Winning the Battle Against Internet Banking Fraud by Leveraging Real-Time Data and Application Integration

A Gravic, Inc. Case Study

Executive Summary

How many of us have received an email purporting to come from a bank or other financial institution, stating that due to "suspicious activity" or some such subterfuge, our account has been frozen until we click the URL in the message to "reset" our account? Of course, this will require divulging personal information such as our user ID, password, home address, etc. This information is then used by crooks to steal money or obtain further personal information, such as account numbers. This, of course, is an example of *phishing*, and it is a very lucrative enterprise tool. In the UK alone, unauthorised financial fraud losses from cards, remote banking, and checks totaled £783.8 million in 2020.[1] Globally, the cost is measured in the trillions of dollars annually. Email phishing is just one avenue; social hacks such as phone calls purporting to be from your bank and even computer viruses are other ways this information is obtained. Simply buying it is also an option. Cybersecurity firm Hold Security recently revealed that it discovered stolen credentials from some 360 million accounts available for sale on the dark web (the "underground internet").

With the information necessary to access online bank accounts so readily available, how is a bank to defend itself (and us) against this ever increasing threat? Moreover, not just defeat the fraud itself, but do so in such a way that enables prosecution and conviction of the perpetrators so they cannot simply do it again? Read on to learn how this goal has been successfully achieved by a major European retail bank.

One European Bank's Internet Banking Fraud Detection System

In the bank's home country, the laws regarding fraud and what constitutes a crime are very specific. Stealing a user ID and password, and then using that information to log in to a customer's internet banking account, while exhibiting an *intent* to commit fraud, is not necessarily criminal in and of itself. An actual *act* of fraud must be perpetrated, such as transferring money from the customer's account to another account, for the act to be criminal.

This fact necessitated the bank to design and implement its internet banking application (IBA) in a very specific way: to detect and prevent fraud, yet still enable the authorities to pursue a conviction against the actual actions committed. For example, simply denying a suspicious logon, while protecting the bank, would not provide sufficient grounds for prosecution.

The basic structure of the bank's internet banking and real-time fraud detection system is shown in Figure 1. The IBA runs on HPE NonStop servers. Changes made by that application to the banking database (primarily implemented using HPE NonStop SQL), are read from the HPE NonStop TMF audit trail by HPE NonStop Shadowbase data replication.[2]

HPE Shadowbase replication feeds the changes from the NonStop server via a TCP/IP connection to Shadowbase processes running on a Linux system. From there, customized user exit procedures running inside the Shadowbase processes structure the changes into a message format similar to a CSV file, and feed those messages via TCP/IP into a RiskShield® fraud detection application.[3] To facilitate low latency yet improve overall efficiency, changes are batched into groups of 50 and fed into RiskShield, or whenever a pre-determined timer expires if 50 changes are not received within that timeframe.

The RiskShield application contains a knowledgebase which allows it to detect and flag potentially fraudulent transactions (for example, User IDs whose credentials are known to have been compromised, known target accounts for fraudulent money transfers, etc.). Having analyzed the input messages (customer ID, source account, target account, amount, etc.), the RiskShield application returns a response to the IBA via a private connection, indicating whether or not the transaction is suspicious. The IBA then proceeds accordingly.

[1] Source: *Fraud – the Facts 2021* — UKFinance.org
[2] For more information, please visit ShadowbaseSoftware.com
[3] For more information, please visit Inform-Software.com/Products/Riskshield

The fraud detection system was cleverly designed, since it is architected to serve both the needs of the bank in preventing fraudulent transactions from completing, and in allowing the online activities of the criminals to proceed to the point where an actual act of fraud is committed, demonstrating actual, attempted fraud. After fraud is demonstrated, the transaction can be reversed. To accomplish this, the system splits the internet banking business activity into a series of steps (Figure 1), with each step comprising a separate database update (executed in the context of a single TMF transaction), up to a final "execute" step which will complete the business activity (commit or abort the TMF transaction).

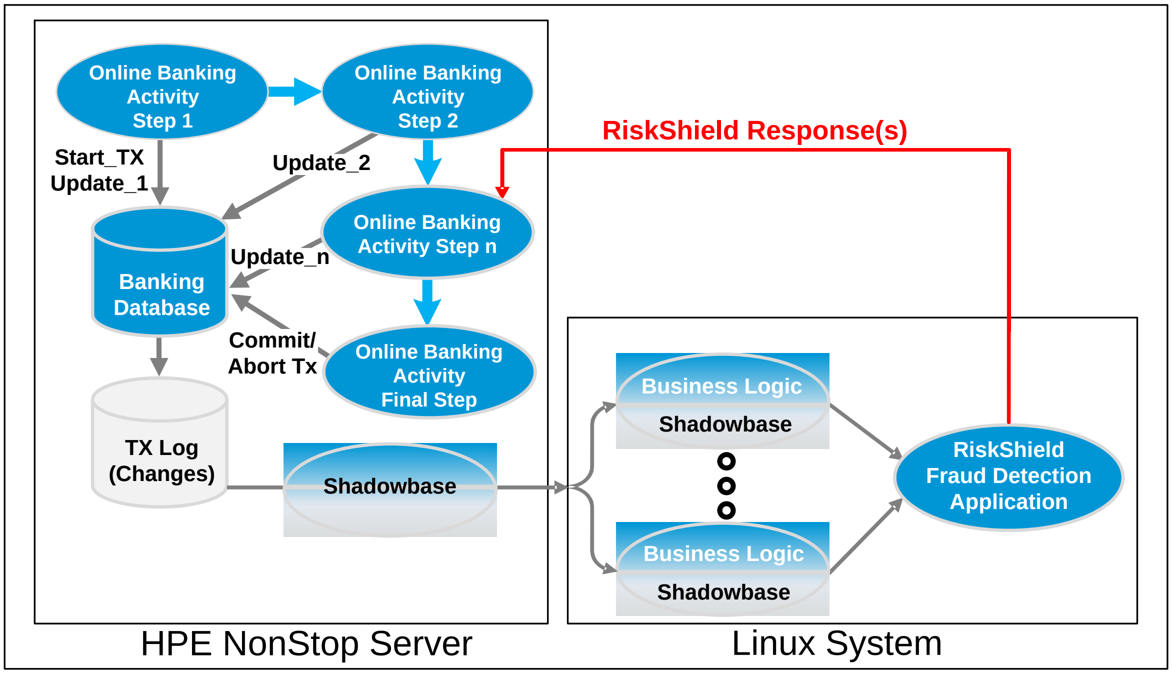

Figure 1 – The Bank's Internet Banking Fraud Detection System

For example, when a criminal intends to transfer money from another account to his account, the first step is the user authentication process. The user ID and password information are captured by the IBA and are logged in the banking database under a TMF transaction. Shadowbase replication reads this information from the TMF audit trail and through the process described above would quickly be delivered to the RiskShield application, which could then begin its analysis. Even if an immediate response were returned by the RiskShield application flagging the transaction as suspicious, the bank would allow the activity to proceed, since an actual criminal act has not yet been committed. Meanwhile, the next step of the internet banking activity proceeds, which might be to validate whether there are sufficient funds in the source account to satisfy the transfer. Likewise, this database update is logged and delivered to the RiskShield application.

For some accounts, rules may have been established which limit the amount of transfers, especially if the transfers are destined for overseas accounts. The RiskShield application includes this additional information with that already received and continues its analysis. The next step for the IBA is to validate the target account for the transfer. Again, the banking database is updated with this information, which is forwarded by Shadowbase technology in real-time to the RiskShield application, which adds yet another piece of information to the puzzle.

Finally, the criminal is presented with a confirmation screen by the internet banking application, showing the FROM and TO account information, the amount to be transferred, and is asked if the information is correct to click an "Execute Transfer" button. If, by this time, a response has been received from the RiskShield application indicating that the activity is suspicious, the TMF transaction will be aborted, the money transfer is not performed, and the fraud is prevented.

The bank will then take further steps as appropriate, for example, notifying the actual account holder that their credentials have been compromised, and suspending the account (similar to the phishing example above!). But, most importantly, because the criminal activity was allowed to proceed to the point where an actual crime was committed (the attempt to fraudulently transfer money from one account to another), the bank will contact authorities and provide them with all of the details that the internet banking and RiskShield applications captured, enabling it to pursue an investigation and possible criminal prosecution.

There is a very interesting point to note with the operation of this fraud detection system. If the response from the RiskShield application is *not* received by the IBA by the time of the final step in the activity (by the time the "Execute Transfer" button is clicked in our example), the bank may nevertheless *complete* the activity (perform the transfer and commit the TMF transaction in this case). If subsequently the RiskShield response indicates possible fraud, the bank will then take the necessary steps retroactively. While this approach is not ideal from the fraud prevention perspective, the bank does not necessarily want to delay a user transaction every time the fraud response is unacceptably "slow" in order to catch the few (by comparison) fraudulent activities. The IBA is optimized for the normal, non-fraudulent case, with reasonable time limits for response time. This approach illustrates the tension between the bank's need to prevent fraud, while not negatively slowing down normal business or customer service.

Another interesting facet of this application is that there are aspects of big data analytics, application integration, and real-time business intelligence (RTBI) involved.[4] There can be as many as 5,000-6,000 transactions per second moving through this system, which requires Shadowbase replication to read and distribute data between heterogeneous applications (running on NonStop and Linux systems) and the RiskShield application to analyze this data – all in real-time with minimal latency and overhead.

Conclusion

Fortunately, the system is working! Figure 2 shows the occurrences of internet banking fraud in the bank's home country over the past few years[5]. The numbers have continually increased, and do not show any signs of slowing down any time soon.

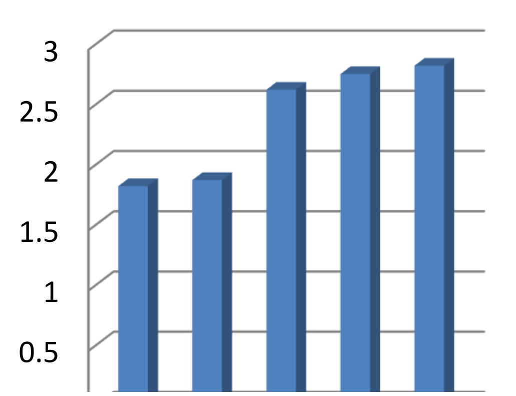

Figure 2 – Total Amount of Payment Card Fraud Cases in Bank's Home Country (in millions)[5]

This example provides a powerful demonstration of what can be achieved with clever application design, coupled with an HPE Shadowbase high-speed/high-throughput heterogeneous data distribution fabric, to deliver large amounts of data in real-time to a data analytics engine. The result is a system that provides critical functionality and produces tangible positive results for the business. In this case, the application is used to prevent internet banking fraud, and has resulted in a significant decrease in the cost of such fraud to the bank, and prosecution of the perpetrators. Of course, there are many other applications of such technologies to enable businesses, to not only detect and defeat criminal activity, but also to gain other competitive advantages in other markets and industries.

The HPE Shadowbase Data Replication Product Suite

The HPE Shadowbase solution suite comprises several products addressing business continuity, data replication, data and application integration, zero downtime migration, and other utilities to deliver a true 24x7 "nonstop" enterprise. HPE Shadowbase Streams change data capture technology allows companies to build real-time business intelligence systems to immediately analyze and process events as they occur in their organization, using an efficient event-driven architecture (EDA). As shown in this case study, it allows disparate applications to interoperate in real-time at the data level, avoiding the need for expensive programming and middleware adapters.

[4] For more information, please see these white papers: *HPE Shadowbase Solutions in a Big Data World*, *HPE Shadowbase Streams for Application Integration*, and *The Evolution of Real-Time Business Intelligence and How to Achieve it Using HPE Shadowbase*.

[5] Source: *Total number of annual fraud cases of payment cards in the United Kingdom (UK) from 2012 to 2020* — Statista.com

International Partner Information

Global

Hewlett Packard Enterprise
6280 America Center Drive
San Jose, CA 95002
USA
Tel: +1.800.607.3567
www.hpe.com

Japan

High Availability Systems Co. Ltd
MS Shibaura Bldg.
4-13-23 Shibaura
Minato-ku, Tokyo 108-0023
Japan
Tel: +81 3 5730 8870
Fax: +81 3 5730 8629
www.ha-sys.co.jp

Gravic, Inc. Contact Information

17 General Warren Blvd.
Malvern, PA 19355-1245
USA
Tel: +1.610.647.6250
Fax: +1.610.647.7958
www.shadowbasesoftware.com
Email Sales: shadowbase@gravic.com
Email Support: sbsupport@gravic.com

Hewlett Packard Enterprise Business Partner Information

Hewlett Packard Enterprise directly sells and supports Shadowbase Solutions under the name ***HPE Shadowbase***. For more information, please contact your local HPE account team or visit our website.

Copyright and Trademark Information