RSA ADAPTIVE AUTHENTICATION AND OUT-OF-BAND AUTHENTICATION

Combating Advanced Attacks and Protecting High Risk Transactions with Layered Authentication

Out-of-band: Additional authentication made easy

- One of the biggest hurdles organizations face when they add strong authentication to their online portals or VPNs is a degraded customer or employee experience.
- RSA Adaptive Authentication and Transaction Monitoring capabilities can be deployed completely invisible to the end user for a convenient experience. However, to protect against threats such as man-in-the-browser Trojans, institutions may opt to visibly challenge a small percentage of customers during the highest risk transactions with out-of-band authentication. Genuine user experience will not be disrupted.
- RSA's Out-of-band authentication provides many benefits. First, it meets the demands by customers for a solution that is easy to use and understand. Second, it does not require end users to buy new hardware or download software. Finally, it relies on common, accessible communication channels such as landlines, mobile phone networks, or e-mail.

"When we decided to look at stronger authentication we had three main criteria to evaluate: cost, ease of use, and additional layers of security. RSA came out on top in all three areas."

ANDY MUDDIMER, HEAD OF INTERNET BANKING AT ALLIANCE & LEICESTER

Trojans and other forms of malware continue to infect end customers and employees. Phishing and spear phishing attacks enable advanced Trojans such as Man-in-the-Middle and Man-in-the-Browser to make fraudulent transactions. Once a genuine user's machine is infected with one of these advanced Trojans, fraudsters have the ability to interact with website or portals without detection. Login protection alone is no longer enough to combat these threats.

The man-in-the-browser attack, which infects an end user's browser, is capable of manipulating web pages and transaction details in real-time without detection by the end user. This Trojan is also difficult to detect from the organization's server side because any activity performed appears to originate from the legitimate end user's web browser. Characteristics such as the Windows language, user agent string, and the IP address will appear the same as the user's real data. Man-in-the-middle attacks, meanwhile hijack end user's authenticated sessions without detection by the online application or end user and initiates new transactions while displaying a message to the end user that the website is currently unavailable.

These attacks take over a user's authenticated session, even if strong authentication methods have been used. To protect customers from these attacks, an additional layer of authentication must occur outside of the channel the transaction has originated from.

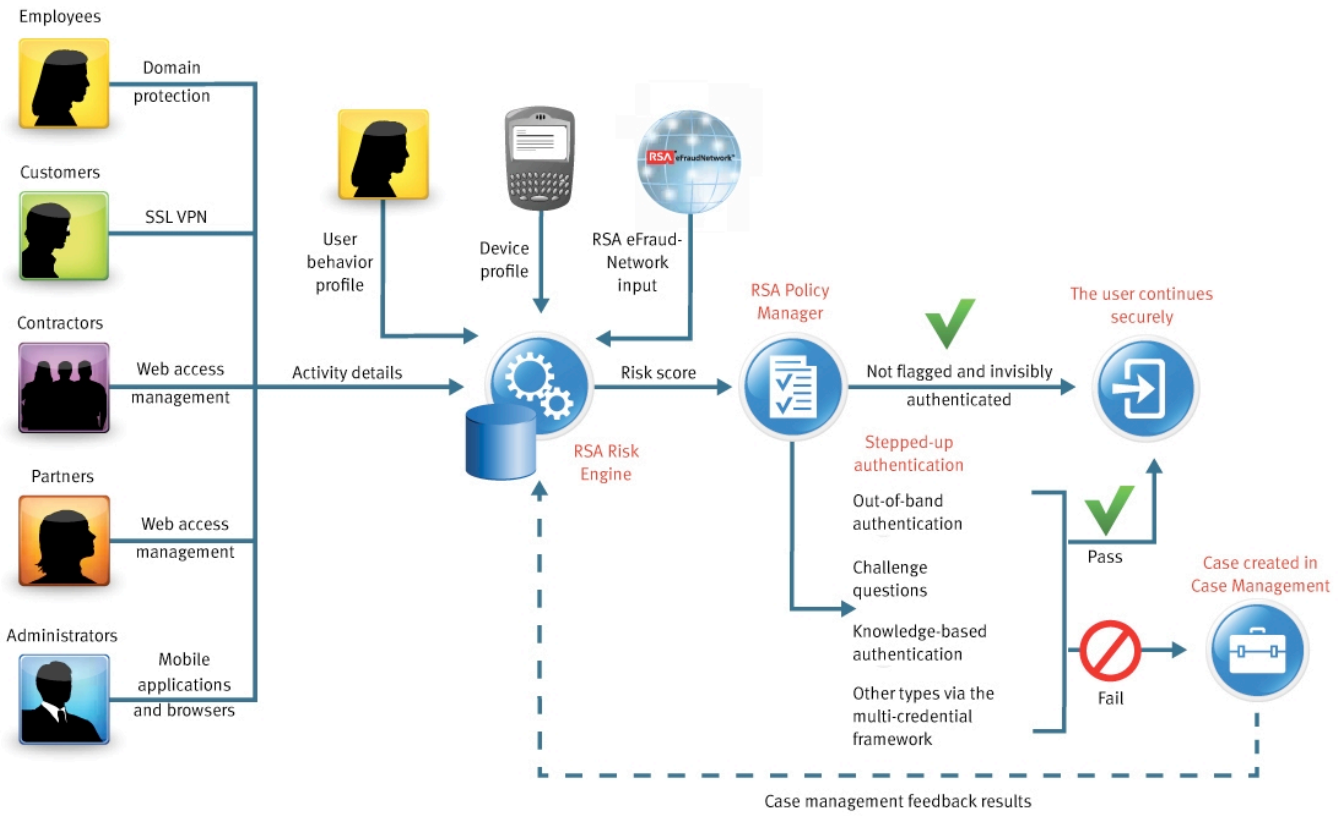
Regulations worldwide, including in the US, India, and China stress layered online security with a focus on protecting transactions. Login protection is no longer good enough, as fraudsters have multiple mechanisms for compromising credentials as well as authenticated sessions. The 2011 FFIEC Guidance, for example, calls for layered security including risk-based fraud detection and monitoring systems which enable out-of-band, multi-factor and step-up authentication for high-risk transactions. Transaction activity – both monetary and non-monetary – need to be monitored for anomalies to determine risk and the appropriate authentication methods. Organizations need the ability to verify the details of a high-risk transaction with out-of-band authentication.

Transaction Protection

Transaction protection refers to an organization's ability to monitor and identify suspicious post-login activities – a capability most often provided by a risk-based authentication solution. Transactions typically require more scrutiny and pose more risk than the act of logging in. An unauthorized user might secure login access to an account, but the damage is done once a transaction is completed. For example, transferring money out of the account, editing a beneficiary on an insurance policy or changing an enterprise password can all result in data or monetary loss. Transaction protection solutions look for anomalies in the end users' behavior and challenge these activities appropriately.

RSA® Adaptive Authentication and Transaction Monitoring are advanced fraud detection platforms that measure over one hundred risk indicators to identify high-risk and suspicious activities.

Adaptive Authentication and Transaction Monitoring are protected by the RSA® eFraudNetwork™, a cross-organization repository of cybercrime data gleaned from RSA's worldwide network of customers, end users, ISPs, and other third party contributors. When a transaction or activity is attempted from a device or IP address that appears in the eFraudNetwork data repository, it will be deemed high-risk and either prompt a request for additional authentication, such as Out-of-Band authentication, or be flagged for further review.



Adaptive Authentication and Transaction Monitoring can monitor and visibly authenticate logins and transactions

Out-of-Band Authentication to Verify Transactions

Out-of-band authentication methods are a powerful weapon against fraud because they work around the compromised communication channel. When a high-risk transaction is flagged by RSA's Risk Engine, organizations can choose to use out-of-band authentication to verify the genuine end user is requesting that specific transaction. Multiple transaction types – both financial and non-financial – can be protected.

Protection for Multiple Transaction Types

- Bill payment verification
- Login verification
- Money transfer verification
- Password change verification
- Address change verification
- PIN request verification
- Checks request
- New card request
- New payee
- PaymentSimple
- Generic request verification

RSA Adaptive Authentication and Transaction Monitoring leverage out-of-band phone, SMS and email authentication to verify transactions in cases where a transaction has been deemed high-risk and the user has been challenged. A communication is sent to the customer either through a phone call, SMS message or email. Then a secure, onetime password will be used to authenticate the genuine user's transaction when verified by RSA's Adaptive Authentication. In addition to a onetime password, RSA's out-of-band authentication can include specific transaction details as to what has occurred in the end user's account, thus increasing consumer or employee confidence.

As an additional level of security Call Forward Detection can be activated on top of Out-of-band Phone authentication. This feature combats fraudsters who attempt to intercept the challenge call by forwarding the genuine user's phone number to their own. RSA Risk Based Authentication system can identify when a phone number has been forwarded and will block the OOB challenge call to the fraudster's phone.

Enrollment process

When signing up for online account access, new customers are prompted to enter one or more contact phone numbers or email addresses. In the event of a high-risk transaction that requires additional authentication, the customer will be contacted at one of these numbers or email addresses. For existing customers, enrollment is either optional or mandated – they can be prompted to enroll during a future online session during a low risk transaction.

How it works

Out-of-band authentication occurs when a transaction is identified by the RSA Risk engine to be high-risk or suspicious or when an institutional policy triggers it (e.g. "challenge all transactions originating in country X or country y"). In both scenarios, RSA Adaptive Authentication challenges the customer to reconfirm the transaction. First, the system will ask the customer to select one of their phone numbers or email addresses at

RSA's Out-of-band phone authentication with Call Forward Detection

which to receive a phone call, SMS or email. Next, the system generates an automated message informing the customer of the transaction details and prompts them to enter the confirmation number displayed either into their phone or the web browser. Once the correct number is entered, the transaction will continue without disruption.

Conclusion

RSA's out-of-band authentication is a flexible, configurable and convenient layered protection method to secure end user's transactions. Fraudsters have become more advanced in their attacks; RSA counteracts their efforts by adding transaction protection with out-of-band authentication.

About RSA

RSA is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.

www.rsa.com

RSA®

EMC²®