GMV PERSPECTIVE

XFS layer behaviour analysis

The last frontier in ATM protection

By Pedro Celis de la Hoz, Checker ATM Security Product Manager, GMV

Pedro Celis de la Hoz GMV

Security solutions for financial self-service networks have followed, as in nature, a process of natural selection. The continuous evolution of attacks on these networks has caused the development of counteractive measures to also follow a process of transformation and specialisation. Only those solutions capable of evolving agilely are saved from extinction. Antivirus is a good example of an endangered species, where only symbiosis with other solutions has saved it from total extinction.

Indeed, symbiosis between different solutions appears to be a successful strategy for achieving results in such a swiftly changing environment. After antivirus, there was white-listing, which needed disk encryption solutions to survive, and which later had to include keyboard and mouse control, followed by the blocking of USB storage devices. This process of development is not going to stop – the attacks continue evolving and so do the methods of protection.

The best way to anticipate the next evolutionary leap is by analysing the modus operandi of the latest attacks

Analyse past breaches to anticipate future ones

Given this situation, it is critical to anticipate the next evolutionary leap – and the best way to do this is by analysing the modus operandi of the latest attacks suffered in these networks, seeking in them some common patterns that can be used to inform the design of a new protection system.

Conclusions obtained from such studies indicate that attackers have greatly expanded their knowledge regarding their targets, especially everything related to the current security solutions, the initial objective of their attacks. Their first step in planning the hit is to look for any weaknesses in the protection's configuration or in its security policy. Such vulnerabilities occur naturally as a result of trade-offs made when balancing the needs of operating as well as securing the ATM. While the security policy seeks to block any remote or local access to the system, those responsible for operating and maintaining the network need to keep easy access to ATMs, remotely and locally, in order to guarantee availability of the ATM network. This creates weak spots, which are used by attackers to gain access to the system and subsequently to disable any installed protection.

So, assuming that such breaches will be exploited and malicious software will be executed within the operating system, the appropriate strategy for protecting against this type of attack, in which installed system protection is clearly not enough, would be to include a new barrier that protects the most critical system components. Once again, the symbiotic relationship between this new layer of security and the existing ones provides an effective, higher level of protection.

Using XFS behaviour analysis

If we analyse past attacks and strategies of criminals, we can define some basic requirements for a new security module. This module should be able to detect, among the processes that are running, those that are malicious, block their attack if possible, and alert a security operator of the situation.

With these requirements in mind, an effective solution would be to use software behaviour analysis technologies. These technologies can detect anomalous behaviour coming from malicious, or at least unknown, software running at the ATM. Software behaviour analysis is especially useful in well-known and stable execution environments, as is the case in ATM networks.

One important consideration when implementing proper behaviour analysis is the process of initial behaviour acquisition (behaviour learning). The broader that learning is, the better the results we will obtain. ATMs are generally suitable environments for this undertaking, owing to the availability of laboratories and good testing environments at almost every deployer.

Challenges are presented, however, by the great diversity of manufacturers, models, operating systems, software versions and components that can be found in the ATM network of a single deployer. Such complexity demands significant effort at the learning stage and is a major deterrent to the use of this type of technology.

In order to manage this complexity, it is expedient to focus on the most critical software components of the ATM and at the same time to look for any component that is standard among different manufacturers, models and operating systems. The XFS services layer meets these requirements; it is sufficiently standardised and widely adopted, it is the interface for accessing the critical components of the ATM and constitutes the entry point for all attacks pretending to be universal through the use of a public, well-known interface.

The use of a software behaviour analysis tool focused on the XFS layer thus eliminates the environmental complexity issue given its standard interface, and at the same time simplifies the process of behaviour learning owing to the reduced scope. Malware attacks produce strong anomalous signals that make their detection simple and reduce the number of false positives. For example, a jackpotting attack would be detected quickly when repeated requests for dispensing of high sums of cash occur outside the regular sequence of a transaction.

XFS services behaviour analysis is therefore an adequate mechanism to detect anomalies. At the same time, the XFS system is the most appropriate place to perform active blocking against any anomalous action. Returning to our jackpotting example, at the moment in which the behaviour analysis system detects an anomaly, it can decide to block all XFS access to the dispenser, preventing the attacker from retrieving the funds. This ability to block XFS commands can also be used as a 'panic button' to locally or remotely block the use of XFS devices.

By bringing together these three layers of protection: detection, blocking and alerting, we can talk about a real-time XFS filtering module, which works similarly to an intrusion prevention system. It would analyse each request to the XFS services using algorithms of behaviour anomalies detection, block all requests that are marked as anomalous, and finally report any anomaly to a central console.

By bringing together three layers of protection: detection, blocking and alerting, we can talk about a real-time XFS filtering module

Protection of XFS layer will be essential

This XFS filter, which may seem like the definitive solution to all ATM security needs, would not survive long on its own in the wild. Again, the filter needs a symbiotic relationship with the other security components deployed in this environment. These already-existing components must provide the additional protection measures that this new filter requires. This includes protection against any illegal attempts at removal or disablement; restricting direct access to any low-level component, known as 'services providers', and integrity validation of any XFS resource used.

Protection of the XFS layer may seem an excessive and intrusive mechanism, however GMV believes that in a short time it will become essential for the protection of ATM networks. Just as it happened with hard disk encryption, which once seemed unnecessary but today is considered a key protection mechanism to avoid 'off-line' alteration of ATM internal data, XFS protection, too, will become a critical component of any ATM security solution. ■

Protection of the XFS layer will soon become essential for the protection of ATM networks