creditor's identity. Identity Theft is a relatively new phenomenon for which there is no universally recognized definition, but overall can be defined as a crime where someone:

"knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation law ..." [17].

The major weakness of the SEPA Direct Debit process is at the beginning of the procedure, in particular during the phase of signing the mandate. In fact, as shown in figure 2, a fraudster can authorize the SDD mandate in the place of the Debtor. This illegal activity, also known as "Mandate Fraud", allows to benefit products or services without paying for it, while the Debtor will recognize the fraud after the direct debit was performed. The management of the mandate can follow two different models:

- **CMF** - Creditor-driven Mandate Flow
- **DMF** - Debtor-driven Mandate Flow

CMF provides that the mandate is stored with the Creditor and it is the unique model in four European country (Germany, Spain, Netherland and UK). DMF, unlike the previous,

[scale=0.35]Mandate.eps

Fig. 2: **Mandate Fraud**

provides that the mandate stays with the Debtor's bank and is adopted in Finland, Greece, Malta, Slovenia, Slovakia, Hungary, Latvia and Lithuania. In Italy and in the remaining countries of SEPA area, CMF and DMF co-exist, but the European Policy Centre (EPC) has unilaterally decided that the SEPA model would be based on CMF. The same European Consumers Organization (BEUC), through a letter to the members of European Parliament (MEPs) dated 25 January 2010, has raised the issue by defining SEPA's Creditor Mandate Flow Model (CMF) "massively open to fraud". With the CMF model, the consumer's bank (i.e. Debtor's bank) does not have control over the mandate, so the risk of fraud is higher [18]. This model prevents the Debtor's Bank from intervening once a payment has left an account, with the consequence that the Creditor is in full control of the transaction. Furthermore, the reduced amount of information required to activate a transaction, allow even to the less savvy criminals to perpetrate a fraud. The precondition of an SDD fraud is an identity fraud. There are different techniques to steal personal information of the victim, as reported in [19], several that don't need high technical expertises (i.e. Dumpster Diving) and other more sophisticated (i.e. Spoofing and Spamming).

V. Four misuse cases

In this section will be described four misuse cases in the SDD transactions. The classification was conducted in order to develop, in future, a support system to recognize SDD frauds with an high detection rate and a low occurrence of false-positives. To categorize the frauds, we have examined a huge amount of real data thanks to collaboration with Sync Lab S.r.l. [20], an Italian SME that manages for his clients over 4 million of direct debit transactions per day. This data have been obtained within the LeanBigData project [21], where Sync Lab figures as a partner. LeanBigData is an European project that has as goal the building of an ultra-scalable and ultra-efficient integrated big data platform addressing important open issues in financial, cloud data and social media big data analytics. Through the analyze of real data , over 2 TB of transactions properly anonymized and, from the observation of different attack patterns, we have extract four misuse cases related to an SDD fraud. The misuse cases will be schematized with indications about the actors involved in the fraud, the preconditions to perpetrate it, a description of the misuse case and the fraudster's goal. To allow a better understanding of the misuse cases, it is appropriate to divide the services that can be connected to an SDD transaction into two categories:

- location-independent
- location-bound

The "location-independent" category identifies services that can be provided in any location and therefore do not require the physical presence of the Debtor (i.e. pay-per-view, smartphone fee) while, the term "location-bound" indicates all services necessarily provided in a specific place and required the physical presence of the user, for example the

gym subscription.

Misuse case 1: Location-independent Service Fraud

- **Actors:** Debtor, Creditor and Fraudster.
- **Objective:** The goal of the Fraudster is to benefit of a service without pay for it.
- **Preconditions:**

1) The Fraudster steals Debtor's identity.
2) The Fraudster signs a mandate for a "location-independent" service in stead of legitimate user.

- **Description:**

1) The Fraudster, impersonating a Creditor, requests a direct debit on the Debtor's account for a "location-independent" service.
2) The Fraudster, to activate the SDD process, signs the mandate with the stolen identity of the Debtor.
3) The Debtor's bank, once verified the correctness of the data into SDDs, transfer the cost of the service from Debtor's account to the account selected by the Fraudster.

Misuse case 2: Location-bound Service Fraud

- **Actors:** Debtor, Creditor and Fraudster.
- **Objective:** The goal of the Fraudster is to benefit of a service without pay for it.
- **Preconditions:**

1) The Fraudster steals Debtor's identity .
2) The Fraudster signs a mandate for a "location-bound" service in stead of legitimate user.

- **Description:**

1) The Fraudster steals the identity of a Creditor and, by using such identity, requests a payment for a "location-bound" service to the unaware Debtor.
2) The Fraudster, to activate the SDD transaction, signs the mandate with the stolen identity of the Debtor.
3) The "location-bound" service provided by Fraudster has a location of use very far from usually places visited/lived by the Debtor.
4) The Debtor's bank, that has the duty of checking only the format validity of personal and banking data of the actors, validates the transaction.

Misuse case 3: Address Spoofing Fraud

- **Actors:** Debtor, Creditor and Fraudster.
- **Objective:** The goal of the Fraudster is to gain money.
- **Preconditions:**

1) The Fraudster steals Debtor's identity .
2) The Fraudster signs a mandate for a service equipment in stead of legitimate user.

- **Description:**

1) The Fraudster steals the identity of a legitimate Creditor and, with the stolen identity, requires a direct debit to an unaware user for a service equipment.
2) The Fraudster, to activate the SDD transaction, signs the mandate with the stolen identity of the Debtor.
3) The Fraudster sets as equipment's receiving address one that he can easily have access to, but different from real Debtor's address.
4) The Debtor's bank accepts the SDDs because it controls only the correspondence between name and bank details of Debtor.

Misuse case 4: Fake Company Fraud

- **Actors:** Debtor and Fraudster.
- **Objective:** The goal of the Fraudster is to gain money.
- **Preconditions:**

1) Fraudster and Creditor are the same actor.
2) The Fraudster steals Debtor's identity.
3) The Fraudster signs a mandate for a service in stead of legitimate user.

- **Description:**

1) A fake company, registered as biller for SDDs, requires a direct debit for a service to an unaware Debtor.
2) The Fraudster, to activate the SDD transaction, signs the mandate with the stolen identity of the Debtor.
3) The Debtor's bank, that is not able to verify the reliability of Creditor, accepts the SDDs.

VI. Conclusion

In this paper we discussed of the new SEPA Direct Debit standard adopted by the European Union to transfer funds within its economic area. From an in-depth study of the Direct Debit process, many safety risks for user's money emerged. In this context, only a strong understanding of the fraud strategies, can indicate the best countermeasures. Our work, starting from real SDDs data, presented an analysis of emerging attack patterns against Direct Debit transactions and it has categorized them in misuse cases. The classification is been conducted in order to ensure an high detection rate and a low occurrence of false-positives. In future, we plan of develop a tool that by correlating attack symptoms in near real time, as done in [22] [23], can recognize ongoing frauds and support the fraud analysts.

Acknowledgment

The research leading to these results has received funding from European Commission within the context of Seventh Framework Programme (FP7/2007-2013) for research, technological development and demonstration under Grant Agreement No. 619606 (Ultra-Scalable and Ultra-Efficient Integrated and Visual Big Data Analytics, LeanBigData Project). It has been also partially supported by the "Embedded Systems in critical domains" POR Project (CUP B25B09000100007) funded by the Campania region in the context of the POR Campania FSE 2007-2013, Asse IV and Asse V and by

the TENACE PRIN Project (n. 20103P34XC) funded by the Italian Ministry of Education, University and Research. The authors also wish to thank Mr. Giuseppe Trincia for the fruitful technical discussions.

REFERENCES

[1] EPC. Euroland: Our single payment area! [Online]. Available: http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/euroland-our-single-payment-area/sepa-whitepaper-0520021pdf/

[2] Direct debit fraud at an all-time high; bacs challenges figures. [Online]. Available: http://www.finextra.com/news/fullstory.aspx?newsitemid=22028

[3] L. Coppolino, S. D'Antonio, V. Formicola, C. Massei, and L. Romano, "Use of the dempster–shafer theory to detect account takeovers in mobile money transfer services," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–10, DOI:10.1007/s12 652–015–0276–9.

[4] L. Coppolino, S. D'Antonio, L. Romano *et al.*, "Use of the dempster–shafer theory for fraud detection: The mobile money transfer case study," in *Intelligent Distributed Computing VIII*. Springer, 2015, pp. 465–474.

[5] S. B. E. Raj and A. A. Portia, "Analysis on credit card fraud detection methods," in *Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on*. IEEE, 2011, pp. 152–156.

[6] R. Patidar, L. Sharma *et al.*, "Credit card fraud detection using neural network," *International Journal of Soft Computing and Engineering (IJSCE) ISSN*, pp. 2231–2307, 2011.

[7] E. Duman and M. H. Ozcelik, "Detecting credit card fraud by genetic algorithm and scatter search," *Expert Systems with Applications*, vol. 38, no. 10, pp. 13 057–13 063, 2011.

[8] S. F. Allison, A. M. Schuck, and K. M. Lersch, "Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics," *Journal of Criminal Justice*, vol. 33, no. 1, pp. 19–29, 2005.

[9] EPC. Sepa core direct debit scheme rulebook. [Online]. Available: http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/sepa-direct-debit-core-rulebook-version-81/epc016-06-core-sdd-rb-v81-approvedpdf/

[10] R. Wandhöfer, "Sepa for corporates: On the path towards cross-border harmonisation," *Journal of Payments Strategy & Systems*, 2015.

[11] L. Coppolino, S. D'Antonio, L. Romano, F. Campanile, and A. V. de Carvalho, "Effective visualization of a big data banking application," in *Intelligent Interactive Multimedia Systems and Services*. Springer, 2015, pp. 57–68.

[12] L. D. Andrei and P. Brezeanu, "Single euro payents area (sepa) - strategic value on the high degree of interoperability for all active participants in the financial transaction," 2014.

[13] EPC. Epc list of sepa scheme countries. [Online]. Available: http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/epc-list-of-sepa-scheme-countries/epc409-09-epc-list-of-sepa-scheme-countries-v21-june-2015pdf/

[14] S. Goswell, "Iso 20022: The implications for payments processing and requirements for its successful use," *Journal of Payments Strategy & Systems*, vol. 1, no. 1, pp. 42–50, 2006.

[15] Iso 20022: Universal financial industry message scheme. [Online]. Available: http://www.iso20022.org/

[16] EPC. Creditor identifier overview. [Online]. Available: http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/creditor-identifier-overview/epc262-08-creditor-identifier-overview-v40/

[17] K. M. Finklea, *Identity theft: Trends and issues*. DIANE Publishing, 2010.

[18] BEUC. Establishing technical requirements for credit transfers and direct debits in euro and amending regulation (ec) no 924/2009. [Online]. Available: http://www.beuc.eu/publications/2011-00202-01-e.pdf

[19] M. P. Pardede and T. Dewi, "E-fraud, taxonomy on methods of attacks, prevention, detection, investigation, prosecution and restitution," 2013.

[20] Sync lab s.r.l. [Online]. Available: http://en.synclab.it/

[21] Leanbigdata project. [Online]. Available: http://leanbigdata.eu/

[22] L. Coppolino, S. D'Antonio, L. Romano, and G. Spagnuolo, "An intrusion detection system for critical information infrastructures using wireless sensor network technologies," in *Critical Infrastructure (CRIS), 2010 5th International Conference on*. IEEE, 2010, pp. 1–8.

[23] M. Ficco, A. Daidone, L. Coppolino, L. Romano, and A. Bondavalli, "An event correlation approach for fault diagnosis in scada infrastructures," in *Proceedings of the 13th European Workshop on Dependable Computing*. ACM, 2011, pp. 15–20.