SWIFT Security Controls

The Role of Privileged Access Management

WALLIX | 2017

WALLIX
TRACE, AUDIT & TRUST

SWIFT Security Controls:

The Role of Privileged Access Management

ABSTRACT

SWIFT provides a framework for customer security controls. It enables global financial institutions to exchange sensitive financial transaction information. Given the huge sums transacted by SWIFT clients, cybersecurity is a high priority. Realizing the framework's goals involves devising controls that cover issues of physical security, credentials and user identities. Privileged Access Management (PAM), which governs access to administrative back ends, is critical to the success of the entire framework. This eBook describes how PAM makes the framework's implementation possible.

WALLIX
TRACE, AUDIT & TRUST

INTRODUCTION

The Society for Worldwide Interbank Financial Telecommunication (SWIFT), the global banking information network, presents a high value target for cyber-attackers. The service facilitates over $5 trillion in bank transfers every day. Concern over customer vulnerabilities has led SWIFT to publish a framework for customer security controls. The framework is designed for SWIFT members to secure their SWIFT environments and to limit access, detect, and respond to security threats.
The framework includes controls affecting physical security, credentials and identities. As a result, Privileged Access Management (PAM), which governs access to administrative back ends, is critical to the framework's success. This eBook describes how PAM is essential to operating system privileged account control, internal data flow security, operator session confidentiality and integrity, physical and logical password storage, logging, and monitoring.

SWIFT at a Glance

The Belgium-based SWIFT provides its members with a network to send and receive information about financial transactions worldwide in a reliable, secure, standardized environment. They also sell software and services used on the SWIFTNet Network. SWIFT links over 11,000 financial institutions in more than 200 countries and territories. Collectively, SWIFT members exchange in excess of 15 million transaction messages per day.

The SWIFT Customer Security Controls Framework 1.0

SWIFT does not handle actual funds. It sends payment orders. Nevertheless, unauthorized access to the SWIFT network could wreak havoc on a financial institution and cause potentially large financial losses. As part of its Customer Security Programme (CSP), SWIFT has published its Customer Security Controls Framework. Comprising 27 mandatory and advisory security controls, the framework is designed to establish a security baseline for the entire SWIFT community. Mandatory controls must be implemented by all users on their local SWIFT infrastructures. SWIFT requires an attestation process to ensure that members are adopting the controls.

The Framework is based on the objectives of 'Secure your Environment', 'Know and Limit Access' and 'Detect and Respond'. Its controls address financial, legal, regulatory, and reputational risk among SWIFT member institutions. The Framework identifies a number of major areas of risk, including:

- Unauthorized sending or modification of financial transactions
- Processing of altered or unauthorized SWIFT inbound transactions
- Business conducted with an unauthorized counterparty
- Confidentiality breach (of business data, computer systems, or operator details)
- Integrity breach (of business data, computer systems, or operator details)

PAM and the SWIFT Customer Security Controls Framework

Management of administrative access is essential to many of the SWIFT security controls. The Framework's objectives, especially "Know and Limit Access" are intended to prevent unauthorized people from accessing sensitive data and messages. For example, to restrict unauthorized sending or modification of financial transactions, the institution has to be in control of who has authorization.

Similarly, being able to prevent the conducting of business with an unauthorized counterparty requires being aware of who can and cannot authorize a counterparty - and being able to track administrative sessions where counterparties have been authorized. This is the province of Privileged Access Management (PAM).

What is PAM?

PAM is a collection of processes and tools that give a SWIFT member visibility and control over who accesses privileged or administrative systems and the data they host. A privileged user is a user with a very wide access to a system, to its configuration, and to the resources it hosts. For example, he or she can create and modify user accounts, access and delete data, and so forth. PAM is about governing who has privileged access, when they have access, and what privileged users are doing during their admin sessions.

A PAM solution enables the IT department to grant and revoke privileged access. Capabilities vary, but the best PAM solutions make it possible to manage and to monitor administrative access in a real-time, fine-grained manner. They log privileged sessions and track administrative steps taken during each session. Having this information makes it easier to respond to a security incident or prove compliance with a security policy.

The Role of PAM in Implementing Framework Controls

Twelve of the Framework's controls directly involve PAM. By analyzing the Control Objective for each of them, we can understand how managing privileged access will make the control effective. In addition, having the PAM logs for the implementation of these controls will aid in the attestation processes called for by the SWIFT Framework.

1.1 SWIFT Environment Protection (Mandatory) – Control Objective: *"Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment."*

Protecting local SWIFT infrastructure requires clustering, awareness of, and control over privileged access. Thus, PAM is an effective countermeasure to IT systems' being compromised, a protection for the heart of the infrastructure. PAM makes this happen by securing access with reinforced password protection and authorizations, as well as session monitoring and recording.

1.2 Operating System Privileged Account Control (Mandatory) - Control Objective: *"Restrict and control the allocation and usage of administrator-level operating system accounts."*

This control is specifically about PAM. A PAM solution is needed to restrict and control the allocation and usage of administrator-level system accounts. The solution controls authorization workflows, limits access according to the need of use and manages passwords while providing a portal that supervises and centralizes all the activities and users on privileged accounts.

2.1 Internal Data Flow Security (Mandatory) - Control Objective: *"Ensure the*

confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC."

A PAM solution establishes who can and who cannot access SWIFT-related application settings for data flows. If the administration of SWIFT-related application security settings is not well-managed, there is the potential for fraud or negligence leading to data breaches. PAM administrators can protect data flows by choosing the appropriate communication protocols between applications and PC operators. For example, a secured protocol such as SSH ensures the confidentiality, integrity and authenticity of data flows.

2.4A Back-office Data Flow Security (Advisory) - Control Objective: *"Ensure the confidentiality, integrity, and mutual authenticity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components."*

As some recent major data breaches have shown, it is the connections between systems that expose an organization to risk. Here, SWIFT is advising its members to enact countermeasures that ensure the integrity and confidentiality of data flowing between SWIFT and applications like middleware. For example, a bank might use an Enterprise Service Bus (ESB) to link mainframe-based banking software with SWIFT infrastructure.

To make sure the data flows are secure, a PAM solution can enforce access policies for the administration of the ESB and its security settings, e.g. requiring security assertions, certificates, or data encryption in messages while in transit. PAM solutions also offer Application-to-Application password management. This allows for the storing and provisioning of credentials in a vault so that a back office application and a SWIFT infrastructure component can authenticate safely.

2.6A Operator Session Confidentiality and Integrity (Advisory) - Control Objective: *"Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure."*

PAM is needed to establish the security settings needed for this control. PAM's ability to conduct session monitoring guarantees that only the right auditor has access to session data and monitoring. The confidentiality and integrity of sessions are

guaranteed by the session protocols employed in the process.

2.8A Critical Activity Outsourcing (Advisory) - Control Objective: *"Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities."*

Outsourced services, especially in IT, exposes the SWIFT member to privileged access risks. A third-party employee may have privileged access to backend systems in order to perform maintenance and upgrades. A PAM solution grants access for outsourced personnel but also revokes access when the person no longer requires access or is terminated by the outsourcing firm. PAM-based session monitoring and recording add further security by controlling and tracking all remote actions and third-party users, and detecting commands executed in the system.

2.9A Transaction Business Controls (Advisory) - Control Objective: *"Restrict transaction activity to validated and approved counterparties and within the expected bounds of normal business."*

A privileged user is able to validate and approve counterparties. To implement this control, therefore, it is essential to have the ability to grant and revoke the validation privilege. A PAM solution can also limit session access to pre-defined times, provide real time alerts of suspicious activities and automatically terminate sessions that go beyond the "expected bounds of normal business." The PAM solution can tell incident response teams who approved the counterparty or if the approvals have been altered, and so forth.

4.1 Password Policy (Mandatory) - Control Objective: *"Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy."*

The best PAM solutions enable sophisticated password management and password masking, even proposing password configuration rules to impose strong password. This includes enhanced features like Application-to-Application Password Management (AAPM). For instance, if a user logs into the PAM solution to conduct a privileged session on another application, he or she user will not actually have the password for

the application. They will only know credentials necessary to access the PAM solution. This effectively reduces the risk of password hacking.

4.2 Multi-Factor Authentication (MFA) (Mandatory) - Control Objective: *"Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication."* MFA are services that can be integrated in PAM solutions. PAM and MFA work together to achieve the objectives of this control: seamless and ubiquitous integration between solutions to reinforce the identification and overall security of critical systems and data.

5.1 Logical Access (Mandatory) - Control Objective: *"Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts."* A PAM solution makes it possible to define and enforce the policies of need-to-know, least privilege and segregation of duties.

- Using PAM, a super-admin can easily create clusters and sub-groups of privileged accounts and users to segregate duties and privileges. A PAM super-administrator can easily see who has access to which system as well as overlaps in privilege that affect segregation of duties, e.g. an admin who has access both the SWIFT and transactional accounting systems.

- "Need to know" - PAM logs or monitors access to control data in real time. Each user has individual access to appropriate resources.

- "Least privilege" - Target access to each resource is controlled by accessing different accounts with different privileges on the same resource.

- "Segregation of duties" - The PAM solution defines several roles with different rights, such as administrator, auditors, users and so forth.

5.4A Physical and Logical Password Storage (Advisory) - Control Objective: *"Protect physically and logically recorded passwords."*

Some PAM systems can store and mask the passwords for physical devices. A PAM solution with a password vault and up-to-date security algorithms ensures that even if a user can

gain access to a physical device, he or she cannot log into it and modify its settings.

6.4 Logging and Monitoring (Mandatory) - Control Objective: *"Record security events and detect anomalous actions and operations within the local SWIFT environment."*

In many security incidents, the "anomalous" actions that set off the breach are privileged account sessions, e.g. creating a phantom user with special access privileges. A good PAM solution will be able to monitor privileged sessions and flag suspicious administrative sessions in real time, or automatically terminate a dangerous session. It will also record the details of administrative sessions so incident response teams can quickly understand what has happened in the attack. This includes the export of logs to Security Incident and Event Management (SIEM) solutions to enable cross-referencing of incident data with other security systems.

Indirect Effects of PAM on the Framework

The controls described above are directly related to PAM. However, PAM bears on virtually every other control in the Framework. The configuration of interdependent systems affects how secure they will be under the Framework controls. For example, the mandatory control 2.3 for System Hardening has the objective *"Reduce the cyber-attack surface of SWIFT-related components by performing system hardening."* System hardening varies from organization to organization. The process of hardening is done by privileged users. Even though the control itself is not about access or identity, PAM is critical for its successful execution.

CONCLUSION

SWIFT members are vulnerable to cyber-attack. To help mitigate the risk of fraud and data breaches, the organization has published a framework for customer security controls. These controls cover a range of countermeasures affecting physical security, credentials and identities. Management of privileged access is at the root of many of these controls. Controlling and monitoring access to administrative back ends makes the entire framework possible. Selecting an effective and adaptable PAM solution will make implementation of the framework successful.

WALLIX
TRACE, AUDIT & TRUST

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

As digitalization impacts companies' IT security and data integrity worldwide, it poses an even greater challenge if the data involved is highly sensitive. The recent regulatory changes in Europe (NIS/GDPR) and in the United States (NERC CIP/Cyber Security Directorate) urge companies belonging to sensitive sectors to place cybersecurity at the heart of their activity.

In response to these challenges, WALLIX created a bastion designed to secure organizations' core assets while adapting to their daily operational duties: WALLIX ADMINBASTION Suite. The WALLIX bastion accompanies more than 100 operators in sensitive sectors to conform with regulations and over 400 organizations in the protection of their critical assets, securing the access to more than 100,000 resources throughout Europe and the MEA region. It was also the first government-certified solution in the market.

WALLIX partners with a trained and certified network of over 90 resellers and distributors that help guarantee effective deployment and user adoption.

WALLIX is the first European cybersecurity software editor to be publicly traded and can be found on EuroNext under the code ALLIX. As one of the leaders of the PAM market, major players trust WALLIX to secure access to their data: Danagas, Dassault Aviation, Gulf Air, Maroc Telecom, McDonald's, and Michelin are among them.

WALLIX is the founding member of Hexatrust. The WALLIX bastion was elected "Best Buy" by SC Magazine and awarded at the 2016 Computing Security Awards, BPI Excellence, and Pôle Systematic.

Twitter: @wallixcom
More information on: www.wallix.com

OFFICES & LOCAL REPRESENTATIONS

WALLIX FRANCE (HQ)
http://www.wallix.com/fr
Email : sales@wallix.com
250 bis, rue du Faubourg Saint-Honoré
75017 Paris - FRANCE
Tél. : +33 (0)1 53 42 12 90
Fax : +33 (0)1 43 87 68 38

WALLIX UK
http://www.wallix.co.uk
Email: ukinfo@wallix.com
1 Farnham Rd, Guildford, Surrey,
GU2 4RG,UK
Office: +44 (0)1483 549 944

WALLIX DEUTSCHLAND
http://www.wallix.de
Email: deinfo@wallix.co
Landsberger Str. 398
81241 München
Phone: +49 89 716771910

WALLIX USA (HQ)
http://www.wallix.com
Email: usinfo@wallix.com
World Financial District, 60 Broad Street
Suite 3502, New York, NY 10004 - USA
Phone: +1 781-569-6634

WALLIX RUSSIA & CIS
http://www.wallix.com/ru
Email: wallix@it-bastion.com
ООО «ИТ БАСТИОН»
107023, Россия, Москва,
ул. Большая Семеновская, 45
Тел.: +7 (495) 225-48-10

WALLIX ASIA PACIFIC
(Bizsecure Asia Pacific Pte Ltd)
Email: contact@bizsecure-apac.com
8 Ubi Road 2, Zervex 07-10
Singapore 408538
Tel: +65-6333 9077 - Fax: +65-6339 8836

WALLIX AFRICA
SYSCAS (Systems Cabling & Security)
Email: sales@wallix.com
Angré 7ème Tranche Cocody
06 BP 2517 Abidjan 06
CÔTE D'IVOIRE
Tél. : (+225) 22 50 81 90

www.wallix.com