ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Risk Based Authentication

Anvesh Gunuganti

USA

ABSTRACT

In the world of cybersecurity, increasing challenges faced by organizations trying to catch up with the technology used by cybercriminals for advanced attacks on their data and systems are becoming increasingly significant. Legacy authentication practices, which rely on static credentials, have become ineffective in fighting new accounts attacks as credential stuffing and taking accounts over by the bad actors. On the other hand, to overcome these obstacles, RBA is a dynamic model based on contextual risk indicators, determining the required authentication level.

This SLR scrutinizes the implementation of Risk-Based Authentication (RBA) employed by the Ping Risk, one of the top RBA platform, in the platforms. Through the process of integrating academic literature and anecdotal evidence, the paper discusses in what ways RBA with Ping Risk makes the cybersecurity more efficient and inviting for the end user in the organizational environment. Through the analysis of RBA, the adaptive nature of RBA is noticed where all identification techniques dynamically changes every authentication based on the user behavior, device information, and location hence, the security posture is improved but the user experience is not compromised.

The results describe about the fact that Resort-Based Authentication (RBA) and Ping Risk can create organizations to do away with the currently happening threats. This mode of operation is much more effective when compared to traditional static authentication techniques. It is considered highly reliable and acceptable under the current circumstances.

The review acquaints organizations with most important areas through which RBA security policies should be developed that include periodic assessment of the RBA risks, engaging users in the educational programs, and continuous monitoring of the RBA policies.

***Corresponding author**

Anvesh Gunuganti, USA.

Received: March 04, 2022; **Accepted:** March 10, 2022; **Published:** March 18, 2022

Keywords: Risk-Based Authentication (RBA), Ping Risk, Cybersecurity

Introduction

In the era of the cybersecurity arena there is an array of increasing dangers aimed at getting confidential data of systems. The conventional authentication means that employ username and password combination have not remained sufficient for serious attacks [1]. To compensate for these difficulties, risk-based authentication (RBA) has built its reputation as an adaptive and dynamic method which guarantees a smooth user experience while at the same time maintaining a high level of security.

Risk-Based Authentication (RBA) is a technique that considers the context like location, time and user behavior to ascertain the level of risk involved in login or transaction attempts. However, the RBA uses dynamic factors such as user behavior record, device information, login time, and so on to authenticate rather than the traditional authentication way of using static factors only including credentials or password. Thus, it continues modules while other systems need to be updated manually [2]. Such and redundant process allow properties of higher reliability while maintaining original speed. RBA is a risk-reducing measure because it decreases the possibility of common risks like account takeovers and illegal system access by designing authentication mechanisms that are suited to the real-time risk assessments thus ensuring compliance with the security protocols.

There are several common approaches to implementing Risk-Based Authentication:

- **Contextual Analysis:** The RBA framework employs contextual variables, such as location, IP address, user's browser information and previous browsing history, to rate a transaction, and then reject any transaction that don't match these criteria. For example, in case of an attack, detected by the system in the form of login transfers from an unfamiliar place or an instrument that is unknown, the system would immediately assign a higher level of risks and consequently would be required to request additional authentication factors to complete the identification of the user.
- **Behavioral Biometrics:** RBA systems can employ behavioral biometrics to authenticate users based on unique recognition of a person's physical features, like his typing speed, mouse movements or touch screen interactions. This method that underlies this approach is further bolstered by consistently identifying the user even as the session continues.
- **Machine Learning and AI:** In depth RBA systems use machine learning algorithm so that they can quickly learn about behavior patterns and the anomalies, hence improving and adapting continuously. Artificial Intelligence based systems through learning experiences and past interactions with security breaches can make more accurate risk

assessments, and respond in time to emerging threats.

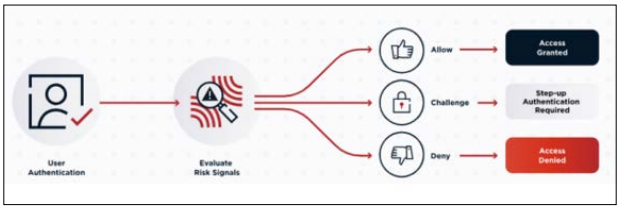

Figure 1: Risk Based Authentication [3].

The application of Risk-Based Authentication (RBA) with Ping Risk at the same time implies a proactive and adaptive nature of cybersecurity in practice. By combining Ping Risk, a leading unified platform, with the existing Identity and Access Management (IAM), we used its advanced risk assessment abilities [4]. Such integration provides system with an ability to analyze risk factors of the surrounding context and implement authentication techniques, which allows improving security and providing a more comfortable user authentication experience.

Problem Statement

Challenges Faced Before RBA Implementation

Identification of Traditional Authentication Limitations

Before the implementation of the RBA approach with Ping Risk, our organization was confined with a rigid authentication pattern. These limitations included:

- **Vulnerability to Credential-Based Attacks:** Classical ways of authentication such as username and password had many forms of attack done by attackers like phishing, credential stuffing, and brute-force attacks [4]. After the hackers gain leverage on the credentials, they can freely get to unauthorized system and data that are noted as confidential.
- **Inability to Detect Anomalies:** Instant authentication mechanisms did not have the opportunity to verify non-standard user behavior or recognize atypical login patterns. This forced us to pinpoint and reduce risks in real-time, which could result in security gaps that can last for extended periods without being identified.

Need for a Dynamic and Adaptive Authentication Approach

The upsurge of the cybersecurity threats demonstrated the importance of moving towards a complex and dynamic authentication solution. Key challenges that necessitated the adoption of Risk-Based Authentication (RBA) included:

- **Adapting to Evolving Threats:** All the same, conventional authentication solutions presented a lack of clairvoyance, which did not permit them to adjust to changing cybersecurity threats [5]. Static approach to the authentication method any longer was not sufficient as there were multiple attacks that target human error, as well as technology weaknesses.
- **Enhancing User Experience and Security:** The security space was looking for the new solutions which developed not only high security working but also good user experience too. A delicate fusion of reliable security techniques and a compliant authentication process was essential in order that users were able to continue working with ease [6]. Through the Risk-Based Authentication (RBA) with Ping Risk implementation in our organization, we were trying to increase the overall effectiveness of security but not to stop in the limitations of traditional authentication methods.

Research Questions

- How does the implementation of Risk-Based Authentication (RBA) using Ping Risk enhance cybersecurity effectiveness and user experience in an organizational context?

Literature Review

Risk-Based Authentication (RBA) is a critical method in cybersecurity as it offers a dynamic and adaptive mechanism in the era where traditional authentication methods are increasingly vulnerable. More than ever before today, contextual factors like location, device usage, and user behavior are evaluated for the purpose of assessing the level of risk associated with every authentication attempt. Outdated security authentication means, like username and passwords which are vulnerable to credential stuffing and takeover of accounts, have not been able to combat the cybercriminal sphere which is increasingly evolving and sophisticated.

RBA solutions, for example, Ping Risk, employs a wide range of parameters such as user behavior, device details, location and time to evaluate a risk score for every access attempt [7]. These scores forms the baseline for the implementation of proper authentication measures to ensure higher protection level for the users at the same time, the internal hurdles for user will be not so noticeable.

Overview of Ping Risk Capabilities

Ping Risk, as an advanced RBA platform, offers a suite of capabilities designed to bolster security effectiveness and optimize the user authentication experience:

- **Contextual Risk Assessment:** Ping Risk harnesses advanced algorithms that detects multifactor context; this makes risk rating of real time authentication possible [8].
- **Adaptive Authentication Policies:** As per the discussion of risk, Ping Risk actively adapts authentication basis on the requirements, making high-risk activities more secured and less complicated for risky activity [4].
- **Continuous Monitoring and Real-time Response:** Ping Risk is the monitoring tool that helps to instantly detect suspicious activities or gaping holes in the authentication procedure [7]. This allows for a quick response and avoiding attacks that are hidden in the actions during the authentication process.

Integration Process with Existing IAM Systems

The integration of Ping Risk into IAM systems involves a strategic implementation process tailored to organizational requirements:

- **Assessment and Planning:** Organizations do a comprehensive analysis of their authentication needs and current IAM infrastructure which is information necessary for determining integration objectives and the breadth of the project [9].
- **Deployment and Configuration:** Ping Ping Risk resides within the IT environment and communicates seamlessly with other present-day IAM systems that exist, so the exchange of data is intact and the machines do not conflict [6].
- **Customization of Risk Factors and Policies:** Organizations will evaluate and design their own risk factors and corresponding authentication policies according to their acceptance to risk, security policies as well as regulation requirements- and they will set thresholds for risk levels and the actions that will be taken, accordingly [10].

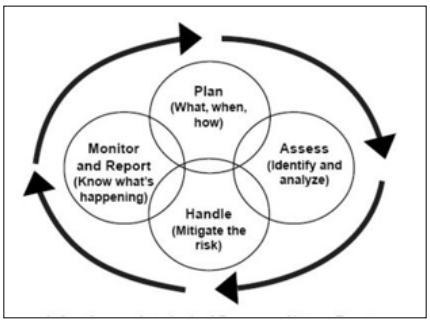

Figure 2: IAM Systems with Ping Risk [11].

- **User Education and Training:** Stakeholders complete broader education and coaching set for themselves to cultivate knowledge about new authentication mechanisms and security improvements from Ping Risk [4].
- **Continuous Monitoring and Optimization:** Organizations regularly monitor and key performance indicators of the Ping Risk implementations, conduct regular assessments, and update risk parameters, authentication policies since new risks and user needs may arise [7].

Industry Adoption and Best Practices

The Ping Risk integration is an industry-wise demonstration of the top of cybersecurity measures in practice in Risk Based Authentication and its adherence to regulative requirements and uplift in overall security posture. Organizations that have adopted RBA solutions such as Ping Risk, among others, are evidently strategically inclined in adopting intuitive security methods that stand a better chance of offering not only robust protection but also a favorable customer experience [6].

The adaptation of Ping Risk is a good case study that catches a yet shallow trend of context and risk-based authentication methods development, which uncannily emphasize the presence of adaptive security measures and the cybersecurity world.

Setting up Risk Factors

In Risk-Based Authentication (RBA) the various factors analysing includes which takes into account with examination of the risk inherent each authentication attempt. The following factors are considered in the implementation of RBA using Ping Risk:

- **Behavioral Factors:** Behavioral tracking implies keeping an eye on user interactions and patterns on authentication. This refers to the way people vary the speed of their keystroke, the pattern of mouse movement, the speed of their typing, and the way they navigate. Out of the ordinary deviation from hit behavior patterns could mean risk occurrence [7].
- **Environmental Factors:** The environmental factors e.g. Geolocation (IP address), time of access and network characteristics are assessed through this approach to authenticate the validity of the access. The unlikeness in geolocation or access times can be the cause of raised risk [5].
- **Device-Related Factors:** Device fingerprinting methods are applied to figure out which device is used to access the event and to verify these devices. The device-related factors include hardware, operating system, browser version and posture. Device attributes' modification or undetected devices upgrade can be a risk factor [9].

Customizing Authentication Policies

Adaptive authentication policies in RBA using Ping Risk enable organizations to tailor authentication requirements based on the assessed risk levels:

- **Thresholds and Rules Definition:** Organizations determine risk categories and rules based on certain risk levels which are deemed as acceptable. For example, high-risk activities can have multi-factor authentication MFA, or step-up authentication, while low-risk activities only need minimal authentication steps [4].
- **Tailoring Authentication Requirements:** Authentication policies are adaptively updated as risk assessment results may alter them. Ping Risk provides the ability to create authentication policies based on customer specifics to ensure the balance between security and user experience. Policy changes can be applied in accordance to the evolving threat ecosystem and the new user trends arising [7].

Continuous Monitoring and Adjustment

It is imperative to marshal Ping Risk's ability to monitor consistently as a key requirement for the effective implementation of RBA, assisting in the timely decision-making and caution ahead. Ping Risk aims at intense and continuous security monitoring covering process checks and login approves. The system automatically triggers response procedures for identified risks as well as long-needed improvements in security measures in accordance with business requirements [9]. Through the application of machine learning algorithms, Ping Risk detects unusual behavior in the course of the authentication process and can therefore instantly take action like access denial or user verification. This preventive strategy is one step ahead of cyber threats, prevents access restrictions violations, and creates a digital security landscape that is easy to maintain through RBA which then means the organizations do not have to worry about cyber threats and follow security protocols seamlessly.

Methodology

This Systematic Literature Review (SLR) aims to analyze and synthesize current academic papers, publications, and industry reports which discuss Risk-Based Authentication (RBA) in cybersecurity domain. The review aims to identify patterns of challenges and solutions in RBA implementation, with special attention to the integration and effectiveness of Ping Risk as an RBA solution.

Inclusion Criteria

The search for information will involve peer-reviewed journal articles, conference papers, technical reports and industry publications dealing with Risk-Based Authentication and Ping Risk. Inclusion criteria are as follows:

- Studies from reputable sources (such as Google scholar, IEEE).
- Publications published between 2019-2024 (last five years) which include the most recent developments.
- Focus on Risk-Based Authentication concepts, approaches, and assessments.
- Publications devoted to the integration or assessment of Ping Risk.

Exclusion Criteria

The following criteria will be used for excluding studies from the review:

- Publications that are not translated into English.
- Articles out of the given parameter (prior to 2019).
- Non-peer-reviewed sources include blogs, news articles, and commentary.
- Studies, which do not explicitly deal with "Risk-Based

Authentication" or "Ping Identity" platforms integration.
- Duplicated publications or studies lack examination detail, making their characterization challenging.

Study Selection and Data Extraction
Study Selection Process
- **Database Search:** Database Search: Comprehensive search across selected databases (e.g., IEEE Xplore, Google scholar).
- **Screening of Titles and Abstracts:** Initial screening based on relevance to RBA and Ping Risk integration.
- **Full-Text Review:** Narrowing the focus of the literature review to a selected group of studies that are qualified by specified inclusion and exclusion criteria.
- **Data Extraction:** Pulling out data of trial characteristics, RBA principles, details of risk process integration, security benefits and user behavior are the key to making this generalization.

Data Synthesis and Analysis
Data derived from extraction will be combined, processed and studied for answering the primary questions and for accessing common motifs, patterns, and insights in the scope of RBA implementation with Ping Risk. Synthesizing data methods used might include thematic analysis, content analysis, and comparison of study results across the board.

Case Studies
The paper considers Risk-Based Authentication (RBA) as a way of dealing with security while combating password stealing which is a hand-maiden of the account takeover attacks [1]. Among the recommendations for a secure authentication adopted by the NIST and NCSC, RBA is one of the most widespread online service strategies since it is effective and easy to use by users according to them, preferred over two-factor authentication. Privacy issue associated with RBA because it is partly based on an IP address and the browsing information which resulted in the need to create a 'Privacy vs Security' balance.

To deal with the challenges, the article suggests privacy-enhancing enhancements for RBA systems and checks their viability through real-world data retrieved from 780 users. The outcome of the research demonstrates that there is a possibility to enhance user privacy without detrimental effect on security, but certain parameters should guide RBA design in order to properly prevent obtaining user data. Finally, these directions are suggested for future research to make the spreading of privacy-preserving RBA technologies a common practice and to make the technologies acceptable by users and comply with privacy regulation.

As pointed out in the document, the Risk-Based Authentication (RBA) improves password security by recognizing and responding to outliers such as any doubtful login features which is useful for credential stuffing, guessing of the passwords, and phishing experiences [2]. Meanwhile, the fact that in many existing RBA systems users are being asked to re-authenticate via email with a number code has also contributed to the drop in the usability aspect which has yet not been fully studied. This study introduces two alternative RBA re-authentication methods: a mix of link (link-based) approach using "magic" links and an additional code (a code-based) method. The randomized between-subjects design was utilized in this research that involved 592 participants to compare the approaches.

Research results indicate a significant capability to speed up the RBA re-identification procedure which does not undermine the security of the process or the user's perception of reliability. But, the chain connection feature using "magic links" in the first place raised more fears than the code-based forms of additional authentication.

This implies that no one universal standard exists and this is the cause for using different procedures for re-authentication. In conclusion, the work delivers fundamental and applicable findings and recommendations concerning the best RBA relog-in methods securing and creating users' experience.

Results
The Systematic Literature Review (SLR) focused on addressing the research question. The literature review with case studies, used as the basis for this article, allows a deep understanding of what impact a RBA implementation with Ping Risk on cybersecurity effectiveness and user experience level is in companies.

Cybersecurity Effectiveness: According to the literature the subjected to review, implementation of Risk-Based Authentication (RBA) using the Ping Risk is proven one of the most efficient approaches to be included within organizational information and cybersecurity sphere. Ping Risk refreshingly addresses the ever-changing authentication challenges utilizing dynamic authentication measures that are based on specified risk levels. The enemy of convenience is security, and Ping Risk strikes the perfect balance for stopping malicious access through credential stuffing, password guessing, and account takeover attacks with traditional static authentication methods. This very adaptive method of checking of credentials notably decreases the probability of intrusion and hacks, thus enhancing the posture of a whole cybersecurity.

User Experience Improvement: Users experience improved usability while utilizing the Ping Risk authentication system in combination with the RBA system than when they utilize traditional authentication systems. In a manner, which concentrates on user conveniences while still maintaining strong security, Ping Risk charges authentication requirements by the contextual sleuthing such as user behavior, device details, and location? Specifically speaking, this tailored system minimizes the end-users' efforts during the authentication process, and thus, improves usability, especially for the employees and clients. Research shows that the users perceive RBA with Ping Risk to be the most user-friendly and intuitive one that gives the users high satisfaction level.

Organizational Context and Case Studies: The SLR offers typical circumstances and walks through the process of using Ping Risk in an organizational setting. These case studies provide an illustrative example of Ping Risk cybersecurity solutions in place, targeting the challenges of proactive detection of threats, compliance with regulatory requirements, and a dynamic strategy of risk mitigation. Tangible correlation between RBA and Ping Risk implementation proves effectively in level of cyber security and positive user experience for an organization within diverse operational contexts.

Finally, summing up the synthesis of literature and case studies we may come to the conclusion that introducing Risk-Based Authentication (RBA) using Ping Risk greatly strengthens cybersecurity and gives an improvement in user experience associated with security issues in organizational settings. Through developing and implementing an adaptive and context-sensitive verification scheme, businesses transform the security practices

in their organizations to create an atmosphere that allows both robust security measures and user-friendly authentication methods at the same time.

Discussion

Through the use of rational approach to this issue, the evidence can be collected from the readings and cases on the deployment of RBA and Ping Risk show that there are several very important implications for the effectiveness of cybersecurity, user-experience in the organizational contexts.

RBA's Role in Enhancing Cybersecurity

RBA findings thus have demonstrated its vital role, especially where such implementations are made with the application of the Ping Risk system which of course enhances the cybersecurity resilience of an organization. Leaving behind simple credential-based authentication tools that solely rely on a given user's credentials, RBA introduces a dynamic layer of security that learns as prolonged threats and issues emerge [4]. The Ping Risk feature of detecting contextual risk factors such as user behavior, device information, and location is what permits the organizations to deploy targeted authentication measures which prove more competent in curtailing the widespread strategies of credential stuffing and account takeover attempts which are very popular nowadays.

Balancing Security and User Experience

The prominent benefit is the great improvement in user experience, which was made possible by the Risk with Pings RBA. The access authorization methods which were historically used usually hinder the productivity and satisfaction of user by means of unpleasant security procedures. Additionally, Ping Risk integrates the ultimate proof-of-life mechanism which enables robust security while ensuring excellent user experience simultaneously [7]. Ping Risk presents authentication requirements that match the risk assessment outcomes, resulting in fewer difficulties during the location process that ends up offering smooth and intuitive experience for customers and employees.

Organizational Context and Real-World Applications

The inclusion of case studies and real-life examples in the review demonstrates how RBA with Ping Risk enhances performance across various organizational contexts. The documents below include the programs of Ping Risk which address particular cybersecurity issues; for example, proactive threat identification and detection, regulatory compliance, and adaptive cybersecurity risk mitigation policies [6]. Through these application implementations, beneficial results justify RBA with Ping Identity's effectiveness in increasing organizational security posture and UEM metric scores.

Threats to Validity

External Threats

- **Generalizability:** The empirical research and the conclusions because of the literature review and case studies may have limitations in external validity. The applicability of RBA along with Ping Risk in different organizational environments or industries may differ from one another, thus affecting the overall potential of generalization of the outcomes.
- **Time Sensitivity:** As cyber threats and technology are evolving at a rapid pace, there might be a possibility that conclusions and applications might be outdated in the future. The changing RBA solutions or increased threats can obstruct the success in the long term of Ping Risk.

Internal Threats

- **Selection Bias:** The selection criteria used for choosing individual articles and case studies to be included in the review can introduce some biases, which may result in the misrepresentation of the available literature or an omission of the relevant perspectives.
- **Measurement Bias:** The use of diverse methodologies and metrics applied to different trials may distort measurements and further complicate the comparability and integration of the results.

Future Directions and Research Implications

The review shows RBA-based Ping Risk is worth using, but more research in certain fields is useful in future. In another vein, testing the expansiveness and operability of RBA solutions among different organizational units and industries with diverse settings can help to identify the key aspects of broader adoption and implementation strategies [4]. Furthermore, ongoing studies on the user's reaction and sentiments about the RBA, including the privacy and security problems, can be of help in the development of more user-oriented authentication solutions.

Practical Recommendations for Implementation

Based on the synthesized findings, practical recommendations emerge for organizations considering RBA implementation using Ping Risk, such as:

- Perform comprehensive risk assessments and integration planning in order to bring RBA strategies in line with organizational security objectives.
- Invest in user education and training to familiarize stakeholders with new authentication processes introduced by Ping Risk.

To summarize, the discussion describes the innovative power of the Ping Risk RBA implementation aimed to make cybersecurity more successful and user friendlier in an organizational environment. Adaptive authentication helps the organization to significantly increase the strength of security to the ease of use, both of which are required in the current security environment. In addition, the weakness, research validation, and ongoing research will contribute to the comprehension and implementation of RBA solutions such as Ping Risk in organizational cybersecurity strategies.

Conclusion

The SLR analysis has been carried out to see the role played by Ping identity in addition to risk-based authentication within the modern organisational security strategies literature which is a very significant aspect as well. RBA with Ping Identity is with a solution to authentication that is dynamic and adaptive. The system will examine different risk factors when determining authorization and thus there is a higher level of security effectiveness while at the same time enhancing user experience. Evaluation reveals data from a variety of sources, including scientific research and case studies, which show that the use of RBA with Ping Identity facilitates organizations to prevent the evolution of risks such as credential stuffing and account takeover vulnerabilities, which cannot be achieved by using conventional static authentication methods. Based on the previous user behavior, device details and location Ping Risk is resolving the real-time risk assessment and allows introducing specific authentication procedure, therefore, they will raise, basically, overall security level.

In the same manner, the attention paid to user experience is the latter of the remarkable differences between RBA and Ping Risk in which sensitive customers' data is protected. Ping Risk minimizes

the authentication process' friction sections and enhances workability. Employees and customers enjoy smooth processes and easy-to-use interfaces. Providing a user-centric perspective leads to higher levels of user acceptance evolves to their satisfaction, which is significant in cybersecurity strategies implementation. From now on, companies ought to look at minimizing the risks of biasness and proposing real-life solutions to this issue, this assessment is comprehensive, risk assessment, user education programs and, yet more monitoring of CBA policy for future implementation. Basically, Ping Risk enables the Facilitation of RBA which appears as a preventive measure for cybersecurity protection and creation of an environment friendly environment for increased cyber risk.

References

1. Wiefling S, Tolsdorf J, Iacono LL (2021) Privacy Considerations for Risk-Based Authentication Systems. 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) https://doi.org/10.1109/eurospw54576.2021.00040.
2. Wiefling S, Patil T, Dürmuth M, Luigi Lo Iacono (2020) Evaluation of Risk-Based Re-Authentication Methods. IFIP advances in information and communication technology 280-294.
3. (2024) Risk-based-Authentication. Pingidentity https://www.pingidentity.com/content/dam/picr/og/assets/misc/idf/Risk-based-Authentication-EN-OG.png.
4. Papadamou K, Savvas Zannettou, Bogdan Chifor, Sorin Teican, George Gugulea, et al. (2020) Killing the Password and Preserving Privacy with Device-Centric and Attribute-Based Authentication. IEEE Transactions on Information Forensics and Security 15: 2183-2193.
5. Wiefling S, Dürmuth M, Lo Iacono L (2020) More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. Annual Computer Security Applications Conference 203-218.
6. Sirapat Boonkrong (2020) Methods and Threats of Authentication. Apress eBooks 45-70.
7. Sepczuk M, Kotulski Z (2018) A new risk-based authentication management model oriented on user's experience. Computers & Security 73: 17-33.
8. Wiefling S, Lo Iacono L, Dürmuth M (2019) Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. ICT Systems Security and Privacy Protection 134-148.
9. Spooren J, Davy Preuveneers, Wouter Joosen (2015) Mobile device fingerprinting considered harmful for risk-based authentication. Lirias (KU Leuven) 6: 1-6.
10. Wiefling S, Dürmuth M, Lo Iacono L (2020) More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. Annual Computer Security Applications Conference 203-218.
11. Risk-based Authentication. https://www.pingidentity.com/en/resources/identity-fundamentals/authentication/risk-based-authentication.html.