ThreatMark

PSD2 Whitepaper

12.17.2018 Petr Grobelný

1. PSD2 Objectives

The new payments service directive, which was adopted by the EU parliament in October 2015 and will come fully into force by September 2019, set out to enhance three major areas in the payment landscape: customer protection, innovation, and security.

Security is being supplemented mainly by the Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and common and secure open standards of communication (CSC). The main objectives are:

- Strong Customer Authentication
- Transaction and Device Monitoring
- Provision of standardized and secure interface for access to payment accounts (e. g. API)

Innovation in the payment landscape is fostered mainly by introducing and regulating new market players, also known as third-party providers, who gain direct access to customers' payment accounts to provide services related to account information, payment initiation, and issuance of card-based payment instruments.

PSD2 also tipped the scales in favor of customers in the area of unauthorized and fraudulent transactions. The customers will still be held liable if acting in a grossly negligent or fraudulent manner, however, they are better protected in the following situations:

- Unauthorized payment – a customer (the payment service user) has to be refunded immediately.
- Misuse of a payment instrument, provided that the customer could not have been aware of it (e. g. copied payment cards, hack attacks, data breaches).
- Loss of a payment instrument provided that the customer has notified the payment service provider.

2. The ThreatMark Solution

ThreatMark's Anti-Fraud Suite (AFS) was developed with PSD2 in mind by security practitioners with uniquely extensive knowledge of online systems security, mainly in banking. It is therefore logical that the solution can solve all the demanding security requirements set out by the Regulatory Technical Standards (RTS) as presented above.

Combining evidence-based detection of cyber threats (such as financial malware and phishing), deep device profiling, user behavior biometrics analysis and transaction analysis, all in real or close to real time, the solution is a perfect fit for transaction and device monitoring, transaction risk analysis, and even for the multi-factor authentication requirements set out by the RTS.

3. How ThreatMark Delivers Compliance

The assessment below links the ThreatMark solution's features to specific RTS requirements, demonstrating clearly how the compliance is achieved.

3.1. Behavioral Biometrics as an SCA Factor

The Article 4 of the RTS states:

> *"Where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication shall be based on two or more elements which are categorized as knowledge, possession and inherence and shall result in the generation of an authentication code."*

The same article further clarifies that the SCA must be used when the payer:

> *(a) accesses its payment account online;*
> *(b) initiates an electronic payment transaction;*
> *(c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.*

These requirements mean that payment service providers are now facing the dilemma of a choice between secure authentication (as required by the SCA) and not jeopardizing customer experience, one of the key factors when using a payment service. The dilemma can be solved by using behavioral biometrics as the inherence factor of the SCA (clarified by the European Banking Authority in their "*Opinion on the implementation of the RTS on SCA and CSC*", paragraph 34).

Behavioral biometrics is a subcategory of biometrics data gathered passively, by monitoring how a person interacts with the interface (laptop, mobile phone). Data collection is performed unobtrusively in the background.

ThreatMark can gather very granular technical data across end-user devices and monitor users' behavior during their entire online sessions. The data does not consist only of actual user activities (logging in to the application, navigation to a specific page, transaction checkout, etc.) but also of information that characterizes the user as a human being (such as mouse movements, typing on a keyboard, touch events).

Such a set of information represents the behavioral biometry which can, with reasonable amount of data and proper processing, uniquely characterize a user.

3.2. Transaction Monitoring Requirements

Article 2 of the RTS states:

> *"Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorized or fraudulent payment transactions."*

The same article specifies the minimum risk-based factors that a provider has to monitor to comply with the requirement. To each of them, we added the main features of the AFS solution that cover it:

> *Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:*
> *(a) lists of compromised or stolen authentication elements (such as a password or mobile device);*

Above mentioned requirements can be fulfilled with these ThreatMark functionalities.

Insecure software configurations

AFS keeps track of all users' devices used to access the internet banking application, including portable devices. For each device, it checks software components such as OS type and version, various frameworks types and versions (.NET), browser plugins (Flash, Java, Silverlight) including versions. These configurations are compared with the database of known vulnerabilities, and the risk of user infection is calculated.

AFS also checks the networks from which a user accesses the internet banking. Network categories include known blacklisted attacker networks, anonymous proxy and TOR, and also secure networks with a proven history. Access from suspicious networks with new IP addresses are considered risky.

All this collected information together with many other parameters (browser language, resolution, available functions, etc.) form a unique device ID that is useful in detecting various attacks.

Insecure mobile device configurations

It is important to keep mobile devices secured the same way as desktop computers. AFS can detect the following vulnerabilities:

- Outdated OS and applications versions
- Risky updates and other changes to the OS (rooted Android, jailbroken iOS)
- Insecure network usage
- Man-in-the-middle attacks – attempts to eavesdrop on the communication between a mobile application and a server
- Certificate issues during communication securing

Behavioral biometrics

Behavioral biometrics can identify anomalies in user behavior by analyzing the way a user interacts with the application, then revealing whether the analyzed identity matches that of a legitimate user, or a likely fraudster. The method is especially useful when authentication elements get stolen through social engineering or other applications (unrelated to the protected application).

(b) the amount of each payment transaction;

ThreatMark answer: AFS monitors the transaction amount and compares it with previous spending behavior. Parameters considered include amount, frequency, time, and other user-entered values.

All transactions are evaluated against various models. Each model includes a group of rules corresponding to a transaction type, the channel used, etc. However, AFS detection does not rely on the rules only – it uses advanced machine learning with human feedback that can adapt to new fraudulent scenarios not covered by the rules.

(c) known fraud scenarios in the provision of payment services;

ThreatMark answer: AFS detects fraudulent scenarios such as phishing campaigns, social engineering, account takeover, and session hijacking.

Phishing detection

AFS has advanced phishing detection capabilities which can identify legitimate web pages being copied by an attacker or even report phishing victim users who provided their credentials.

Mobile phones are protected mainly from overlay and SMSishing which the fraudsters use to gain users authentication factors.

Social engineering attacks detection

The combination of scripted access detection and behavioral biometry can prevent almost all forms of social engineering. This is the past and, more importantly, the future of fraudulent schemes, as attackers are forced into social engineering attacks because of continually stricter security measures.

The ability to detect social engineering attacks is one of the greatest advantages of the AFS over any similar system currently available on the market.

Account takeover

Regardless of the attack vector used (phishing, man-in-the-browser malware, social engineering or other), the attacker will eventually try to log in to the application and perform a criminal activity, and that is where AFS stops them, able to recognize that this is not the legitimate user.

AFS monitors interactions of external actors (users, bots, hackers) with form fields, buttons and other page elements, page navigation anomalies, application usage habits, mouse and keyboard usage, swipe behavior biometry, actions and payment transaction context. All this is continually analyzed and compared to the user's behavior during several previous sessions. If a new session is evaluated as anomalous, that is, considerably different from the previous ones, an alert is raised and the user and all their further activity in the current session (a transaction, for example) are assigned higher risk levels.

Session stealing

Session stealing is a subcategory of the account takeover attack. The core aspect of the session stealing detection is identifying new access within the same session with unexpected parameters (location, language code, location switch in a short time, etc.). Moreover, AFS is able to detect session stealing even when an attacker uses the same device as the legitimate user (for example using VNC).

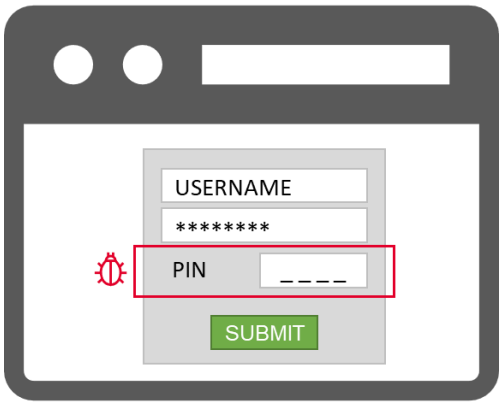
(d) signs of malware infection in any sessions of the authentication procedure;

ThreatMark answer: AFS can detect many types of malware-related attacks, for example:

- Bypassing second-factor authentication through mobile malware, offered to a user for download.
- Attempts to obtain user sensitive information (PIN, PUK, control questions, the password for other channels, OTP, etc.).
- Attacks occurring when an attacker waits for a user to perform legal transactions then modifies the outgoing values and edits the response to hide their changes.

To detect malware, AFS does not only check known signatures – it uses many other techniques like automated connections detection, overlay detection, and others.

One of the most common banking malware attack strategies during the past years has been **HTML injection** (man-in-the-browser attack). AFS observes and tests all data displayed by a browser or hidden in the application code. Its JavaScript component makes snapshots of a web page as a user can see it, then sends it to the analytical server as a data message and compares it with the original page that had been sent to the user from a web server. Any differences are tested automatically for a match to known malware signatures; positive detections are reported. Unknown detections are sent to fraud analysts for manual control. There are many known software components that inject HTML code (spyware, adware), so only a small number of detections is marked specifically as financial malware (this affects the risk score for user devices).



Other detection methods include monitoring of outgoing communication initiated by a browser, for example, AJAX calls. There have been reported cases of malware using this approach to communicate with their command and control servers.

Another type of attack covered by AFS uses **overlaying** the original content and blocking any action until the user performs an action required by the attacker, for example downloading mobile malware. AFS detects this kind of attack through its JavaScript component.

Zero-day malware detection is one of the unique features of the AFS solution. Unlike most competitors' products, it does not rely on signatures only. It tests every injection or code change and is, therefore, able to detect a new type of attack in a matter of hours. In some cases, it is even possible to identify the attacker before they start the campaign.

Another type of attack that can be prevented by AFS is **form grabbing**, used to steal user credentials. AFS uses selective application level encryption and message signing, which makes the intercepted passwords useless to the attacker. The feature also blocks attacks such as MiTM (man-in-the-middle) when common approaches fail for any reason (SSL/TSL).

(e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

ThreatMark answer: AFS constantly monitors the device, session, transactions, and user behavior – from the moment when a user accesses the application channels (such as the internet or mobile banking) to the moment when the session is terminated.

3.3. Transaction Risk Analysis

Transaction Risk Analysis (TRA) was introduced by the European Banking Authority (EBA) mainly as an additional exemption from the SCA, applicable when a transaction is white-listed, or the overall risk rate of a transaction is low. PISPs (Payment Initiation Service Provider) therefore can leverage this functionality in case they are able to do the analysis **in real time**, which can be challenging.

The AFS solution is able to analyze the risk parameters laid out in the Article 18 by monitoring and scoring all client activities in real time during the whole session. An excerpt from the article follows, with relevant AFS features filled in (added text in color):

Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.
(c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:
(i) abnormal spending or behavioral pattern of the payer;

ThreatMark answer: See section Transaction Monitoring Requirements, point (a), description of behavioral biometrics. In addition, AFS evaluates transaction details, such as the amount, source or partner account, transaction time, frequency, etc. to detect anomalies and differences from previously collected spending patterns.

(ii) unusual information about the payer's device/software access;

ThreatMark answer: See section Transaction Monitoring Requirements, point (a).

(iii) malware infection in any session of the authentication procedure;

ThreatMark answer: See section Transaction Monitoring Requirements, point (d).

(iv) known fraud scenario in the provision of payment services;

ThreatMark answer: See section Transaction Monitoring Requirements, points (b) and (c).

(v) abnormal location of the payer;

ThreatMark answer: AFS monitors usual locations and IP addresses and uses artificial intelligence to decide whether a location is suspicious. This includes advanced evaluation, not just simple observing of locations that a user has never logged in from before.

(vi) high risk location of the payee.

ThreatMark answer: A common list of countries that are considered high risk (defined by FATF) is used. AFS allows customers to define their own list, too.

3.4. Protecting the Authentication and Authorization Portal

Each communication session in which the authentication data is transmitted must be protected against data capturing or manipulation by unauthorized parties (RTS Article 4, 3(c)).

As mentioned previously, AFS possesses a unique set of features that include financial malware and phishing detection capabilities, deep device profiling, and user behavior biometrics analysis; in combination, these features can reveal fraudulent scenarios such as account takeover, financial malware, or session hijacking.

AFS is a powerful tool that can effectively protect online interfaces (web and mobile) that a payment service user enters their authentication data into.

3.5. Screen Scraping and How We Can Help

PSD2 also states that screen scraping/web scraping (using collected user credentials) will no longer be allowed once the transition period has elapsed and the RTS come fully into effect.

ThreatMark can detect scripted access and bot access by browser identification, tracking unusual use of mouse and keyboard, and monitoring the speed of navigation between pages, thus allowing you to stay compliant with the PSD2 requirements.

4. Recapitulation

ThreatMark AFS solution is a complex threat and fraud detection system which by nature is ready to address the transaction monitoring and transaction risk analysis requirements of the RTS along with protecting the integrity of the authentication/authorization portal a bank can use to perform an SCA of a request initiating from a third-party provider.

Its advanced user profiling based on behavior biometry can identify a returning user and as such can be used as one of the SCA factors or recognize a non-human like behavior which can detect a screen scraping activity ongoing on your page.