Trusteer

Trusteer’s Comments to “Recommendations for the Security of Internet Payments (April 2012)”

By the European Forum on the Security of Retail Payments SecuRe Pay

new threats, ***new thinking***

Table of Contents

About Trusteer and Our Role in Global Fraud Prevention

Trusteer is a leading[1] provider of financial fraud prevention solutions for the banking industry worldwide. Since its inception in 2006, Trusteer's anti-fraud solutions helped more than 200[2] banks protect tens of millions of end users against malware and phishing attacks. Indeed, "Man-in-the-Browser" and "Man-in-the-Middle" malware represent a major online banking fraud risk, and also enable other forms of cross-channel fraud based on data harvested by cybercriminals.

Trusteer welcomes regulatory guidance and best practices that will lead to improved fraud prevention. Prescribing sound principles and focusing on the end goal of preventing fraud (as opposed to specific measures and technologies) establishes a lasting framework that can accommodate changes in the threat landscape and the evolution of fraud prevention capabilities.

Trusteer has unique visibility into massive amounts of fraud-specific intelligence gathered by its network of tens of millions protected endpoints. We continuously publish our findings in a public blog (www.trusteer.com/blog) and are considered a world-leading authority on fraud tactics and methods.

Trusteer's service is built on global fraud intelligence platform, a dedicated malware research organization and architecture designed for instant adaptation to emerging threats. Using these capabilities, Trusteer is able to achieve **sustainable fraud prevention** that has withstood the test of time, the rapid change in the threat landscape and is proven to prevent fraud[3].

Our customer success and proven fraud prevention track record make Trusteer uniquely qualified to provide valuable commentary to the European Forum on the Security of Retail Payments SecuRe Pay ("The Forum") on this important upcoming guidance document.

We hope you will consider our comments and suggestions for inclusion in the final version of the document. Trusteer supports the Forum in this important regulatory effort and welcomes any questions you may have about this document. We are also willing to engage in discussions with the Forum as applicable.

Regards,

Mickey Boodaei
Chief Executive Officer
Trusteer Ltd.

[1] Trusteer is positioned as Leader in the 2012 Gartner Magic Quadrant for Web Fraud Detection.

[2] Trusteer Customers include 7 out of the top 8 banks in the United Kingdom, 9 out of the top 20 banks in the U.S, 4 out of the top 6 banks in Canada, 2 out of the top 4 banks in Australia, large banks in the Netherlands and France and hundreds of other financial institutions in North and Latin America, the middle east and Africa.

[3] Synovous bank case study.

Specific Comments to Key Considerations (KC) and Best Practices (BP)

In the sections below we offer comments to the document. The convention used:

- Original text is quoted in Gray
- Suggested amendments are in **bold black**
- **Trusteer comments**: provide the rational for the change

Missing Elements in the Guidance

The following items are not directly addressed in the guidance as we believe they should be:

Mobile devices: Mobile devices are commonly used as transaction devices (to conduct internet payments) and as a security tool (to authorize transactions in other channels). Malware and phishing attacks target weaknesses in both contexts. The majority of attacks aim to bypass mobile devices as authorization devices (e.g. SMS one -time-password), because the availability of mobile payments is still limited. We therefore recommend that mobile fraud risk detection and mitigation is addressed in the final document Guiding Principles.

Page 5

> First, […] a regular **and frequent** assessment of the relevant risks is of utmost importance.

Trusteer comment: The frequency and timeliness of online risk assessment is a serious challenge to most PSPs. The velocity of these threats is not compatible with point-in-time assessments. PSPs should try to achieve near-real-time detection of emerging threats and establish processes to rapidly react to these changes.

> Second, as a general principle, the internet payment service provides by PSPs should be initiated by means of **secure** strong authentication.

Trusteer comment: Hardware tokens, SMS one-time-passwords and other forms of strong security controls have all been successfully attacked[4] by financial malware. Anti-malware solutions can help **secure** strong authentication against malware attacks by blocking MitB from launching social engineering attack on the end user.

Page 6

> Third, PSPs should implement effective processes for authorising transactions, as well as for monitoring transactions and systems in order to identify abnormal customer payment patterns, **malware infected devices and sessions**, and prevent fraud.

Trusteer comment: PSPs should detect **device and session infection** when evaluating **transaction risk** even if strong authentication was applied. Protecting end users from financial malware and/or preventing financial malware from attacking the browser will help ensure authentication is not compromised. Overall, by eliminating or disabling MitB malware, a large portion of financial fraud attempts can be eliminated at the source.

Recommendation 2: Risk Identification and Assessment

> **[new] 2.1 BP: PSPs should aim for near real-time and automated risk assessment process to ensure they can develop a timely response to changes in the threat landscape thus reducing the window of exposure for them and their customers.**

Trusteer comment: The damage caused by a malware attack campaign is inversely correlated to the speed of the mitigating response. PSPs must strive to improve their visibility to emerging threats, to enable them to respond on time to campaigns that are designed to exploit weaknesses in their controls. By the time fraud losses start to accumulate the damage is already done.

[4] Trusteer research has found several examples of MitB and phishing attacks bypassing strong security controls:

- Fraudsters bypass SMS based authentication by taking over victims' mobile SIM cards or installing malware on mobile devices that redirect SMS messages to fraudsters.
- Cybercriminals social engineer users into providing the one-time-password themselves: "fraudsters tricked users into entering a TAN"
- Malware adds a chat box to online banking sessions that enable fraudsters to portray themselves as "trusted banks representatives" and request users to perform any required strong authentication.
- Malware was used to trick users into disclosing their phone account details to the "bank". Later, the stolen data is used to authenticate with the phone carrier and take over the victim's phone line.

Recommendation 4: Risk Control and Mitigation

4.2 KC: Public websites and backend servers should be secured in order to limit their vulnerability to attacks. PSPs should use firewalls, proxy servers or other similar security solutions that protect networks, websites, servers and communication links against attackers or abuses such as "man in the middle" and "man in the browser" attacks. **PSPs should consider the deployment of endpoint anti-malware solutions that can prevent compromise of the web session from the end user browser to the PSP web site.**

Trusteer comment: Network solutions cannot effectively deal with Man-in-the-Browser malware, which is an endpoint threat. An endpoint security solution must be considered.

[new] 4.1 BP: PSPs should develop tools and capabilities to alert users before they submit their credentials to suspicious sites or known phishing sites while takedown is in progress.

Recommendation 6: Initial Customer Identification, Information

6.2 KC: PSPs should ensure that the prior information supplied to the customer contains specific details relating to the internet payment services. These should include, as appropriate:

– clear information on any requirements in terms of customer equipment, software or other necessary tools (e.g. **antivirus or anti-malware** software, firewalls)

Trusteer comment: Financial malware like Zeus, Spyeye and Torpig is designed to bypass antivirus solutions using zero-day, polymorphic variants. Antimalware solutions, like Trusteer, address this capability gap, and are proven to mitigate these threats[5].

[5] Trusteer performs periodic assessment independent evaluation of its solutions against financial malware.

Recommendation 7: Strong Customer Authentication

7.2 KC: Obtaining access to or amending sensitive payment data requires **secure** strong authentication **(i.e, authentication performed in a malware-free environment, or an environment that is secured against malware attacks).**

Trusteer comment: Hardware tokens, SMS one-time-passwords and other forms of strong security controls have all been successfully attacked[6] by financial malware. Detecting the presence of session and device malware infection in the context of the authentication or authorization must be included in the transaction risk scoring. Anti-malware solutions can help secure strong authentication against malware attacks.

7.3 KC: [amend] **PSPs should factor in the threat of MitB infected sessions into their risk scoring. Such indication implies a high risk of 3-D secure credentials loss.**

Recommendation 10: Transaction Monitoring and Authorization

10.1 KC: PSPs should use real-time fraud detection and prevention systems to identify suspicious transactions, for example based on parameterised rules (such as black lists of compromised or stolen card data), abnormal behavior patterns of the customer or the customer's access device (change of Internet Protocol (IP) address or IP range during the internet payment session, sometimes identified by geolocation IP checks, abnormal transaction data or e-merchant categories, etc.), **indication of malware infection in the session** and known fraud scenarios. The extent, complexity and adaptability of the monitoring solutions should be commensurate with the outcome of the fraud risk assessment

[6] See also footnote 4 for specific examples.

Trusteer comment: MitB malware uses the customer machine to automate fraud. In some cases, it harvests data such as credentials and token values used to perpetrate fraud from different machines. The challenge with the proposed approach for abnormal transaction detection techniques is that it ignores the "root cause" of most fraud (the malware). Looking at the symptoms and not the root cause creates a large number of "false positives", burdens the PSP customer support and the customers, and slows down the velocity of business. Detecting malware presence in the context of account access:

- Indicates the risk of immediate fraud through the user device
- Indicates risk of account credentials compromise that could lead to later fraud from a different device
- Can be done prior to transaction submission enabling early detection and prevention that is essential in "instant clearing" transaction settlement environments.

Malware detection can help prioritize manual transaction verification processes. It also enables automated fraud countermeasures against known attack tactics (for example, preventing "add payee" actions with malware infected devices).

Recommendation 11: Protection of Sensitive Payment Data

11.2 KC: [amend] the secure end-to-end channel should extend all the way from the keyboard to the browser and the networking interface to protect against endpoint threats such as MitB.

Trusteer comment: MitB malware uses the weak link, the end user device, to compromise credentials and other payment data such as payment card numbers and personally identifiable information (PII). Network protections have no impact on the ability of MitB malware to steal the user credentials directly from the end user device and browser session.

Annex 2: Security of the Environment Underpinning Internet Payments

Page 21 Top right

> As an additional step, the financial industry could promote the development of specific tools for carrying out financial transactions on the internet, such as secure customised browsers, **fraud prevention endpoint and server software**, operating systems, and authentication methods specifically designed to mitigate the risk of "man in the middle", "man in the browser" and "man in the application" attacks perpetrated via malicious code.

Trusteer comment: PSPs should balance risk and end user impact. Some approaches do not impact the user experience, while others (like custom browsers and hardware devices) force users to change the way they work. Risk-driven fraud prevention should determine what measure to use that matches the risk profile and has the least impact on end user experience.

Page 22 top left

> 4) Infected machine policies: defining specific security rules related to infected network-connected machines. Infected machines could, for example, host a "phishing" website or be part of a botnet, thus polluting the digital environment. Security rules in this sector could require internet service providers to disconnect compromised machines **or require PSPs to restrict access to sensitive application functions (i.e., add payee or transfer funds) and act to remediate the infection.**

Trusteer comment: Disconnecting infected machines (especially end user machines), may place a large burden on customers. By using infection prevention, malware removal software and malware detection capabilities on the server, it is possible to manage MitB risk without completely disabling end-user access.