PUBLIC SUBMISSION

As of: 4/25/22 12:26 PM
Received: April 20, 2022
Status: Pending_Post
Tracking No. l27-udha-huo7
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0022
Comment on FR Doc # N/A

Submitter Information

Name: Opeoluwa Odusan
Ad[redacted]
Email:[redacted]
Phone:[redacted]

General Comment

Access to, and security of information, electronic assets and data are now in the forefront of business and private use. Companies are under tremendous pressure and concern about their information and data and how these are protected in today's fast technological world. Data breaches that may happen because the levels of security are not as optimal as can be poses liabilities for companies. In the present-day management of information where most people access their data and offices from home or situations that they are away from the office – poses concerns as to who can access the data and what limitations are included in such access.

Access to data and information is a first level concern – with the ancillary concern being how much access is granted to anyone who now has access to the information repository. An example could be an employee who can get permission to review non-critical information and another who needs control over that information for the attendant decisions that a company needs to operate. This may apply to employees with different levels of security clearance and the requirement that such employees do not have visibility to information without a need to know or reach. This can also be extended to data that may need to be manipulated only by some employees and access to same needs to be managed and controlled by the establishment to prevent undue challenges.
NIST's Framework for Improving Critical Infrastructure Cybersecurity has been an exceptional resource for assisting organizations and entities with their cybersecurity efforts and development. After having read the Framework's Core functions (identify, protect, detect, respond, and recover), there are many ways in which the document could be updated to account for the various recent changes within the cybersecurity landscape of standards, protocols, and software development.

With increased remote work, cybersecurity threats and ransomware incidents have become more complex

in their approach regarding identity management, authentication, authorization, and access control. Systems and networks rely on assured and approved access to physical, electronic, and data assets ad the ability to limit authorized users, devices, and processes. As a result, risk-based authentication solutions (RBAS) were developed and commercialized in the market basing their software on the industry standards and protocols regarding authentication:

Basing authentication on the following:
-Something you know (i.e., password): most common authentication method
-Something you have (i.e., smart access card): this form of authentication removes the problem of forgetting something you know – but now an object must accompany you any time you want to be authenticated
-Something you are (i.e., fingerprint):basing authentication on something intrinsic to the principal of being authenticated

These three authentication components are very successful in managing access; however, the existing commercial systems possess gaps when it comes to protecting access to data, electronic assets, entities from both internal and external theft. For example, having access to a document management system via single sign-on tools may not authorize you to download all information in the document management systems especially document that are classified as secret and or sensitive. Current methods of accessing data and electronic assets are based largely on 2 step verification or two step authentication which uses a combination known (password) and a second factor. This process is limited in ability to access risk and limits cybersecurity software developers in creating complete risk management approaches.

That said, Risk Secured System's proprietary risk-based authentication and authorization solution (RBAAS) is the only solution that goes one step further – incorporating an additional set on top of something you know, something our have, and something you are. The RBAAS solution adds an additional layer of protection based on someone you know or someone who knows you and can approve your access in real-time to that classified resource or data asset. To expand, the benefit of this additional step is an enhanced safeguard against both internal and external unauthorized access to secret or sensitive data and assets within an enterprise's data ecosystem.

As a result, the NIST "Protect (PR) Identity Management, Authentication, and Access Control (PR.AC)" should consider revamping its approach and understanding of traditional authentication protocols and include an additional standard of approach when considering authentication methods. Additionally, this additional layer of protection can utilize algorithm and proprietary classification databases in real-time to provide access – thereby securing enterprise data and information systems from both known/unknown users while offering a platform that provides an audit trail, escalation process, and compliance monitoring.

Attachments

Final - NIST Request for Additional Information (Ope Review)

National Institute of Standards and Technology (NIST)
NIST-2022-0001 Request for Information (RFI)
Risk Secured Systems LLC
Docket Number: 220210-0045

National Institute of Standards & Technology (NIST)

Request for Information (RFI): *Framework for Improving Critical Infrastructure Cybersecurity*

Proposer: Opeoluwa Odusan; CEO/Founder of Risk Secured Systems LLC;
oodusan@risksecuredsystems.com

Access to, and security of information, electronic assets and data are now in the forefront of business and private use. Companies are under tremendous pressure and concern about their information and data and how these are protected in today's fast technological world. Data breaches that may happen because the levels of security are not as optimal as can be poses liabilities for companies. In the present-day use and management of information where most people access their data and offices from home or situations that they are away from the office – poses concerns as to who can access the data and what limitations are included in such access.

Access to data and information is a first level concern – with the ancillary concern being how much access is granted to anyone who now has access to the information repository. An example could be an employee who can get permission to review non-critical information and another who needs control over that information for the attendant decisions that a company needs to operate. This may apply to employees with different levels of security clearance and the requirement that such employees do not have visibility to information without a need to know or reach. This can also be extended to data that may need to be manipulated only by some employees and access to same needs to be managed and controlled by the establishment to prevent undue challenges.

NIST's *Framework for Improving Critical Infrastructure Cybersecurity* has been an exceptional resource for assisting organizations and entities with their cybersecurity efforts and development. After having read the Framework's Core functions (identify, protect, detect, respond, and recover), there are many ways in which the document could be updated to account for the various recent changes within the cybersecurity landscape of standards, protocol, and software development.

With the increased proliferation of remote work, cybersecurity threats and ransomware incidents have become more complex in their approach regarding identity management, authentication, authorization, and access control. Systems and networks rely on assured and approved access to physical, electronic, and data assets ad the ability to limit authorized users, devices, and processes. As a result, risk-based authentication solutions (RBAS) were developed and commercialized in the market basing their software on the industry standards and protocols regarding authentication:

- Basing authentication on the following:

- *Something you know (i.e., password)* – most common authentication method
- *Something you have (i.e., smart access card)* – this form of authentication removes the problem of forgetting something you know – but now an object must accompany you any time you want to be authenticated
- *Something you are (i.e., fingerprint)* – basing authentication on something intrinsic to the principal of being authenticated

These three authentication components are very successful in managing access; however, the existing commercial systems possess gaps when it comes to protecting access to data and electronic assets (including intangible assets) and to protect entities from both internal and external theft. For example, having access to a document management system via single sign-on tools may not authorize you to download all information in the document management systems especially document that are classified as secret and or sensitive. Current methods of accessing data and electronic assets are based largely on 2 step verification or two step authentication which uses a combination known (password) and a second factor. This process is limited in ability to access risk and limits cybersecurity software developers in creating complete risk management approaches.

That said, Risk Secured System's proprietary risk-based authentication and authorization solution (RBAAS) is the only solution that goes one step further – incorporating an additional set on top of *something you know, something our have, and something you are*. The RBAAS solution adds an additional layer of protection based on *someone you know or someone who knows you* and can approve your access in real-time to that classified resource or data asset. To expand, the benefit of this additional step is an enhanced safeguard against both internal and external unauthorized access to secret or sensitive data and assets within an enterprise's data ecosystem.

As a result, the NIST "Protect (PR) Identity Management, Authentication, and Access Control (PR.AC)" should consider revamping its approach and understanding of traditional authentication protocols and include an additional standard of approach when considering authentication methods. Additionally, this additional layer of protection can utilize algorithm and proprietary classification databases in real-time to provide access – thereby securing enterprise data and information systems from both known/unknown users while offering a platform that provides an audit trail, escalation process, compliance monitoring, and actionable intelligence.