Authentication and Authorization on Dräger Devices

Cybersecurity in Hospitals

Dräger

Technology for Life

Introduction

The advantages of networked medical technology have become increasingly apparent in recent years and were clearly demonstrated in the SARS-CoV-2 pandemic. With increased connectivity, stand-alone medical devices are no w exposed to networks and allow for extended functionalities, such as distributed alarming and remote access to data or device functions. Recent attacks have shown that critical infrastructure like healthcare is no longer out-of-scope for attackers like ransomware groups and other malicious actors.

To allow for secure operations within the hospital environment, Dräger devices are developed to protect against unauthorized access to device functions and data, while maintaining usability. Across all Draeger device interfaces, different authentication and authorization mechanisms are employed to ensure adequate levels of protection.

Usability aspects – especially regarding patient safety – are a central consideration during the development of authentication mechanisms. While the prevention of unauthorized access is highly desirable, the authentication mechanism must not negatively impact clinical treatment and patient safety by preventing or delaying authorized access.

In addition to the user-to-device access, device-to-device access via a medical network is also critical. This paper will provide you with an overview on the authentication & authorization controls we have implemented in our embedded medical devices in both aspects, user-to-device and device-to-device access.*

Based on the widely accepted NIST Cybersecurity Framework (Fig. 1), we will give you insights into how we protect devices from unauthorized access, how our devices help detect potentially malicious access and how responsible organizations can best respond to such situations.

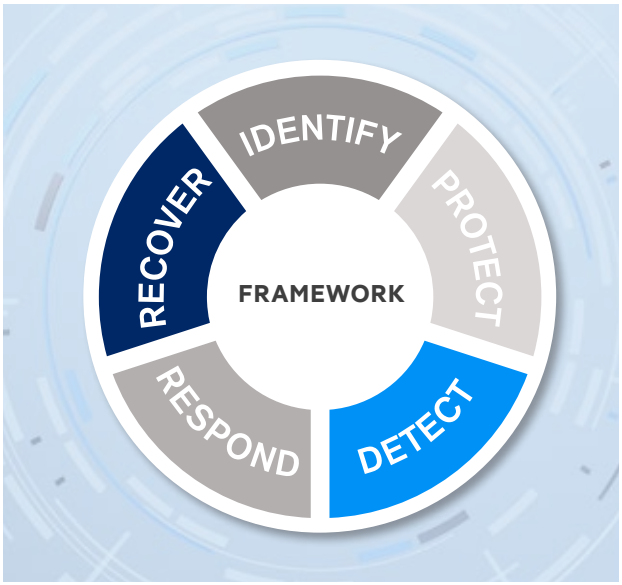

Fig. 1: Functions of the NIST Cybersecurity Framework

While all 5 NIST functions are important to a holistic approach to security, authentication and authorization supports specifically the protect function. However, our devices are also able to help with the detect and respond functions, but there will responsibility on our customers end to act upon this help.

* Valid for all devices currently under development or recently launched. Does not apply to legacy devices.

Protect

Role-based Authentication & Authorization

Dräger devices employ a role-based access control model, in which all device functions span across four defined roles. One role does not need to authenticate at all to access clinical application functionalities, 2 roles authenticate via the user interface, each of which is explained in the following section. The fourth role is authorized to access critical device functions and needs to connect to the device and **authenticate via the network interface.** This is explained in more detail in the service network authentication section.

User Interface Authentication

Our devices are controlled locally via the means of graphical user interfaces. On the one hand, unauthorized access to the device functions must be prevented, while on the other hand, rapid access for caregivers must be ensured throughout the care process and in emergency situations. This illustrates the challenge of balancing security concerns with usability aspects.

Standard User operations, like changing device parameters during clinical use, may be performed without authentication via physical access to the user interface of the device.

Advanced User operations are e.g. changing default alarm limits and authenticate with changable group passcodes via the user interface.

Service User (e.g. Biomedical engineer) are users responsible for routine inspection and maintenance of clinical devices and authenticate with changable group passcodes via the user interface.

These passcodes are individual per device after manufacturing and must be changed by the responsible organization during the set-up of the devices. Authenticated sessions expire after a set timeout, to ensure that sessions can't be used even if the authenticated user forgets to log out after leaving the device.

Network Authentication

Device-to-device authentication within medical and service networks is based on modern cryptography by utilizing industry-standard X.509-Certificates in Public-Key-Infrastructures.

These certificates can be understood as the "digital passport" identifying each "participant" in the network, with the Public-Key-Infrastructure resembling the authorities vouching for the correctness of the presented identity-information.

Service Network Authentication

Specialized Service Users are service technicians who are authorized to access critical device functions like performing software updates. This highly privileged access is only accessible via the network interface and is protected by user-individual digital certificates.

These digital certificates have a validity of 30 days and are issued only to registered specialized service users by a Dräger-wide **trusted Dräger Service Root Certificate Authority.**

Medical Network Authentication

Dräger devices can interact with each other and with compatible third-party devices via the Service Oriented Device Connectivity protocol (SDC protocol).

SDC, an ISO/IEEE 11073-standard, is a web services-based architecture that allows for interoperability between point-of-care medical devices and compatible hospital information systems [**LINK**]. SDC enables new clinical applications, such as seamless data integration, remote control of medical devices and automation of clinical workflows, taking into account the particularly high requirements for use in acute care areas, such as the operating theatre, intensive care unit and neonatal care unit.

SDC compatible devices mutually authenticate by using **device-individual digital certificates.** In order to accept connections from a device via the medical network, SDC-devices ensure that they trust the presented certificates by validating against a list of trusted **Root Certificates**. Dräger Devices are released with the **Dräger Device Root Certificate Authority**, to authenticate other Dräger devices. Third-Party devices can be authenticated by adding their respective Root Certificates into the Dräger Trust Store via **specialized service user access.**

Medical Network Authorization

Hospitals will want to control which devices may interact with each other by maintaining and distributing **access control lists** to the devices. A device's access control list contains device identifying information which will allow it to establish connections to authorized devices and systems. With this we help hospitals to manage their networks to their security, usability and maintainability needs.

To update these access control lists on Dräger devices, **specialized service user** access is required.

Detect

Dräger devices are implemented to detect and log several **Indicators of Compromise,** so called **Security Events.** These events range from repeated failed login-attempts via the user interface to expired device certificates in connection attempts. All identified Security Events are logged in tamper-proof log entries, by utilizing – where available – hardware-backed cryptographic message authentication codes.

Respond

To enable hospital IT-security staff to act swiftly on certain Security Events, relevant events are distributed via the technical means of SNMP-Traps into the hospital network, and can be received by one of the several readily available network management tools on the market. Thereby, an integration into hospital's Security Information and Event Management (SIEM) system is possible.

Corporate Headquarters
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23558 Lübeck, Germany

www.draeger.com

Region Europe
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23558 Lübeck, Germany
+49 451 882 0
+49 451 882 2080
info@draeger.com

Region Asia Pacific
Draeger Singapore Pte. Ltd.
61 Science Park Road
The Galen #04-01
Singapore 117525
+65 6872 9288
+65 6259 0398

Manufacturer:
Drägerwerk AG & Co. KGaA
Moislinger Allee 53–55
23542 Lübeck, Germany

Region Middle East, Africa
Drägerwerk AG & Co. KGaA
Branch Office
P.O. Box 505108
Dubai, United Arab Emirates
+971 4 4294 600
+971 4 4294 699
contactuae@draeger.com

Region Central and South America
Dräger Indústria e Comércio Ltda.
Al. Pucurui - 51 - Tamboré
06460-100 - Barueri - São Paulo
+55 (11) 4689-4900
relacionamento@draeger.com

Locate your Regional Sales Representative at:
www.draeger.com/contact

102605 | 2310-2 | PR | LE | Subject to modifications | © 2023 Drägerwerk AG & Co. KGaA