imc
part of Scheer

Security Whitepaper

imc Learning Suite
Information security

im-c.com

Security Whitepaper

imc Learning Suite
Information security

Author(s): Christoph Gast, Patrick Pekczynski
Date: 2022-07-12

Document	Description
Version	ILS 14.13
Status (Draft / Review / Finalisation)	Finalisation
Contact Person(s)	Christoph Gast, Patrick Pekczynski

History	Status	Who
2016-12-13	Draft	Christoph Gast
2022-01-14	Review	Patrick Pekczynski
2022-03-15	Review	Patrick Pekczynski
2022-07-12	Review	Patrick Pekczynski
2022-07-12	Finalisation	Dr. Peter Zönnchen

imc
information multimedia communication AG
Headquarter Saarbrücken
Scheer Tower, Uni-Campus Nord
D-66123 Saarbrücken
T. +49 681 9476-0 | Fax -530
info@im-c.com
im-c.com

Content

1 Information Security

This document provides an overview of imc Learning Suite and IT security.

1.1 Confidentiality

During the electronic processing of transactions or exchange of information, it is desirable that the communication between sender and recipient remains confidential and is only accessible to the authorised persons.

1.1.1 Threat: Unauthorised information gain

Data confidentiality is threatened when a third party gains access to the transmitted or stored information. For instance, this can take place through intercepting communication or through direct access to a computer.

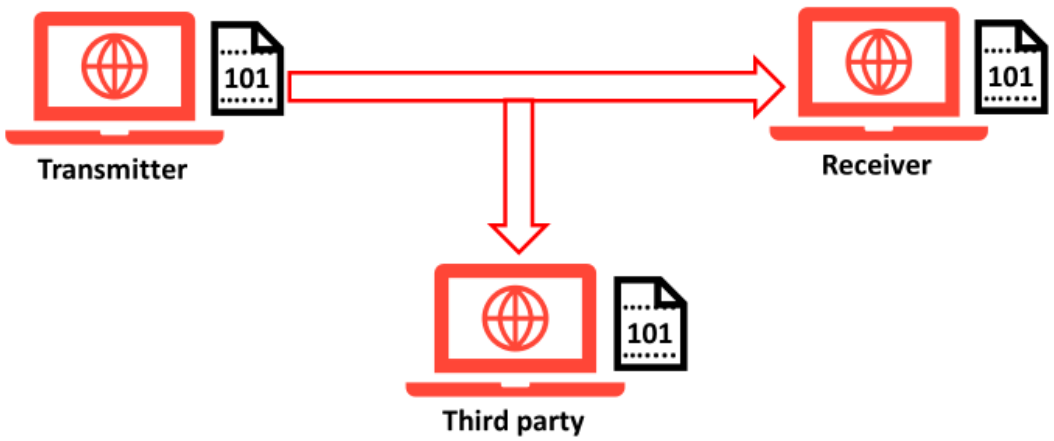

Fig. 1.1: Unauthorised information gain

1.1.2 Countermeasures: Encryption

As a countermeasure, data is often encrypted in order to make the information contained incomprehensible to third parties. imc Learning Suite facilitates secure TLS encryption between client and server and prevents interception by a third party. Further communication channels can be encrypted individually according to the security requirements. Access to computers can also be limited by means of technical measures.

1.2 Integrity

Integrity means that information is correct and unchanged. The recipient of a message assumes that the message reaches him just as the sender composed it.

1.2.1 Threat: Unauthorised modification

If a third party fraudulently modifies information this represents an attack on the integrity of the data. Modification can occur at the time of transmission or take place directly, for instance by unauthorised access to computers.

Fig. 1.2: Unauthorised modification

1.2.2 Countermeasures: Encryption and redundancy

When information is encrypted, the attacker cannot make any meaningful changes as he is not able to see the content. Another option is the use of redundancy. Through redundancy, a recipient can detect whether data has been modified. imc Learning Suite secures all communication using TLS encryption as well as additional token procedures and a secure session procedure. With these techniques, communication between client and server is additionally protected and data manipulation can be detected and prevented.

1.3 Authenticity

Authenticity is the assurance that information originated from a certain person.

1.3.1 Threat: Unauthorised creation

When data is generated in such a way that this data is assigned to the incorrect person, this represents an attack on the authenticity. For instance, transfers can be executed at the expense of an uninvolved person because a third party has impersonated this person.

Fig. 1.3: Unauthorised creation

1.3.2 Countermeasures: Securing identity

There are a lot of measures that should secure the identity of a person. Some of them are easier to crack, for instance, the authentication with username and password, others are more secure, like e.g. a digital signature or a fingerprint. Besides encryption and secure login data, imc Learning Suite also focuses on token procedures which prevent manipulation of identity data and make it visible in case of emergency.

1.4 Availability

Availability means the provision and functionality of data, computers and communication means.

1.4.1 Threat: Unauthorised interruption

If an IT system is not or only partly accessible or information is not accessible, this can have serious economic consequences. A denial-of-service attack (DoS) for instance, represents unauthorised interruption. Here, systems are intentionally overloaded and are no longer available or only available for a limited period.

Fig. 1.4: Unauthorised interruption

1.4.2 Countermeasures: Avoidance of "single point of failure"

Systems which cannot be paralysed by an error at one single point (single point of failure) are better protected against unauthorised interruption. This can be achieved through the use of high availability and redundant systems. When a system fails, a second, identical system steps in.
imc Learning Suite supports different system architectures which avoid a single point of failure. Thus, high system availability can for instance be achieved through clustering. Clustering means that individual system components are transferred onto separate, networked servers. Suggestions for possible system architectures are described in the technical whitepaper for imc Learning Suite.

1.5 Information on security and vulnerabilities

Further information on frequent vulnerabilities in software products can be found under the following links:

- Federal Office for Information Security (BSI):

  Comprehensive information on vulnerabilities and measures one can take to protect oneself against security risks. http://www.bsi.de

- National Vulnerability Database (NVD):

  Database listing concrete vulnerabilities in software products. http://nvd.nist.gov/

2 Standards

2.1 Transport Layer Security (TLS)

The encryption protocol *Transport Layer Security* (TLS) is a further development of *Secure Sockets Layer* (SSL) protocol and facilitates secure data transmission between two applications (confidentiality and integrity of the communication).
The benefit of TLS protocol is it's independency of application protocols such that different protocols can be secured using TLS. An example of this is the *Hypertext Transfer Protocol* (HTTP). If an application offers HTTP and supports a secure communication channel for data exchange it is available via the uri-scheme "https". In this context one has to consider that "https" can refer to either SSL or TLS encryption.
BSI (TR-02102-2, 2021) and NIST (SP800-52, 2019) recommend to use at least TLS version 1.2.
imc Learning Suite provides the opportunity to encrypt the communication between client and server using TLS. This allows different encryption algorithms to be implemented and the certification key can be selected according to the security requirement.

Generally TLS facilitates

- authentication of the communication partners
- confidentiality of data through encryption
- integrity of data using hash values as checksums

2.2 EV-SSL/TLS certificates

Furthermore, imc Learning Suite supports so-called Extended Validation SSL/TLS certificates (EV-SSL/TLS). For an EV- SSL/TLS certification, the client must undergo further inspection by a certification body. Identity and business address of the client are checked amongst other things. Websites with EV-SSL/TLS-certification are identified in the browser by company name highlighted in green in the address bar.

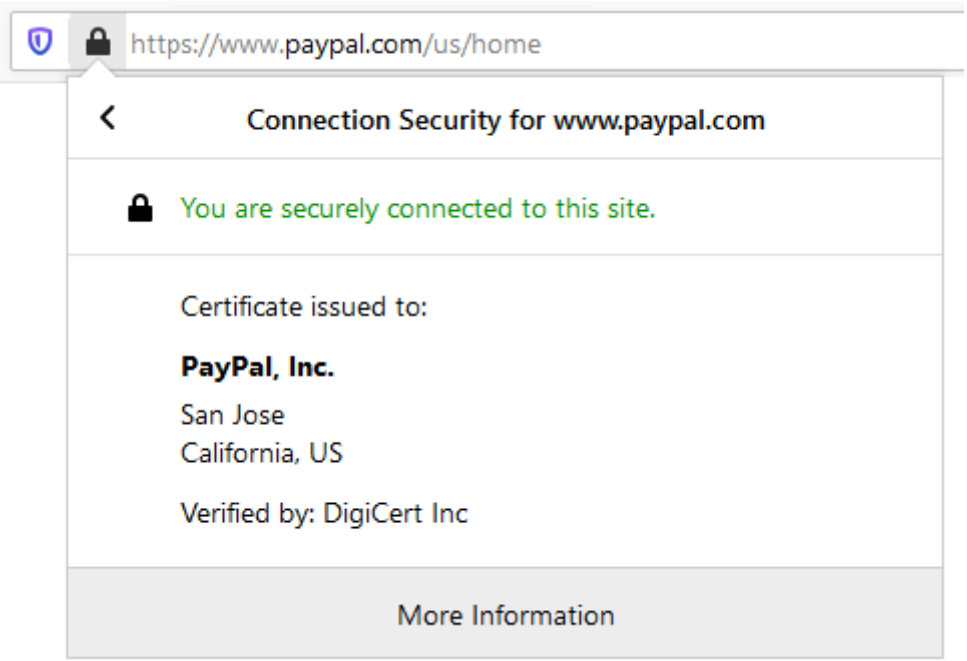

Fig. 2.1:Example of a website with EV-SSL certification

EV certificates are used for instance in online banking.

2.3 SHA-2 family of hash functions

The SHA-2 family (Secure Hash Algorithm 2) of hash functions is the generic term for the four cryptological hash functions SHA-224, SHA-256, SHA-384 and SHA-512, standardised by the US NIST in 2001 as the successor to SHA-1. To generate the hash value with SHA-256, the source data is divided into 512-bit blocks or 16 32-bit words and iteratively calculated with 64 constants and six logical functions. The process begins with a start hash of eight 32-bit words. The first 32 bits of the decimal part of the square roots of the first eight prime numbers (2 to 19) are used for this.

imc Learning Suite uses hash functions of the SHA-2 family for functionalities that require a so-called “digital fingerprint” of data. With these one-way functions it can be determined whether a user is in possession of a certain text (e.g. password). During the password check in imc Learning Suite, the hash values of the entered and stored password are compared to each other. The procedure is made even more secure by using multiple security mechanisms.

The hash function to be used can be configured in imc Learning Suite. The default setting is SHA-256 and follows recommendations of BSI (TR-02102-2, 2021) and NIST (SP800-107, 2012).

2.4 Encryption standards

2.4.1 Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a FIPS[1]-approved encryption standard that can be used to protect electronic data (FIPS-197 AES, 2001).

imc Learning Suite uses AES amongst others to create encrypted URLs for content access (“securedata”). Regarding the AES configuration imc Learning Suite follows recommendations of BSI (TR-02102-2, 2021) and NIST (SP800-38A , 2001) using AES/CBC/PKCS5PADDING as default with a key length of 128-Bit.

[1] FIPS – Federal Information Processing Standard

2.5 Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP, 2022) is a non-commercial organisation. The aim of OWASP is to improve software security. OWASP draws attention to frequent vulnerabilities and helps to mitigate these. Further, OWASP defines standards for secure development and application of software.

2.5.1 OWASP Top 10

An important OWASP publication is the OWASP Top 10 of the most critical security risks to web applications (OWASP Top 10, 2021).
imc follows OWASP standards when further developing imc Learning Suite. The tools and libraries recommended by OWASP are used in order to adapt the security of imc Learning Suite to the required standards; imc subjects imc Learning Suite permanently to new tests and thus ensures that the level of security is adhered to throughout all patch and release cycles and is increased through additional security measures.

3 imc Learning Suite security measures

Below, you will find a selection of security measures integrated into imc Learning Suite.
Advanced concepts for security experts can be introduced in the context of a non-disclosure agreement.

3.1 Authorisation and visibility concepts

The following chapter describes measures which users of imc Learning Suite can implement themselves or which have to do with user input into the system.

3.1.1 Profile data

At different places in imc Learning Suite, user profiles can be displayed or users can input data. Profiles contain personal information on individual people like for instance their name or email address. For instance, a user can record the contact details of other users or search for people in their address book.
imc Learning Suite offers the opportunity to display different data according to context and user or to make different input fields available. Thus, you can determine precisely which personal data is to be entered in imc Learning Suite and which of these profiles is visible to other users. Thus, imc Learning Suite supports different levels of confidentiality which is flexibly adaptable depending on the context.

3.1.2 Organisational chart

Each organisation or company who uses imc Learning Suite has its own internal structure. This structure can be illustrated in detail via client, group and approval management.

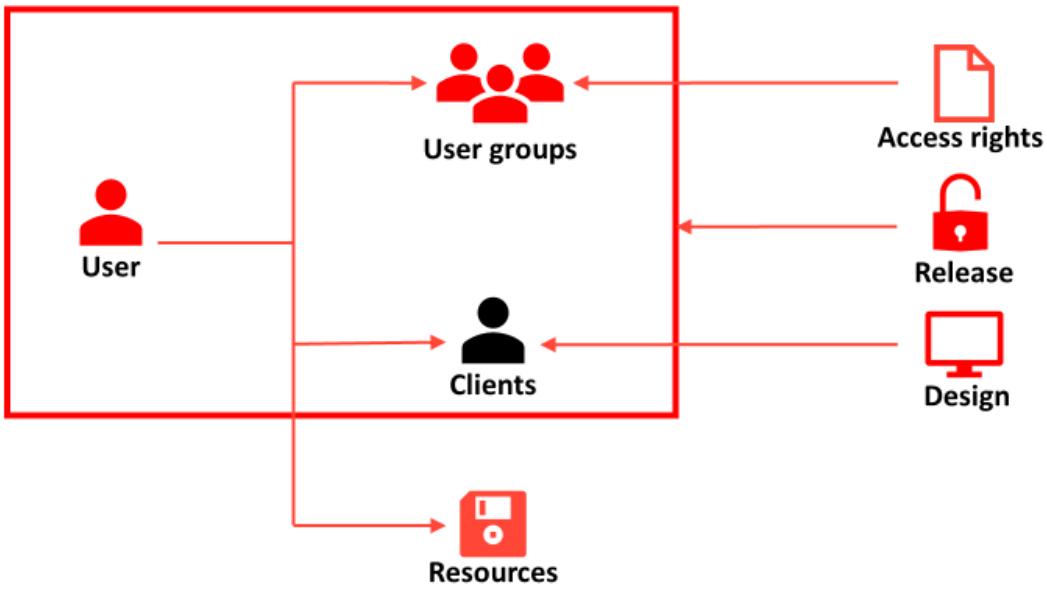

Fig. 3.1: Organisational chart

Clients

Clients serve to divide a single physical system into multiple partial systems. The sub-systems can for instance, represent different departments within an organisation and can also differ in design. Different settings in imc Learning Suite can be made client-specific such as, for instance, the determination of a recipient group for a message. Any number of clients can be created.

User groups

Individual users can be broken down into user groups. Via user groups, it is controlled which functions are accessible to members of a user group. For example, it is possible to determine which navigation menus are visible and which functions the group members can find there. Any number of user groups and sub-groups can be defined.

Releases (ACL)

Via an Access Control List (ACL), the releases of objects for users, user groups and clients are determined. Release represents an access right. For each object in imc Learning Suite (e.g. a certain type of content) it can be defined which users, user groups or clients have access to this object. For each object, only those specific rights which are required for administration clearances exist, for example, "Edit", "Delete" or "Release".

Organisational chart

Through the combination of client and group affiliation and release, one can define for each person which content this person can see, how the content is presented and to which functions the person has access to. The imc Learning Suite organisational chart thus supports optimal confidentiality and content integrity. Users only see the content which is destined for them and can only make changes or access functions to which they have access.

3.1.3 Passwords

Autocomplete

Login to imc Learning Suite takes place using a unique combination of user name and password. Depending on how the used browser is set up, this login data is possibly saved in the browser. In this way, the user does not need to enter the login data every time, rather the browser fills in the login fields automatically (autocomplete = auto-completion). The disadvantage of this is that attackers can possibly upload and misuse this saved login data.
imc Learning Suite prevents automatic saving of login data in the browser. Thus, it makes no difference whether users have activated the autocomplete function in the browser or not. The passwords of the internet sites remain unaffected.

Identical passwords

If a user creates a password for their imc Learning Suite access, a hash value of the password (“digital fingerprint”) is saved in the imc Learning Suite databas. If different users randomly select identical passwords, then normally the hash values of these passwords are also identical. Thus, for example, a malevolent administrator who has access to the imc Learning Suite database can compare password hashes and draw conclusions from them.
In order to avoid this, imc Learning Suite adds a personal random sequence of characters to each password, which is called "salt" in computer cryptography. This sequence of characters is added to the password and causes that the password hashes are never identical, even if the password plain texts are identical.

3.1.4 Account locking

Logging into imc Learning Suite is executed by using a username and password. If a user consecutively enters the wrong password several times, imc Learning Suite automatically locks the user account for security reasons (Account Locking). This account locking results in the individual user beinge temporarilty locked out of the application. However, it is important that the system with the ability to lock accounts is protected against brute-force attacks on user passwords. Brute-force means that an attacker tries passwords until he has eventually cracked one of the passwords and thus can potentially cause greater damage. Locking the account prevents this.
The number of login attempts until account locking occurs and the period up to automatic unlocking can be configured.

3.1.5 Audit Log

In the audit log, participant-related data such as, for example, the booking date or the booking status of a course is managed and logged. Changes trigger by the course participant are also logged in the audit log.
The audit log is usually only accessible to trained administrators. With the audit log, an administrator can trace when, where and by which person changes have been made. If these changes were unintentional, for example, if a participant has accidentally ended a course early, these changes can be reversed.
With the audit log, imc Learning Suite administrators have access to an important tool through which data integrity can be ensured.

4 Penetration tests

A penetration test, also referred to as pentest, is a comprehensive security test of an IT system or software. Based on the methods which a possible attacker would use in order to penetrate a system, potential vulnerabilities are systematically revealed.
The goals of a penetration test are

- detection of weak spots,
- detection of errors which can occur through incorrect operation,
- increase of application security.
- confirmation of IT security through an independent third party.

imc regularly has penetration tests performed for imc Learning Suite. The results of the tests are incorporated into new patches, service packs and releases of imc Learning Suite.

5 References

BSI Bundesamt für Sicherheit in der Informationstechnik. (12. März 2021). Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. (Version 2021-01). Deutschland. Abgerufen am 22. 06 2021 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=2

NIST National Institute of Standards and Technology. (26. 11 2001). FIPS 197 Announcing Advanced Encryption Standard (AES). United States of America. doi:https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

NIST National Institute of Standards and Technology. (12 2001). Special Publication 800-38A Recommendation for Block Cipher Modes of Operation Methods and Techniques . (2001 Edition). United States of America. doi:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

NIST National Institute of Standards and Technology. (08 2012). Special Publication 800-107 Recommendation for Applications Using Approved Hash Algorithms. (Revision 1). United States of America. doi:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf

NIST National Institute of Standards and Technology. (08 2019). Special Publication 800-52 Guidelines for the Selection,Configuration, and Use of Transport Layer Security (TLS) Implementations. United States of America. doi:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

Open Web Application Security Project (OWASP). (2021). *OWASP Top 10 - The Ten Most Critical Web Application Security Risks*. doi:https://owasp.org/Top10/

Open Web Application Security Project (OWASP). (2022). *Open Web Application Security Project*. doi:https://owasp.org/