Journal of Technological Innovations

Est. 2020

Cipher Compliance Strategies for Updating SSH Cryptographic Standards: Common Problems & Solution

Prashanth Kodurupati
Information Technology Managed File Transfer Engineer
PragmaEdge LLC
Alpharetta, United States of America
E-mail: prashanth.bachi21@gmail.com

Abstract:

This paper examines the critical issue of cipher expiration and compliance within secure shell (SSH) communications. As governments worldwide mandate the use of approved cryptographic standards, organizations must deal with the complexities of updating SSH ciphers and public keys to maintain secure connections to customer servers. The study identifies the prevalence of commonly used ciphers, the impact of cipher expiration on operational security, and the challenges organizations face in transitioning to higherstandard or latest ciphers. It proposes a comprehensive solution for updating cryptographic protocols in SSH to ensure continued compliance, security, and operational integrity.

Keywords: *SSH Protocol, Cipher Compliance, Cryptographic Standards, Cryptographic Standard*

1. Introduction

The advent of the digital age has ushered in an era of unprecedented connectivity, with the Secure Shell (SSH) protocol emerging as a cornerstone for secure network operations. Developed in 1995 by Tatu Ylönen, SSH was a response to the glaring vulnerabilities in remote login protocols, offering an encrypted channel for secure data communication and server management over unsecured networks. [1] Over the years, SSH has become indispensable for administrators and organizations worldwide, safeguarding data transfers, remote system control, and cryptographic authentication.

However, the digital environment evolves relentlessly. This evolution requires a corresponding progression in cryptographic standards, including the ciphers used within SSH protocols.

Governments and international standards bodies, recognizing the critical role of encryption in national security and data protection, have instituted regulatory frameworks mandating the use of approved cryptographic algorithms [2]. These algorithms are periodically reviewed and updated to counteract emerging threats and leverage advancements in cryptographic research.

The imposition of these standards, while essential for maintaining the integrity and confidentiality of digital communications,presents significant challenges for organizations. Compliance is not merely a technical issue anymore; it is a combination of operational, legal, and strategic considerations.

This paper looks into the issue(s) pertaining cipher compliance in SSH communications against the backdrop of this ever-evolving digital world. It explores the delicate balance organizations must strike between operational security and regulatory adherence, emphasizing the importance of proactive and informed management of cryptographic standards.

2. Literature Review

The literature surrounding the topic of cipher compliance in SSH communications reveals several key insights into the challenges and potential solutions faced by organizations in maintaining secure connections and adhering to cryptographic standards.

Research in this area emphasizes the dynamic nature of cryptographic protocols and the necessity for organizations to continuously update their SSH configurations to align with evolving regulatory frameworks and emerging threats. Studies by Jøsang (2018) and Williams (2011) look into the technical intricacies of SSH protocols.

Additionally, research by Zhu et al. (2004) sheds light on the legal and operational implications of encryption practices. Furthermore, the work of Liu et al. (2018) and Yang et al. (2007) addresses the challenges associated with transitioning to new cryptographic standards, emphasizing the importance of selecting ciphers that not only meet current security requirements but also offer resilience against future cryptographic advancements.

3. Problem Statement: Expiration, Compliance, & Transitioning Issues With Ciphers

In the world of digital communications, the Secure Shell (SSH) protocol is a primary concern for securing data transfers and administrative operations across networks.

However, the integrity of SSH communications relies on the cryptographic ciphers employed to encrypt data. Governments and international bodies, recognizing the paramount importance of robust encryption, have delineated approved ciphers, which are periodically reviewed and updated.
This cyclical nature of approval and expiration poses a nuanced challenge for organizations striving to ensure both compliance and security in their operation.

3.1 Cipher Expiration and Compliance Challenges

Cryptographic standards are marked by a continuous cycle of evaluation, approval, and, eventually, expiration of ciphers. This process, driven by advancements in computational power and cryptographic research, aims to phase out algorithms vulnerable to exploitation.

The expiration of a cipher does not merely signal a recommendation for updates; it often carries legal and operational implications for organizations. Compliance with governmental and sector-specific regulations becomes a moving target, necessitating vigilant management of cryptographic practices [3].

3.2 Common Ciphers and Organizational Practices

Today, organizations gravitate towards a core set of ciphers for SSH communications, driven by factors such as performance, compatibility, and perceived security.

This inclination, however, is double-edged; while standardization simplifies some aspects of network administration, it also exposes organizations to collective risk should a widely adopted cipher be compromised or reach its expiration.

Furthermore, the transition to newer, approved ciphers is not merely a technical task—it involves a comprehensive reassessment of IT infrastructures, application dependencies, and even vendor relationships.

3.3 Difficulties in Transitioning to Approved Ciphers

Transitioning to new ciphers, especially under the duress of looming expiration deadlines, is fraught with challenges. Technical hurdles, such as the integration with legacy systems and the need for crosscompatibility, are just the tip of the iceberg.

Organizations must also contend with the operational disruption that can accompany such transitions,

including potential downtime and the training requisite for IT staff. Moreover, the the proper selection of "high" or "standard/latest" ciphers involves a delicate balancing act between adopting cutting-edge security measures and ensuring that these choices do not prematurely obsolesce in the face of future cryptographic advancements. [4]

This problem statement highlights the critical intersection of compliance, security, and operational efficiency in managing SSH cipher standards. It sets the stage for a detailed exploration of the mechanisms organizations can employ in this complex terrain, emphasizing the importance of an informed approach to cryptographic management.

4. Academic Review of Key Challenges and Proposed Solutions

Research	Challenge	Solution
Jøsang (2018); Williams (2011)	The dynamic nature of cryptographic protocols and key exchange mechanisms in SSH communications.	Continuous updating of SSH configurations to align with evolving regulatory frameworks and emerging threats.
Zhu et al. (2004)	The legal and operational implications of encryption practices, including compliance with regulatory requirements and ensuring scalability.	Complex environment regulatory requirements while maintaining the security and scalability of cryptographic implementations.

5. Proposed Solution: Cipher Update of SSH & Public Keys

To deal with the aforementioned problems with SSH communications effectively, organizations must adopt a multifaceted approach that balances compliance, security, and operational continuity.

5.1 Framework for Cipher Update and Compliance The first step involves updating the cipher and SSH keys to ensure that the connection is secure against third-party influences. It involves four primary steps:

5.1. 1 Assessment and Planning

Begin by conducting a thorough assessment of the existing SSH infrastructure, identifying all ciphers in use and mapping their compliance status against current regulations. This phase should prioritize ciphers nearing expiration and those already deemed non-compliant. The planning stage should set clear timelines and milestones for the transition, considering the impact on both internal stakeholders and external users.

5.1.2. User Engagement

Early and continuous engagement with all users and stakeholders, including IT staff, management, and external partners, is crucial. Communication plans should outline the scope of the transition, expected outcomes, and the roles and responsibilities of involved parties.

5.1.3. Phased Rollout and Testing Implement the transition through a phased rollout, starting with non-critical systems to minimize operational risk. Each phase should include rigorous testing to ensure compatibility and maintain security standards, with lessons learned informing subsequent phases.

3.1.4. Documentation and Training

Comprehensive documentation of the new cipher configurations and associated processes is essential. Additionally, training programs should be developed to enhance the technical capabilities of IT staff, ensuring they are equipped to manage and troubleshoot the updated SSH environment.

5.2 Guidelines for Secure Cipher Transition

To implement the steps above, the following guidelines must be established: *5.2.1 Cipher Selection*

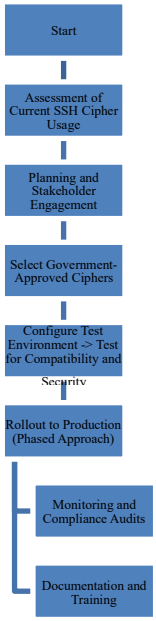
Select appropriate government-approved ciphers that align with organizational security policies and operational requirements. This selection should also consider future-proofing, opting for ciphers with a longer anticipated lifespan and resistance to emerging cryptographic threats. [5]

5.2.2.Configuration and Automation Update SSH configurations to include the selected ciphers, removing or deprecating those that are noncompliant.

Automation tools can streamline this process, enabling efficient updates across multiple servers and systems.

5.2.2 Monitoring and Compliance Verification

Establish continuous monitoring mechanisms to detect any unauthorized changes or attempts to use deprecated ciphers. Regular compliance audits should be conducted to ensure ongoing adherence to cryptographic standards.



The idea with this approach is to update SSH ciphers and public keys in a manner that mitigates the risks associated with cryptographic transitions, especially for government entities and similar settings [6].

The approach helps prioritize planning, user engagement, and rigorous testing to mitigate the challenges of cipher updates, safeguarding their digital communications against emerging threats while maintaining operational excellence.

5.3 Use Case

To update the SSH cipher on a server and ensure secure connections to customer servers for file transfers, follow these steps. This process involves identifying the current SSH cipher configuration, selecting and configuring a government-approved cipher, testing the new configuration, and finally, applying the changes across the environment. Automation can facilitate the update process, especially in environments with multiple servers.

First, determine the ciphers currently supported by your SSH server. This can be accomplished with the following command:

```
ssh -Q cipher
```

This command lists all ciphers supported by your SSH client, helping you identify which ones are currently enabled and need to be replaced or updated.

After identifying the current ciphers, select a government-approved cipher that meets the latest security standards. For this example, let's assume aes256-gcm@openssh.com is the approved cipher. To configure your SSH server to use this cipher, you would add it to your SSH daemon configuration file (sshd_config).

```
echo "Ciphers aes256-gcm@openssh.com" | sudo
tee
-a /etc/ssh/sshd_config
```

In environments with multiple servers, automating the update process is essential. Ansible, a popular automation tool, can be used to apply the cipher update across all servers efficiently. The following is a basic Ansible playbook snippet that updates the SSH cipher configuration:

```
---
-          hosts: all   tasks:
-          name: Configure SSH
to use approved cipher
lineinfile:
    path: /etc/ssh/sshd_config
    line: 'Ciphers aes256-gcm@openssh.com'
    state: present
  - name: Restart SSH service
systemd:
    name: sshd
state: restarted
```

This playbook specifies a task to update the sshd_config file with the approved cipher on all target hosts and then restarts the SSH service to apply the changes. Using such automation tools ensures consistent application of security updates across the infrastructure with minimal manual intervention.

6. Conclusion

The need to update SSH ciphers and public keys in response to government mandates and the expiration of cryptographic standards is not just a technical challenge but a necessity for maintaining secure and compliant digital communications.

This paper has highlighted the complexities organizations face issues with approved ciphers, underscored by the need to balance operational security, regulatory compliance, and the continuity of business operations.

Through the proposed Adaptive Security Framework (ASF), organizations are equipped with a comprehensive strategy to manage cipher transitions effectively. Focusing on emphasizing assessment, stakeholder engagement, phased testing, and the use of automation, the framework ensures that organizations can update their SSH configurations smoothly and maintain secure connections to customer servers for critical file transfers.

In doing so, organizations can safeguard their digital infrastructure against emerging threats, ensuring their operations remain secure, compliant, and resilient in the digital age.

7. References

[D. A. Jøsang, "ECCWS 2018 17th European 1 Conference on Cyber Warfare and Security] V2," in *ACPI*, Oslo, Norway, 2018.

[S. C. Williams, "Analysis of the SSH Key 2 Exchange Protocol," *Lecture Notes in Computer*] *Science,* vol. 7089, no. 2011, pp. 356-374, 2011.

[M. D. S. S. L. Bin Benjamin Zhu, "Encryption 3 and authentication for scalable multimedia:

] current state of the art and challenges," *Internet Multimedia Management Systems V,* vol. 5601, no. 2004, pp. 1-14, 2004.

[T. H. Y. P. Z. &. K. L. Joseph K. Liu, "Time4 Based Direct Revocable Ciphertext-Policy

] Attribute-Based Encryption with Short Revocation List," *Applied Cryptography and Network Security,* vol. 10892, pp. 516-534, 10 06 2018.

[B. B. Z. S. L. a. N. Y. Yang Yang, "Efficient and 5 Syntax-Compliant JPEG 2000 Encryption

] Preserving Original Fine Granularity of Scalability," *Hindawi Publishing Corporation,* p. 13, 23 11 2007.

[T. K. C. N. Mihir Bellare, "Authenticated 6 encryption in SSH: provably fixing the SSH

] binary packet protocol," *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security,* pp. 1-11, 01 09 2002.