Security for CompTIA Tech+

Explain Fundamental Security Concepts and Frameworks



Phil Chapman
Senior Instructor and Subject Matter Expert

www.cyberphil.co.uk

Course Introduction

Security for CompTIA Tech+ (FC0-U71)

New starters in the world of IT

Non-technical staff

Refresh of foundation IT concepts

Course Introduction

CompTIA Tech+ Exam Objectives (Domains)

- 1.0 IT Concepts and Terminology (14%)
- 2.0 Infrastructure (22%)
- 3.0 Applications and Software (18%)
- 4.0 Software Development Concepts (14%)
- 5.0 Data and Database Fundamentals (14%)
- **6.0 Security (18%)**

Course Introduction

About the exam (FC0-U71)

- Number of questions: 75
- Type of questions: multiple choice
- Length of test: 60 minutes
- Passing score: 650 *(on a scale of 100-900)*

Comptia.org/certifications/comptia-tech-plus

Course Introduction

Security for CompTIA Tech+ (Domain 6)

- 6.1 Explain fundamental security concepts and frameworks
- 6.2 Explain methods to secure devices and security best practices
- 6.3 Explain password best practices
- 6.4 Identify common use cases for encryption
- 6.5 Given a scenario, configure security settings for a small wireless network
- *Course summary, exam tips and other resources*

Up Next:

The CIA of Security

The CIA of Security



The CIA of security

- Confidentiality
- Integrity
- Availability



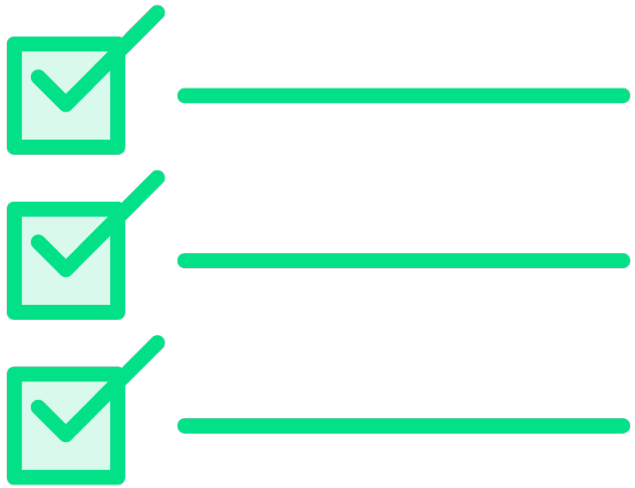
Confidentiality

- NIST: ‘Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information’
- Keeping your data and information protected from unauthorized access
- Allowing access only to those that need to know it (in order to do their job)



Maintaining confidentiality (controls)

- Cryptography – encryption
- Authentication and authorization
- Policies
- Physical security



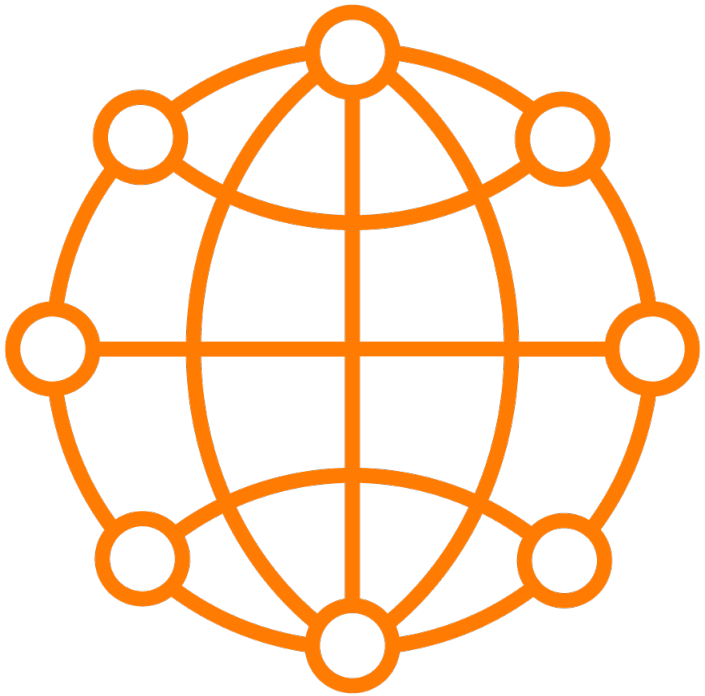
Integrity

- NIST: Guarding against improper information modification or destruction and ensuring information **non-repudiation** and authenticity
- Making sure that data is not tampered with
- Ensuring that you know where the data has come from and can trust it
- Ensuring that a user or system cannot deny sending data/information (non-repudiation)



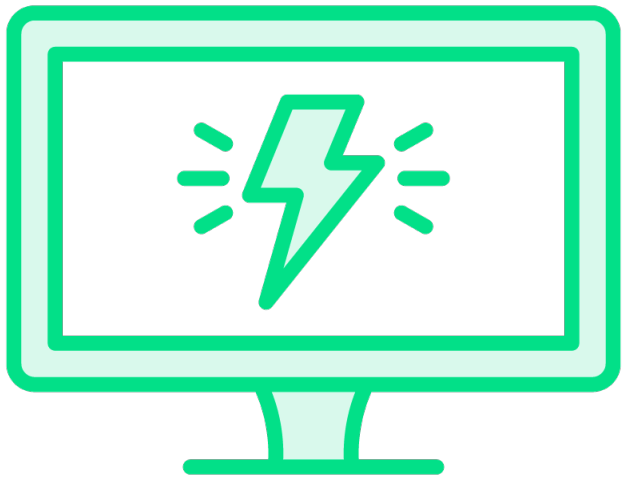
Maintaining integrity (controls)

- Cryptography – hashing
- Authentication and authorization
- Policies
- Physical security



Availability

- NIST: Ensuring timely and reliable access to and use of information
- Ensuring that data and systems are available to those that need it, when they need it



Maintaining availability (controls)

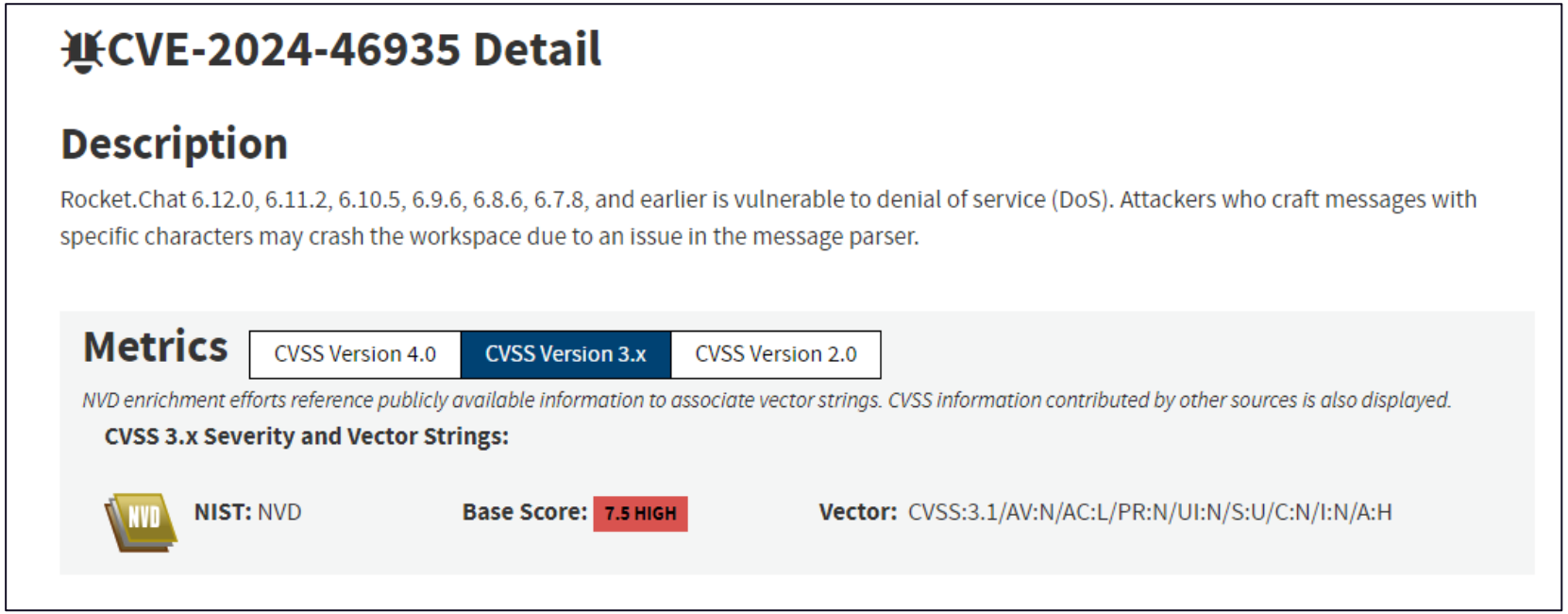
- Redundant systems
- High availability systems
- Maintenance and monitoring
- Patching
- Physical security



The CIA model

- Underpins all aspects of data and information security
- Includes system security (infrastructure)

How Is the CIA Model Used?



CVE-2024-46935 Detail

Description

Rocket.Chat 6.12.0, 6.11.2, 6.10.5, 6.9.6, 6.8.6, 6.7.8, and earlier is vulnerable to denial of service (DoS). Attackers who craft messages with specific characters may crash the workspace due to an issue in the message parser.

Metrics

CVSS Version 4.0 | **CVSS Version 3.x** | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

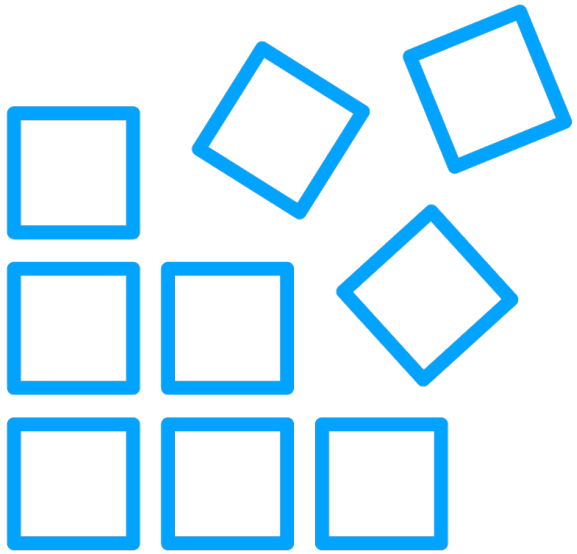
NIST: NVD **Base Score:** 7.5 HIGH **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Up Next:

Understanding the Importance of Personal Identifiable Information

Understanding the Importance of Personal Identifiable Information

What Is Data?



Data

- ‘Facts, figures (measurements or statistics) used as a basis for reasoning, discussion or calculation’
- May be created in a digital form that can be stored, transmitted and processed

What Is Information?



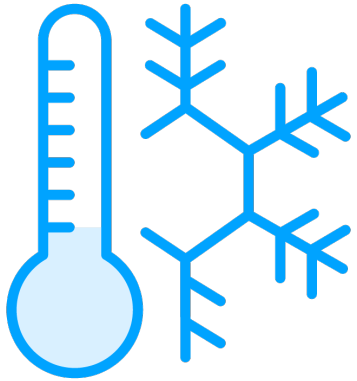
Information

- ‘Facts (data) provided or learned about something or someone’
- May be represented by a particular arrangement or sequence of data

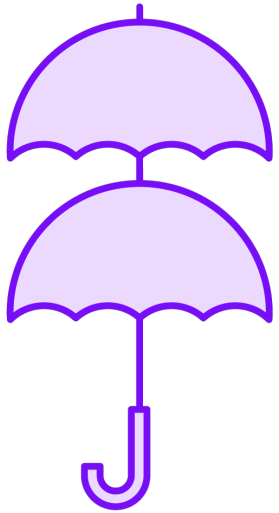
Data vs. Information



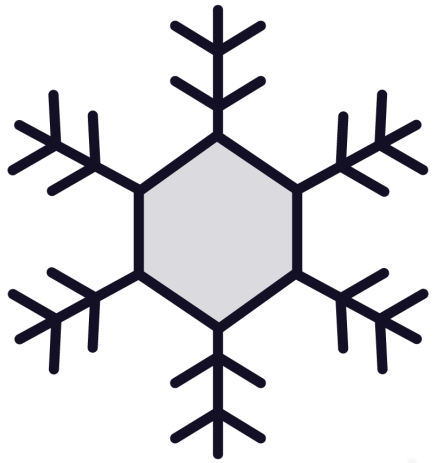
Scotland



-10°C



10cm rainfall



Weather report

Data vs. Information



Phil



123 Acacia Ave



phil@email.com



Personal Identifiable Information (PII)



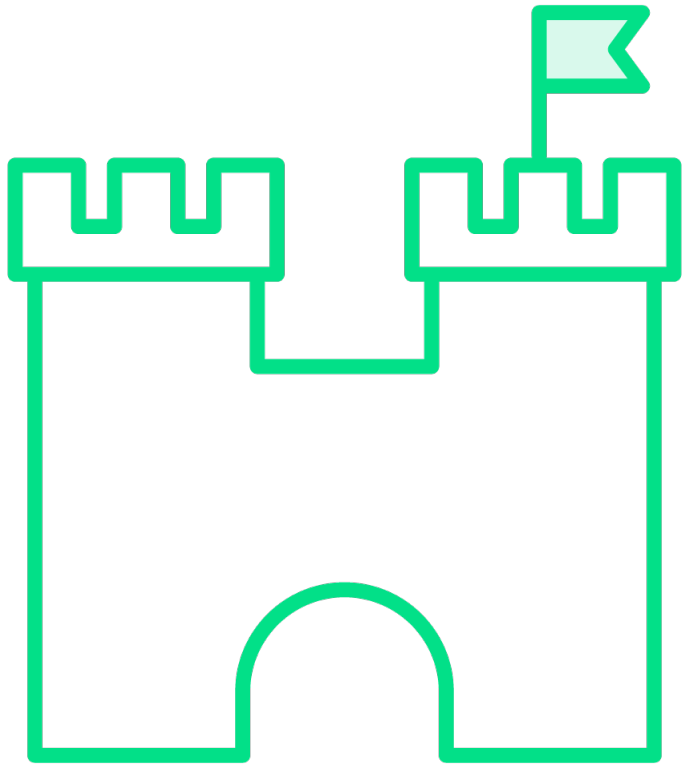
Data privacy

- Social networking sites
- Online sites (ecommerce, banking etc)
- Instant messaging
- Website cookies
- Internal company data



Data has to be protected

- Laws (e.g. Data Protection Act - DPA)
- Regulations (e.g. General Data Protection Regulation - GDPR)
- Standards (e.g. Payment Card Industry Data Security Standard – PCI DSS)



How do we protect data ‘leakage’

- Procedural controls
  - User awareness and training
  - Security policies
- Technical controls
  - Firewalls
  - File checking systems
  - Monitoring
- Physical controls
  - Dumpster diving

Up Next:

Understanding the AAA of Security

Understanding the AAA of Security



The AAA of security

- Authentication
- Authorization
- Accounting

What Is an Identity?



A set of claims about a ‘subject’



A subject may be a person (user), device, application or organization



An identity is an attribute about a subject

What Are Attributes?



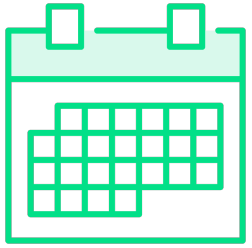
Name/username



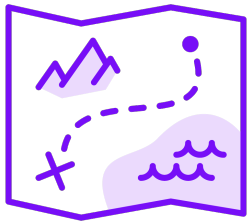
Job title



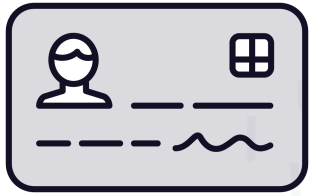
Physical feature



Date of birth



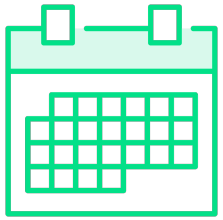
Location



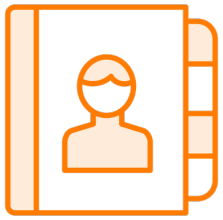
Possession



Name



DOB



Address

Identification attributes are used as part of the authentication and authorization process

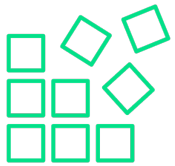
Identity needs to be kept secure especially when multiple attributes are used or stored

- Personal Identifiable Information (PII)

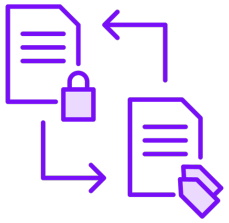
What Is Authentication?



Where a subject proves its identity to a system



May use one or more attributes



Each type of attribute is known as a factor

Multi-factor Authentication (MFA)



Something that you know (password / PIN)



Something that you have (smartcard / token / mobile)



Something that you are (biometric)



Something that you do (behavior)



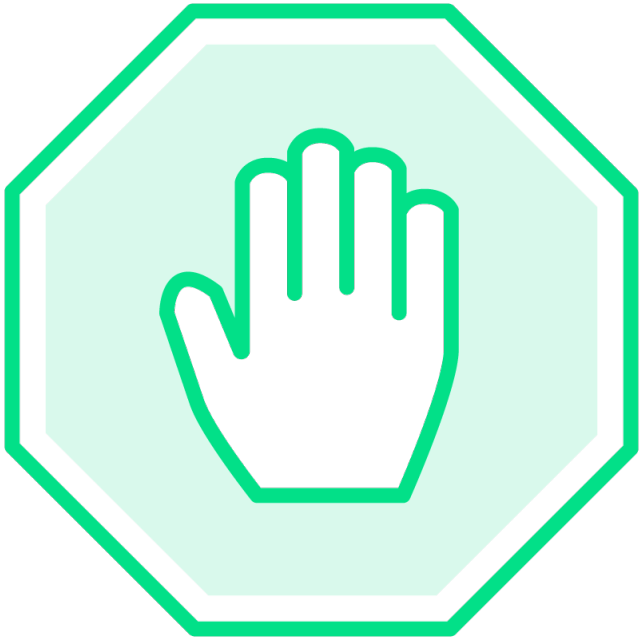
Somewhere you are (location)

What Is Authorization?

Allows access to resources for authenticated accounts

Gives permissions to the subject in order to perform actions on the resource

Employs different types of access control systems



Authorization

- Users will be assigned permissions to gain required access to resources
  - access control lists
- Administrators will have higher privileges than standard users
- Least privilege model is applied



Single Sign-on (SSO)

- Allows the user to use a single authentication and authorization process to gain access to resources
- Often uses a centralized system such as:
  - Active Directory (Kerberos)
  - Cloud-based authentication

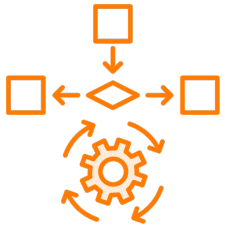
What Is Accounting?



Allows administrators to monitor access (logs)



Allows for auditing for compliance



Security violations and investigation (web, location tracking)

What Is Non-repudiation?



Ensures that a user or entity cannot deny their actions



In legal documents uses a physical signature



Digital transactions use hashing and digital signatures (cryptography)

Up Next:

Explain Methods to Secure Devices and Security Best Practices