Redfish
Local Host Authentication Security Options

Redfish Forum
February 2020

Disclaimer

- The information in this presentation represents a snapshot of work in progress within the DMTF.
- This information is subject to change without notice. The standard specifications remain the normative reference for all information.
- For additional information, see the DMTF website: http://www.dmtf.org

The Problem

- Redfish was designed for secure, network-based remote access, and always requires user credentials to access the Service
  - Typical implementation for servers uses a Baseboard Management Controller (BMC) that includes both network and host OS interfaces
- Legacy management interfaces, however, allow users with host operating system administrative privileges to manage the local server, through a host interface, without needing BMC credentials
  - Many users rely on this behavior and are reluctant to adopt Redfish due to the requirement of credentials, even for local access
- The *Redfish Host Interface Specification* (DSP0270) defines a method of providing BMC credentials to the host OS via UEFI variables
  - This mechanism not adopted by the industry
  - UEFI variables are readable by all users on some OS's, not available in other OS's, and unable to be read in "legacy BIOS mode"

Work in Progress

- The Redfish Forum is developing a new mechanism for providing Redfish user credentials to host OS applications
  - Intended to replace the existing UEFI variables mechanism in DSP0270
- The group evaluated multiple proposals using various physical interfaces and protocols
  - The group also consulted with PMCI and other workgroups within DMTF
- The current proposal utilizes existing hardware interfaces, originally defined for IPMI, to provide Redfish user credentials to the host
  - This has the significant benefit of working on existing hardware and operating systems, **allowing implementation across vendors on existing products**

Feedback on security approach

- Any mechanism to provide credentials raises security concerns
  - Local Host Authentication is not appropriate for every situation, and would be disabled (or configured with limited permissions) in high security environments
  - Users should be able to choose the balance between security and compatibility with existing tools or processes
- The goal is to be *secure enough for most users or deployments*
  - The difficulty is deciding what counts as "enough"
  - There is no perfect solution – all options come with tradeoffs
  - The Redfish Forum is seeking input from the community
- The proposal has three implementation options to share credentials between the BMC and the host OS…

Summary of options for credential sharing

- Option #1 – Host retrieves plain text password from the BMC
  - A “Keep It Simple” approach
  - Similar level of security to existing in-band IPMI
  - **This option is the recommendation of the Redfish Forum**
- Option #2 – Host sends hashed password to the BMC
  - Moderately complicated approach
  - Potentially more secure than Option #1
- Option #3 – Encryption
  - Not actively being considered – included here for completeness
  - Much more complicated than other options

Assumptions common to all options

- The IPMI Host Interface (KCS, SMBUS, etc.) provides a *sufficiently secure* transport between host and BMC, and doesn’t need an additional layer of security or encryption added on top of it
  - The host interface hardware makes it difficult or impossible for an external attacker to observe the messages between BMC and host
  - The threat model for Local Host Authentication is external attackers
- Products intended for deployment into high security environments would have the option to disable this functionality
  - Choice could be made by manufacturer or end user

Option #1 – Host retrieves plain text password from BMC

- BMC generates a random password, and host retrieves the password in plain text using the IPMI Host Interface
  - Easy to implement for both host and BMC
  - Doesn’t require that BMC receive hardware notification of host reboot
  - Doesn’t require coordination between host applications
  - Works in UEFI pre-boot environment

- This is the path recommended by the Redfish Forum
  - Based on ability to implement and deploy quickly
  - Gain overall security benefits of moving to Redfish and away from legacy management interfaces

Option #2 – Host sends hashed password to the BMC

- Host generates random password and sends salted hash to the BMC using the IPMI Host Interface
  - Plain text password is never sent
    - This removes the assumption that the IPMI Host Interface cannot be observed
  - Moderate implementation effort for both host and BMC
    - Some scripting languages won’t be able to generate password hash
  - May require that BMC receive hardware notification of host reboot
  - Host applications must cooperate to share credentials
    - Credentials are established by first application that needs them
    - Must save credentials so other applications can use them
  - Difficult for UEFI to use because no way to share credentials with OS

Option #3 – Encryption

- Encrypt all communication between host and BMC
  - Host and BMC agree on shared encryption key
    - Possibly using ECDHE
    - Still relies on Host Interface hardware for assurance that host is communicating with BMC and not a “man in the middle.”
  - Host and BMC then proceed with option #1 or #2, but with encryption
  - Significant implementation effort for both host and BMC
    - Some scripting languages won’t be able to perform the needed cryptographic operations

Call To Action

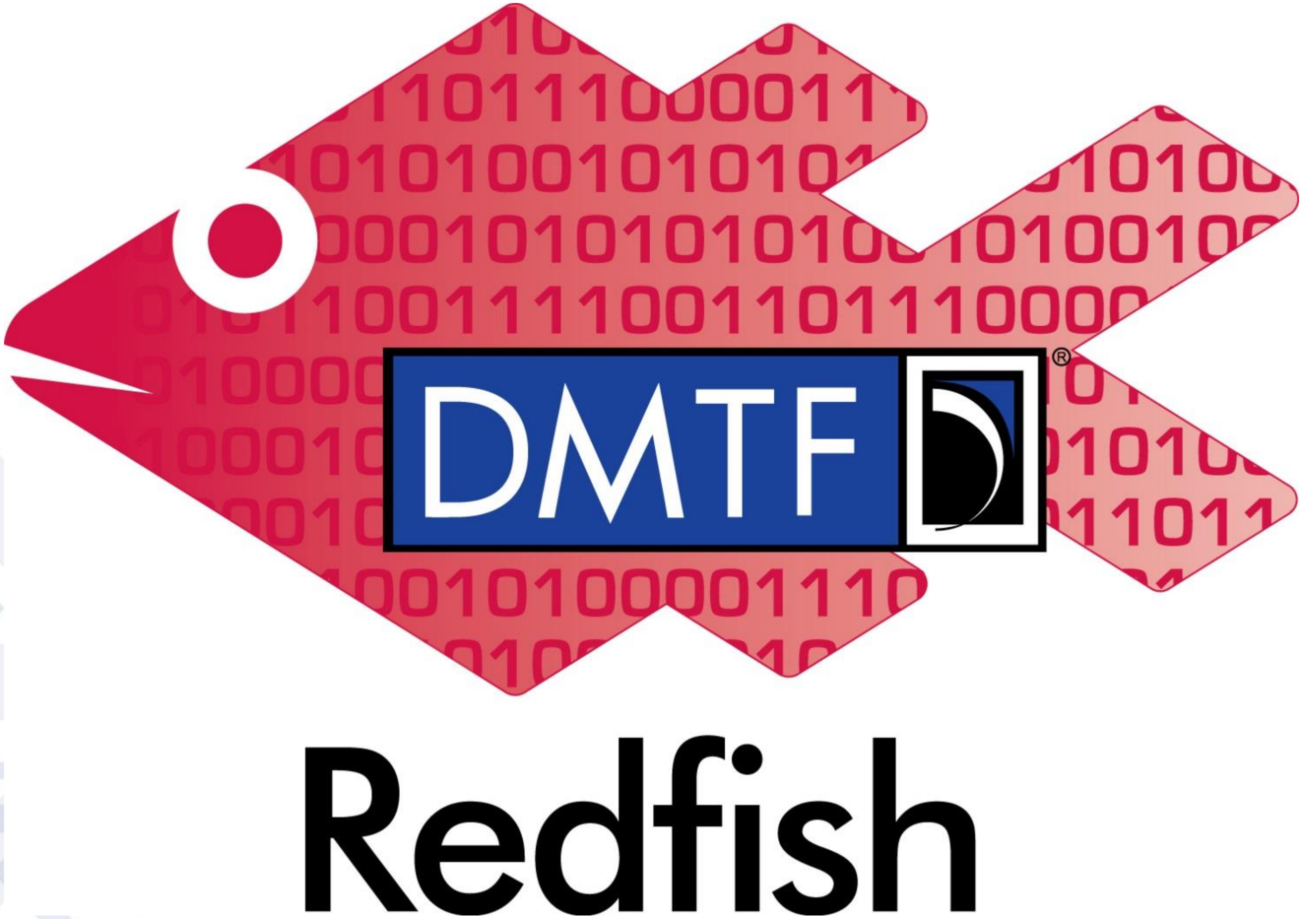
- The Redfish Forum desires feedback from the community on which security option is most appropriate for next release of the specification
  - Recommended path is to utilize “Option #1” to share credentials with the host operating system

- Feedback can be provided via multiple paths:
  - Post feedback on the Redfish User Forum
  - Provide feedback through the DMTF feedback portal
  - Contact Redfish Forum member company representatives

Getting involved in Redfish

- Redfish Standards page
  - Schemas, Specs, Mockups, White Papers & more
  - http://www.dmtf.org/standards/redfish
- Redfish Developer Portal
  - Redfish Interactive Resource Explorer
  - Educational material, documentation & other links
  - http://redfish.dmtf.org
- Redfish User Forum
  - User forum for questions, suggestions and discussion
  - http://www.redfishforum.com
- DMTF Feedback Portal
  - Provide feedback or submit proposals for Redfish standards
  - https://www.dmtf.org/standards/feedback
- DMTF Redfish Forum
  - Join the DMTF to get involved in future work
  - http://www.dmtf.org/standards/spmf

Q&A & Discussion



www.dmtf.org