Cybersecurity (CSCI 2413): Mid-Term Review Companion Guide

Elite Academic Professor

December 10, 2025

Contents

1 OSINT (Open-Source Intelligence)

Key Definition: OSINT

Open-Source Intelligence (OSINT) refers to the systematic process of collecting, analyzing, and acting upon publicly available information to gather actionable insight and intelligence regarding a specific target. This practice is foundational in threat intelligence and the initial reconnaissance phase of security auditing.

The term emphasizes the use of data that can be legally and ethically accessed by anyone, circumventing the need for covert measures. Crucially, the sources utilized for OSINT are incredibly diverse, covering almost any material released to the public domain.

1.1 The OSINT Ecosystem

The types of information sources that contribute to OSINT can be visualized as a comprehensive ecosystem, ranging from traditional media to private professional networks.

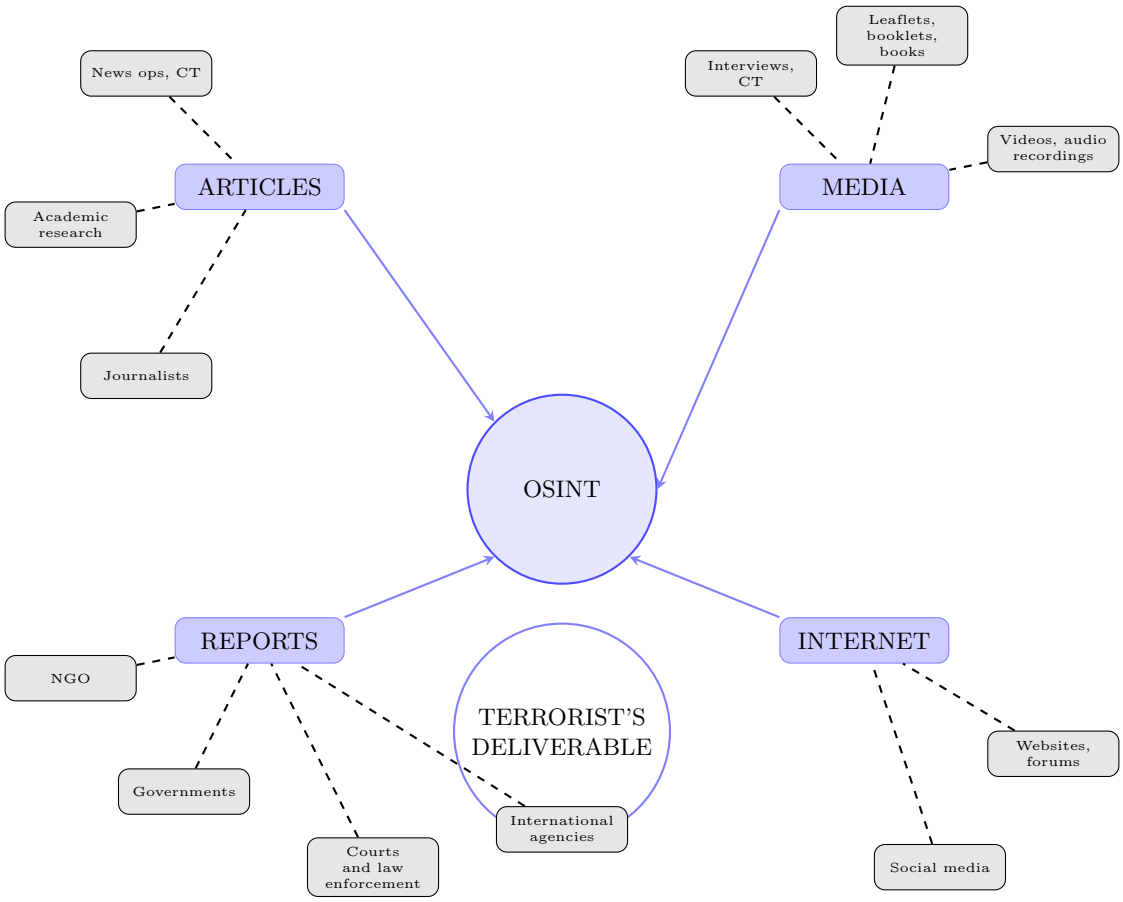

Figure 1: The Diverse Sources Contributing to Open-Source Intelligence

2 The OSINT Workflow

The collection and analysis of open-source intelligence typically follows a structured, cyclical process composed of several key phases:

2.1 Planning and Direction

This initial phase is critical for success. It requires establishing clear objectives, often driven by intelligence requirements. Analysts must precisely define what information is needed and, critically, why it is needed, ensuring that subsequent efforts are targeted and efficient.

2.2 Collection

This stage involves the actual gathering of raw data from public sources. This includes social media monitoring, scanning public records (such as property or court documents), reviewing news archives, and utilizing deep web search tools. The collection process employs both manual techniques (human searching) and automated methods (scrapers, APIs) to maximize data acquisition.

2.3 Processing and Organization

Raw collected data is voluminous and often messy. Processing involves filtering this data to retain only relevant information pertinent to the established objectives. Duplicate entries must be removed, and the data is often structured or indexed. This stage remains highly manual, as human expertise is needed to contextualize and validate the sources.

2.4 Analysis and Correlation

During analysis, the processed data is examined to identify patterns, emerging relationships, and defining trends. A crucial component is correlation, where findings are cross-referenced and corroborated using multiple independent sources to ensure accuracy and reduce the risk of relying on disinformation or single points of failure. This validation process transforms raw data into actionable intelligence.

2.5 Dissemination

The final phase involves reporting the verified findings to the relevant stakeholders, who might be internal security teams, external clients, or management. The report must be delivered in a structured, coherent way, typically taking the form of a formal report, a detailed briefing, or an alert notification.

3 OSINT Targets and Applications

OSINT techniques are applied across various domains for reconnaissance, threat intelligence, and risk assessment. Common targets include:

3.1 Individuals

Investigating individuals often involves social media intelligence (SOCMINT), identifying personal networks, behavioral patterns, and associated risks. For instance, a background check or assessment of an employee's external activities falls under this category.

3.2 Organizations and Businesses

For corporate entities, OSINT can reveal organizational structure, partnerships, technological footprints, public financial filings, and supply chain vulnerabilities. This information is vital for competitive intelligence and penetration testing reconnaissance.

3.3 Critical Infrastructure

This involves gathering public information related to essential services like power grids, water supply, and transportation networks. Such reconnaissance helps identify weaknesses that could be exploited by adversaries, allowing defenders to preemptively harden systems.

3.4 Cybersecurity and Threat Intelligence

OSINT is a core component of threat intelligence, used to monitor forums, dark web activity (where accessible publicly), and security blogs to track new attack vectors, malware campaigns, and threat actors.

3.5 Governments and Nations

This involves collecting publicly available governmental documents, policy statements, legislative debates, and open-source military data to inform strategic decision-making and foreign policy analysis.

3.6 Public Health

In public health, OSINT is used for tracking disease outbreaks, monitoring public reaction to health policies, and identifying regional resource deficits by analyzing publicly shared reports and data.

4 Sock Puppet Accounts and SOCMINT

Key Definition: Sock Puppet

A **Sock Puppet** is a covert online account or identity utilized by an investigator that is deliberately not related to their true personal or professional identity.

The primary purpose of using a sock puppet account in intelligence gathering, especially within the scope of Social Media Intelligence (**SOCMINT**), is anonymity. By using a fabricated identity, the analyst protects their true identity from being revealed to the target or other associated parties. This protection is essential to avoid burning the identity of the analyst or compromising the investigation.

When conducting such operations, it is crucial to maximize operational security (OPSEC). Best practices dictate isolating the investigative environment entirely:

- **Virtual Machine (VM):** Operations should be conducted from a Virtual Machine (VM). This isolates the activities from the analyst's primary operating system, creating a clean, disposable environment that minimizes the risk of infection or leakage.
- **VPN (Virtual Private Network):** Using a VPN ensures that the physical location and the network IP address of the analyst are masked, preventing geographical tracking and IP-based attribution by the target or platform providers.

These measures ensure that the only trace left behind belongs to the constructed sock puppet identity.

5 Cryptography Basics

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior. It primarily deals with two processes: encryption and decryption.

5.1 Encryption

Encryption is the method by which plain text (readable data) is transformed into cipher text (unreadable, scrambled data).

- **Algorithm:** An algorithm is utilized to scramble the plain text based on a specific set of rules and a key.
- **Shared Protocol:** For successful communication, the sender and receiver must agree on the specific algorithm being used.
- **Security:** Without knowing the correct protocol and key, the resulting message is computationally difficult to reverse-engineer back into the original plain text.

5.2 Decryption

Decryption is the complementary process, involving the reversal of the scrambling protocol (the encryption algorithm) using the correct key. This process transforms the cipher text back into the original comprehensible plain text message.

5.3 Sample Encryption and Decryption Process

6 Cryptography Basics (Continued)

Cryptographic ciphers are traditionally categorized based on how they manipulate the plain text:

6.1 Transposition Ciphers

Transposition ciphers rearrange the order of the letters in the plain text without changing the letters themselves. Intuitively, this is like shuffling a deck of cards; the cards remain the same, but their sequence is altered.

6.2 Substitution Ciphers

Substitution ciphers systematically replace each letter or group of letters in the plain text with a different letter, number, or symbol.

6.2.1 Types of Substitution

Substitution methods are further classified based on key management:

1. **Single/Symmetric Key Encryption:** This uses the same secret key for both encryption and decryption.
    - **Stream Ciphers:** Encrypt one bit or byte of plain text at a time.
    - **Block Ciphers:** Encrypt a fixed-size block of bits simultaneously (e.g., 64-bit or 128-bit blocks).
2. **Public/Asymmetric Key Encryption:** This uses a pair of mathematically related keys: a public key for encryption and a private key for decryption.

7 Transposition Ciphers: The Rail Fence

A classic example of a transposition cipher is the Rail Fence cipher, which writes the plain text downwards on successive "rails" and then reads the result off row by row.

7.1 Example: Rail Fence Encryption

Consider the message: **"Defend the east wall"** with a **key of 3** (meaning 3 rails). Spaces are removed and the plaintext is $DEFENDTHEEASTWALLX$ (19 characters).

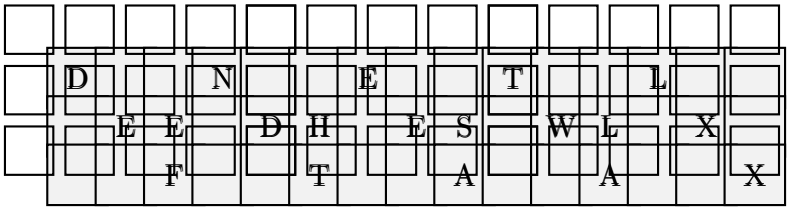

Figure 2: Rail Fence Grid (Key=3)

The cipher text is generated by reading the content row by row, starting from the top rail:

DNETLEEDHESWLXFTAAX

8 Transposition Cipher: Decryption Example

Decryption of a Rail Fence cipher requires knowing the length of the message and the key (number of rails). The process involves reconstructing the fence pattern using placeholders and then mapping the cipher text back into the pattern.

Ciphertext: **TEKOOHRACIRMNREATANFTETYTGHH**
Length: 28
Key: **4**

8.1 Step 1: Determine Rail Lengths and Placement

We map the 28 letters onto the 4-rail zig-zag pattern to determine where each letter of the ciphertext belongs.

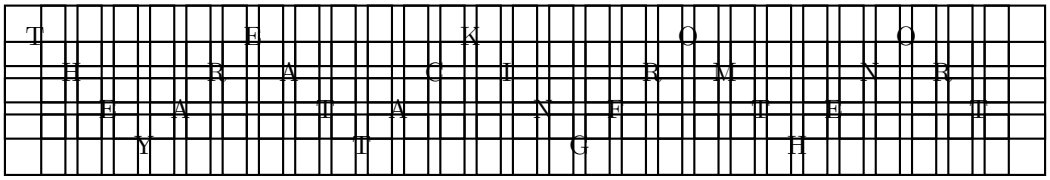

Figure 3: Rail Fence Decryption Grid (Key=4)