From: Ed M. Scheidt
To: comment@fedpaymentsimprovement.org
Cc: Ed M. Scheidt
Subject: Response to FRB Payments System Improvement-Public Consultation Paper - Tecsec Response to FRB for Security and Safety
Date: Thursday, December 12, 2013 9:03:29 AM
Attachments: image003.png

Response to Federal Reserve Board (FRB) published “Payment System Improvement-Public Consultation Paper”

Ed Scheidt
C/Scientist
Tecsec Inc

A Technical Solution Provider

Response to FRB for Security and Safety questions:

Extract from Paper:

Desired outcome 5: The Federal Reserve Banks have collaborated, as appropriate, with the industry to promote the security of the payment system from end-to-end amid a rapidly evolving technology and threat environment. In addition, public confidence in the security of Federal Reserve financial services has remained high.

New ways of making payments and advanced fraud schemes and technologies present new risks and challenges to maintaining public confidence in the payments system. Maintaining the confidentiality of payment information from end-to-end, such as by preventing data breaches, is made more difficult as complexity and interconnectedness of networks have increased. The impact of a significant fraud event, cyber-attack, or natural disaster on the public’s confidence may adversely impact the flow of commerce that is increasingly electronic or “digital.”

Safety

Q17. Payment security encompasses a broad range of issues including authentication of the parties involved in the transaction, the security of payment databases, the security of software and devices used by end users to access payment systems, and security of the infrastructure carrying payment messages.

i. Among the issues listed above, or others, what are the key threats to payment system security today and in the future?

The security of payment databases is significant. The bulk of the reported breaches of personal information have been shown to be from data base attacks. This particular problem can be addressed immediately via the adoption of existing technology and standards, e.g., ANSI X9.73-2010. Move the protection to the data object itself, and this approach will result in an immediate improvement in the security with little impact on the existing infrastructure.

The security of software and devices used by end users to access payment systems can be addressed by a concerted effort to move participants to a standards based approach. There are existing technologies that can assist in providing the protection of software and devices. The appropriate use of cryptography can facilitate both the stability of application software and the devices upon which it executes.

The infrastructure carrying payment messages is heterogeneous, and it already exists as an open architecture, with security built into it. It is unlikely the infrastructure will be torn down or a major rebuild. As such, the advent of a new protective mechanism direction such as protecting the data itself may be independent of the infrastructure security and such as found in the transport layer or in concert with protection associated with the transport layer.

Another way exists to examine a direction or scope for future security within the payments environment. There are many responses that can be contributed, but perhaps three categories could be as effective:

1) Identity: who or what machine is initiating or receiving a payment. Identity is still a challenge even with many methods of authentication that are available. Before we can get into direction, we have security tools that can be related to identity, but costs, risks, legacy impact, user friendly, policy impact, something new -all add to a direction decision. Relatively new on the Identity front is biometrics with good and reserved results – biometrics are a closer security technology to relate the human to a machine. - A possible security direction. The smart card as a security token can be effective, but legacy issues with the payment environments can create a challenge. – A possible security direction. Mobile payments are on the scene, and Identity has surfaced. – What do the sensor capabilities of the mobile device offer that can be coupled to a payment environment and ensure the wanted transaction is consummated for the intended parties of the transaction – A possible security direction.

2) Protecting Content: Information and data associated with a payment may be protected within a secure channel or may be protected at the content/data level. Historically, content has used various security tools associated with channel protection – a security tool such as encryption is available for an encrypted channel between two or more parties to a transaction or payment. – An emphasis has evolved around SSL channels. However, the threat has surfaced against these channels, and a new direction must be considered that reexamines the computing & communications technologies with a broader role for

encryption. In addition to the channel for protection, data itself must be protected. – The channel protection can only extend to the transmission points, but data in storage or data within databases also needs protection. Encryption can be an effective security tool with available advances in object level, dynamic encryption.

3)   Denial of Services and Malware: the banking community must be able to continue business with the financial support infrastructure. The customer, whether at home or mobile, needs to work within their personal environment and be able to maintain a link to their financial environment. The threat to the information & communications chain between the customer, the various Internet ISPs', and financial back end is real. - A tiered approach to security can be a viable solution. Combining selected security tools for Identity, Protecting the channel, and Protecting Content can be a reasonable security direction. Interesting that security technologies are available, but new policy may be needed.

ii. Which of these threats are not adequately being addressed?

The ability currently exists to address all of these issues; the largest and most immediate is the data base/content protection issue. The current situation exists with policy which can be viewed as beyond the availability of a solution. It is more a matter of a decision to adhere to standards, both in policy and use.

iii. What operational or technology changes could be implemented to further mitigate cyber threats?

A significant improvement can be achieved by regulators demanding the deployment of EXISTING standards across the financial industry.

Q18. What type of information on threat awareness and incident response activities would be useful for the industry?

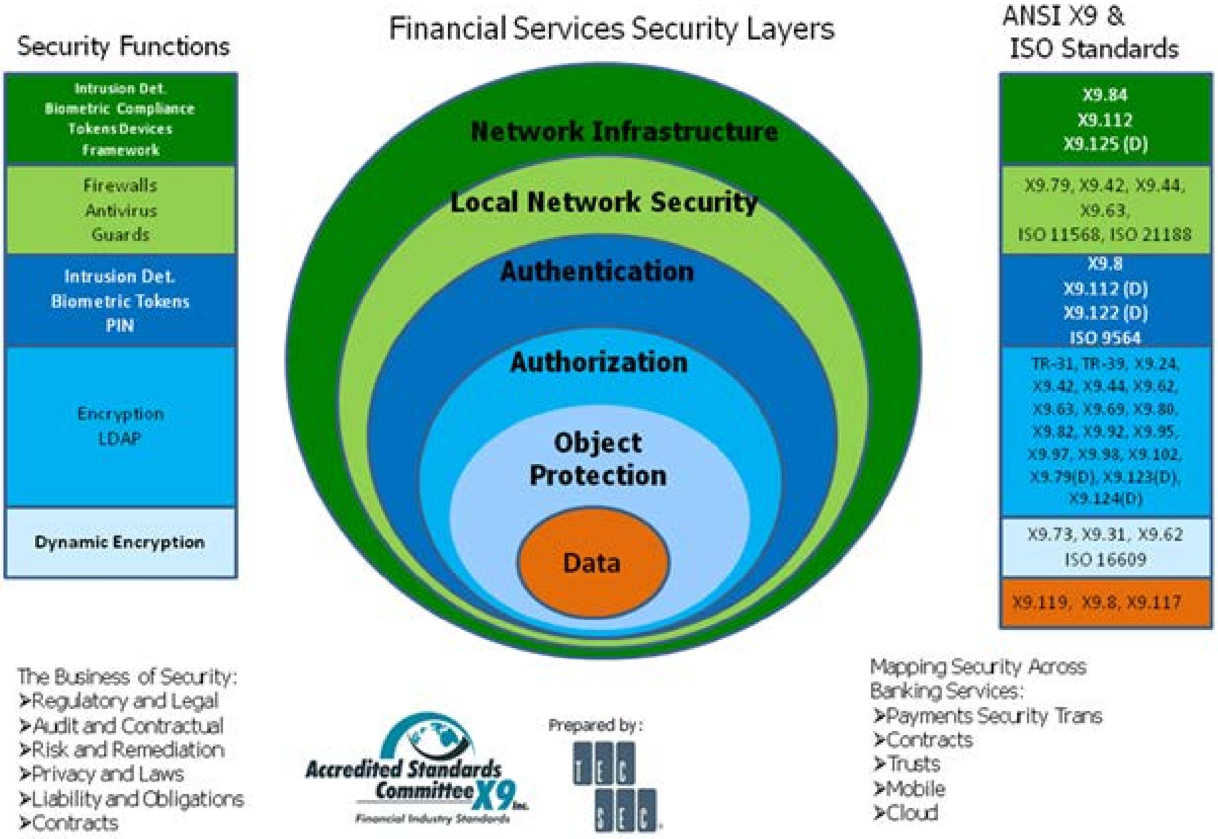
i. How should this information be made available?

The question seeks an answer to what type of information and access to threat information would be useful. – Sources of this information are varied including data in the public domain as well as data from the defense domain. Establishing trustworthy links that can respond in a timely manner and with relevant data is another challenge. Sources exist, but they may not be identified in a public phone book. The FED needs to ensure that their channels of threat data are real and effective.

Q19. What future payment standards would materially improve payment security?

The move to adopt existing security standards can be viewed as significant in itself. However, merely informing of a threat or a potential security problem may not be useful, or as effective as having the financial industry more supportive of a standards based solution, which leads to a decision, and resulting in a specific coordinated action.

The financial community looks to ANSI x9 for applicable security standards. Included is a framework of current security standards that illustrate the scope and potential applications for these standards.



These standards constitute much of the security tools that are implemented in the FED payment infrastructure. Another step can be expanding the security tools into solutions which may be further standardized. X9 looks to the financial community for direction. Time and costs are two challenges that have been associated with developing and implementing a standard. – A standard can be in development for more than a year, could have international implications, could be advancing a new security tool, and needs financial community support and consensus. Costs of a standard development are absorbed by the financial development participants. – There are instances of correlation of economic conditions and standard involvement.

i. What are the obstacles to the adoption of security-related payment standards?

The single largest obstacle to the adoption of standards is the will of the industry to mandate action.

Q20. What collaborative actions should the Federal Reserve Banks take with the industry to promote the security of the payment system from end to end?

Like the payment world, the security world has undergone changes, and it is anticipated that further changes are on the horizon. Parallel paths for formats and for payments can be reflected in a similar vain for security. Mobile and cloud usage is exploding. With these newer initiatives comes the concern for security. The threat just follows the new electronic avenues, sometimes with vengeance.

The emergence of Virtual Currency is an interesting phenomenon. The consumer's wanting to maintain anonymity like their experience with cash is vying with the financial infrastructure and computing technologies that are demanding levels of oversight. In the middle is security for the consumer which can be in questioned as the society chooses directions.

Collaboration is needed between industry and the FED to advance an end-to-end security solution. Within the diversity of the current technologies and the availability of many current infrastructures, applying various industry security solutions will be a norm. Putting emphasis on security standards is important, ensuring monetary policy includes security is important, and ensuring the political will of the consumer is included.

End