Offensive Security Testing

VISION SPACE

Safeguarding the Final Frontier

Software in a Space Mission

Software systems power all segments

Space Segment

- On-board software

Ground Segment

- Mission Control Systems
- Ground Station equipment
- Flight Dynamics
- Mission Planning
- All other auxiliary software systems

User Segment

- Instrument execution planning systems
- All types of software for data processing



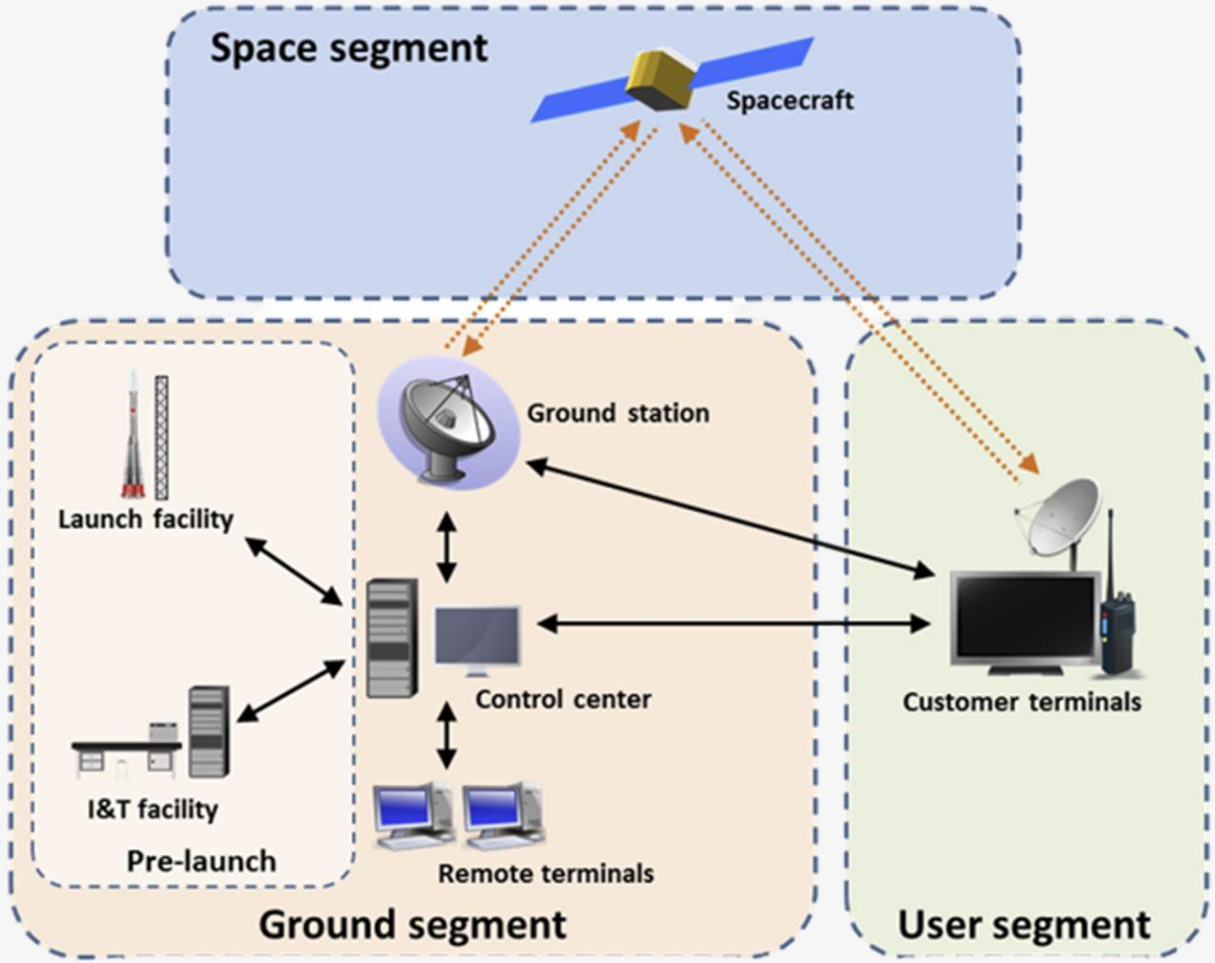
Ground Segment

Ground Segment

- Consists of many interconnected elements
- Different elements have different functions
- Depend on each other
- Most don't require user interaction

Mission Control System

- Main interface to other ground segment components
- Serves as the primary interface between the controllers and the spacecraft
- This makes it arguably the most vulnerable element of the Ground Segment



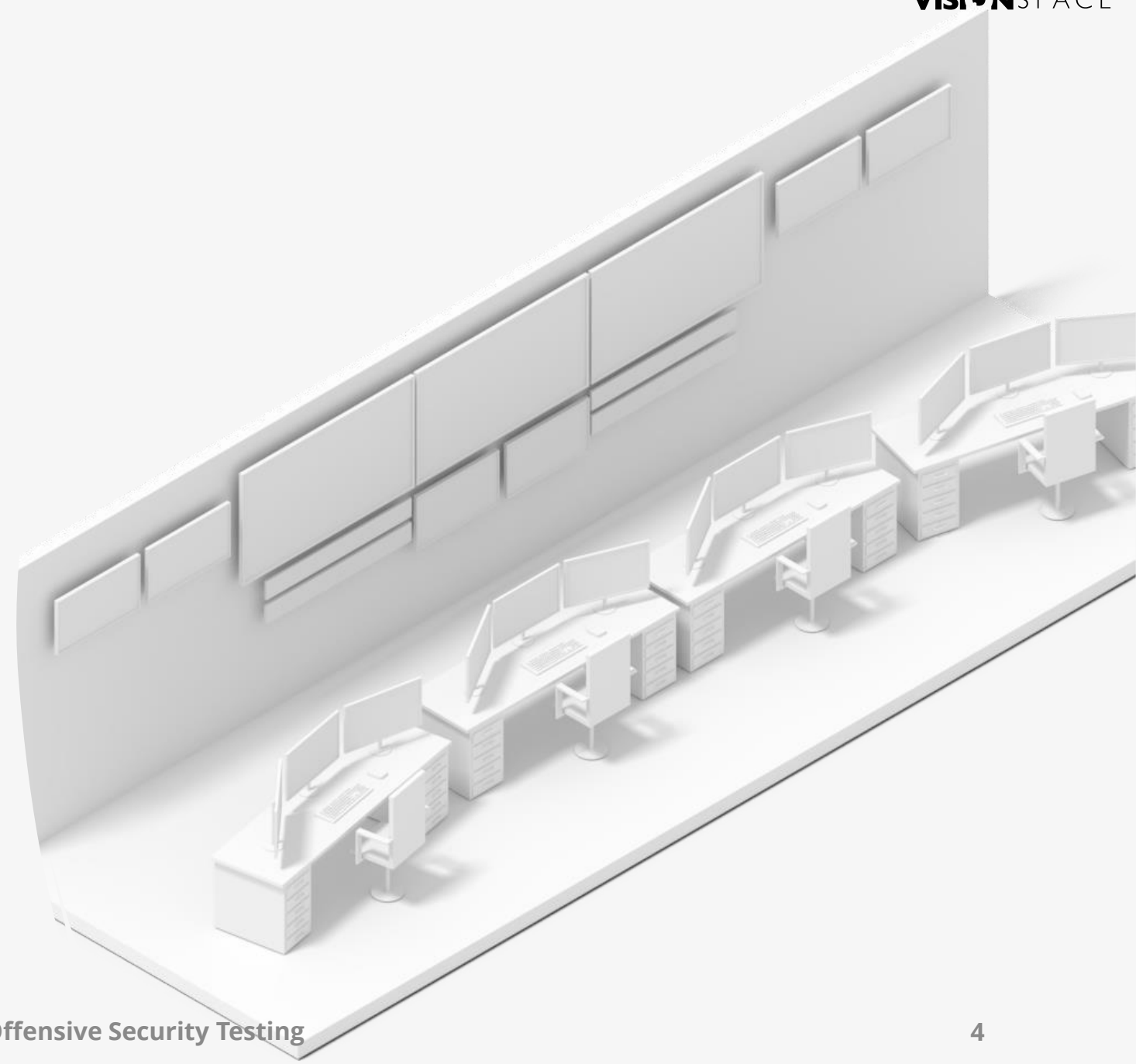
Mission Control

No more isolated environment?

- No more restricted physical access
- Spacecraft Operations conducted remotely
- Mission Control Systems – a new attack surface

What is being done about it?

- Expanding strategies to include security aspects
- Imposing security policies
- Introducing security requirements



Public Disclosure Reports



Photo by NASA on Unsplash

Prototype Pollution in NASAs Open MCT CVE-2023-45282



Photo by Kurt Cotoaga on Unsplash

XSS in NASAs Open MCT v3.1.0

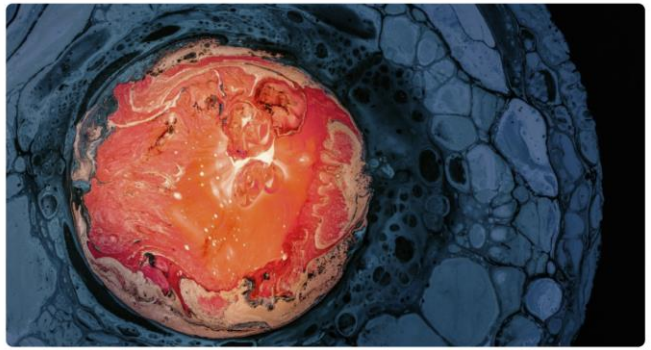


Foto by Pawel Czerwinski on Unsplash

Remote Code Execution via Man-in-the-Middle (and more) in NASA's AIT-Core v2.5.2

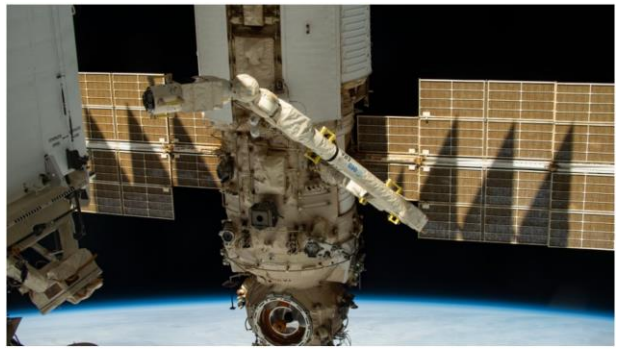


Photo of the European Robotic Arm (ERA) by NASA on Flickr

Yamcs v5.8.6 Vulnerability Assessment



Foto by NASA on Unsplash

More XSS and Clickjacking in Yamcs v5.8.6

OpenMCT CVEs

CVE	NVD Score	Type
CVE-2023-45282	7.5	Prototype Pollution
CVE-2023-45885	5.4	XSS Vulnerability
CVE-2023-45884	6.5	CSRF Vulnerability

YaMCS CVEs

CVE	NVD Score	Type
CVE-2023-45277	7.5	Directory Traversal
CVE-2023-45278	9.1	Arbitrary File Deletion
CVE-2023-45281	6.1	Session Hijacking
CVE-2023-45279	5.4	XSS Vulnerability
CVE-2023-45280	5.4	XSS Vulnerability
CVE-2023-46471	5.4	XSS Vulnerability
CVE-2023-46470	5.4	XSS Vulnerability
CVE-2023-47311	6.1	Clickjacking

AIT-Core CVEs

CVE	Type
CVE-2024-35056	Prototype Pollution
CVE-2024-35057	XSS Vulnerability
CVE-2024-35058	CSRF Vulnerability
CVE-2024-35059	Directory Traversal
CVE-2024-35060	Arbitrary File Deletion
CVE-2024-35061	Session Hijacking

YaMCS - exploitation

CVE	NVD Score	Type
CVE-2023-45277	7.5	Directory Traversal
CVE-2023-45278	9.1	Arbitrary File Deletion
CVE-2023-45281	6.1	Session Hijacking
CVE-2023-45279	5.4	XSS Vulnerability
CVE-2023-45280	5.4	XSS Vulnerability
CVE-2023-46471	5.4	XSS Vulnerability
CVE-2023-46470	5.4	XSS Vulnerability
CVE-2023-47311	6.1	Clickjacking

YaMCS
Chaining Vulnerabilities

XSS vulnerability

↓

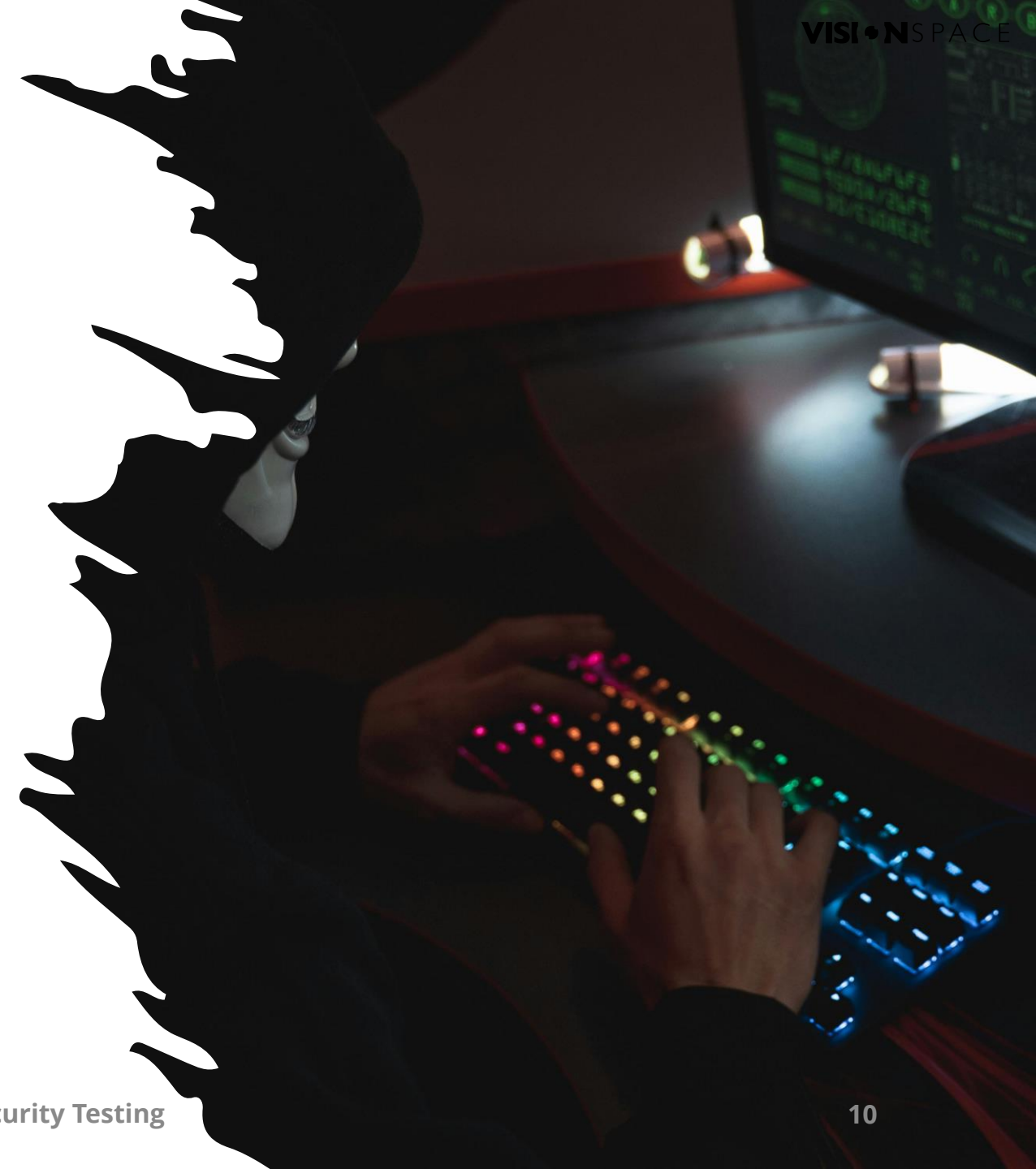
Session Hijacking

↓

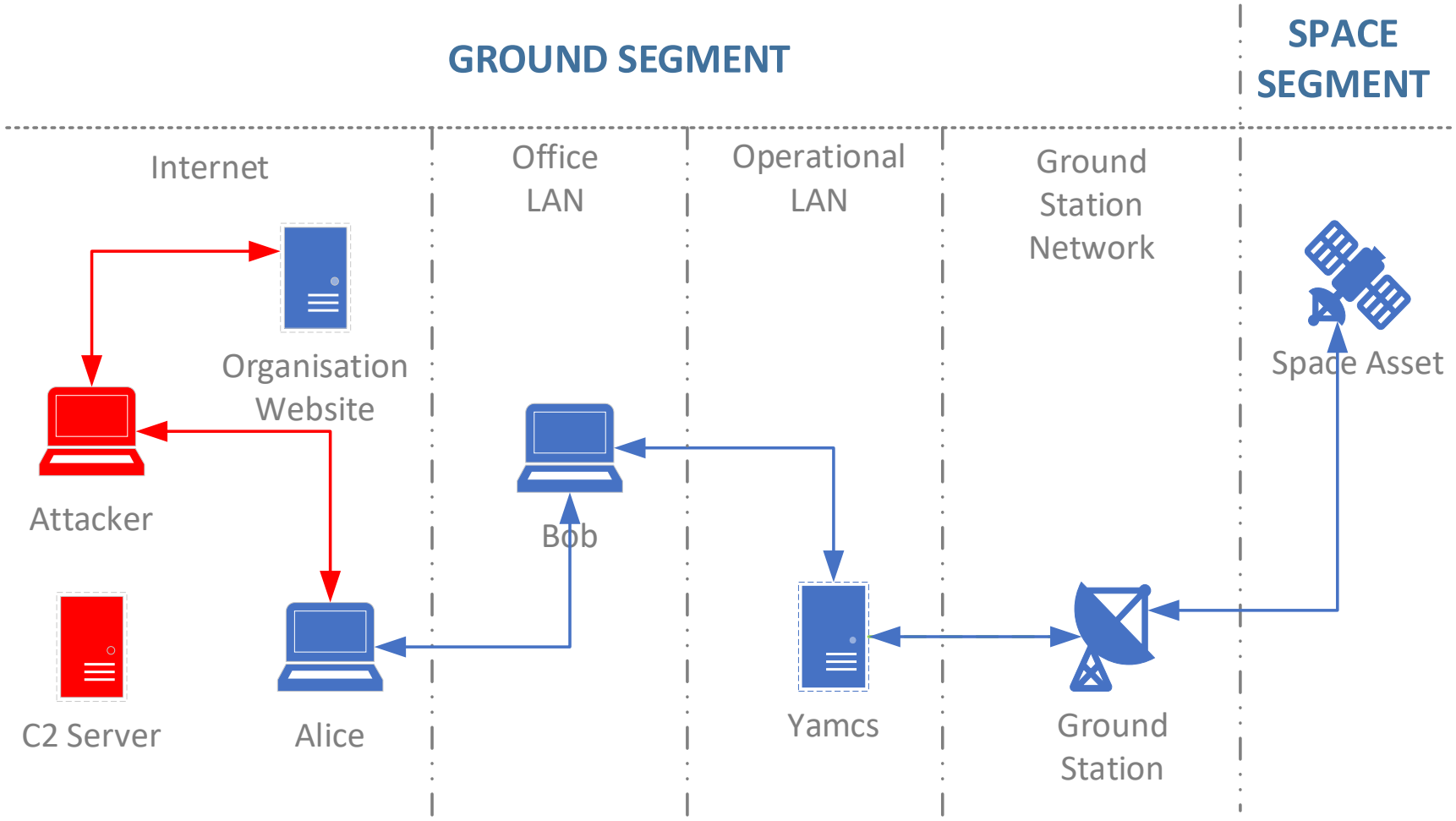
Directory Traversal

↓

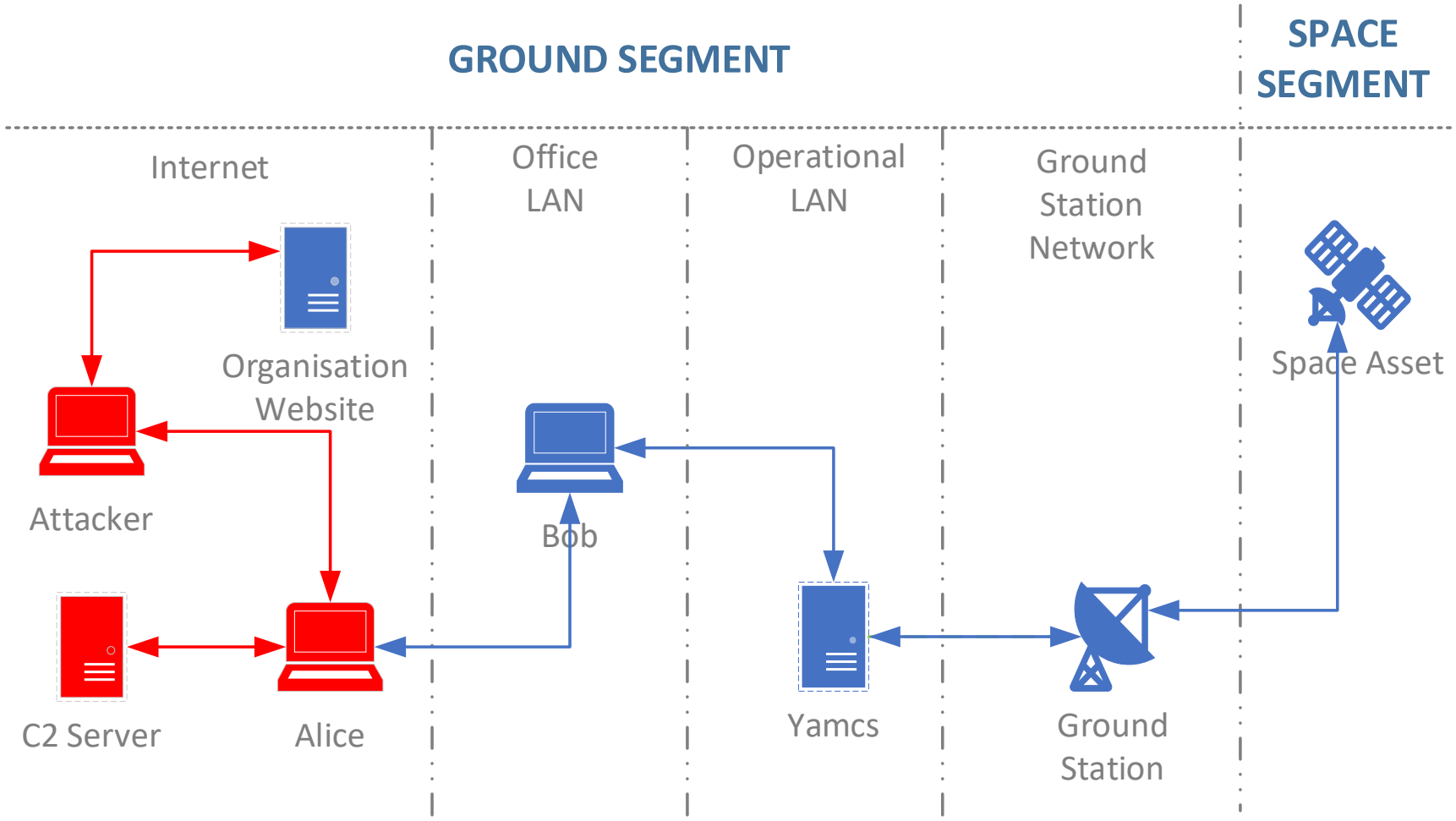
Sensitive information disclosure



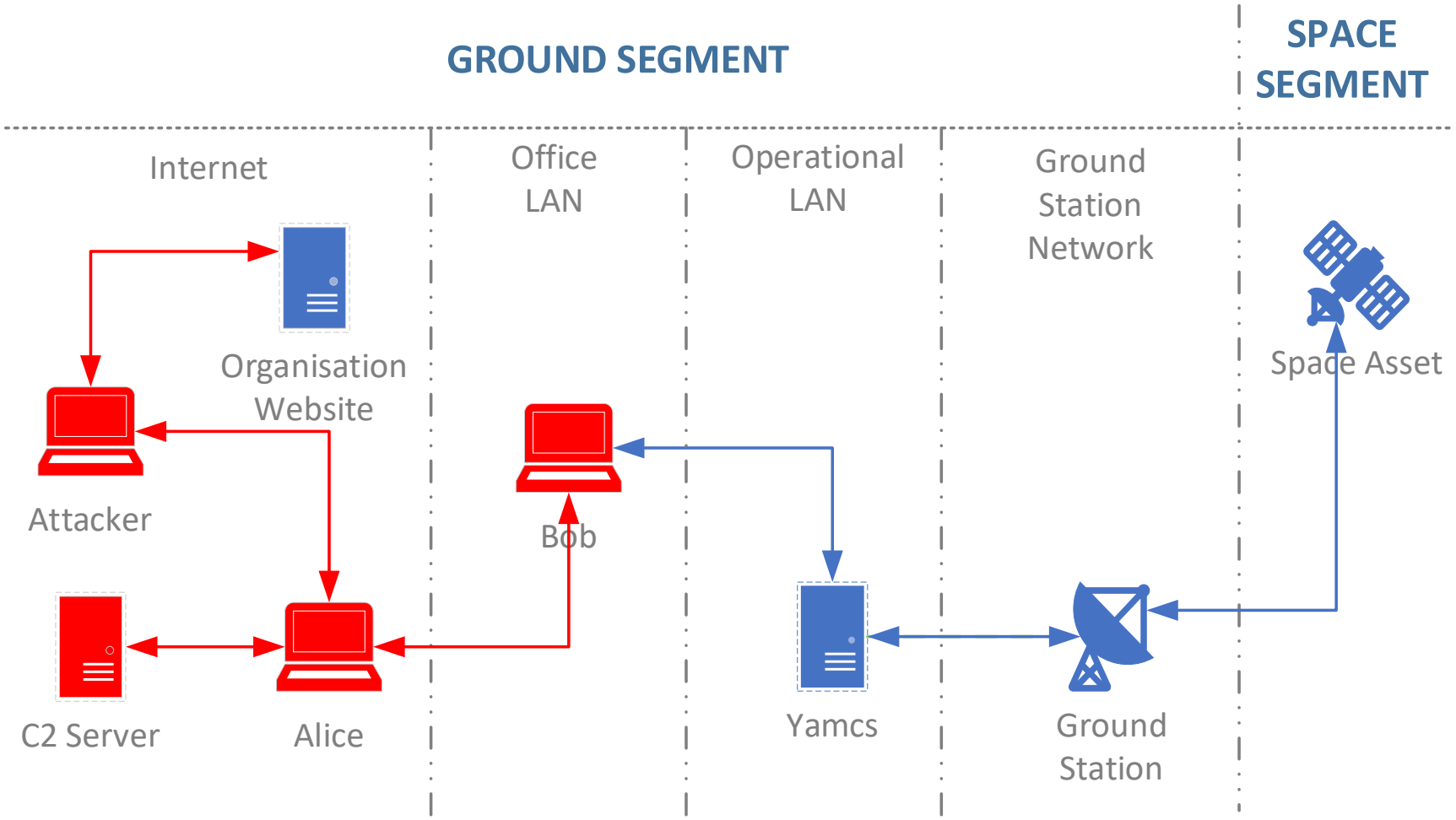
Attack Scenario – recon + phishing



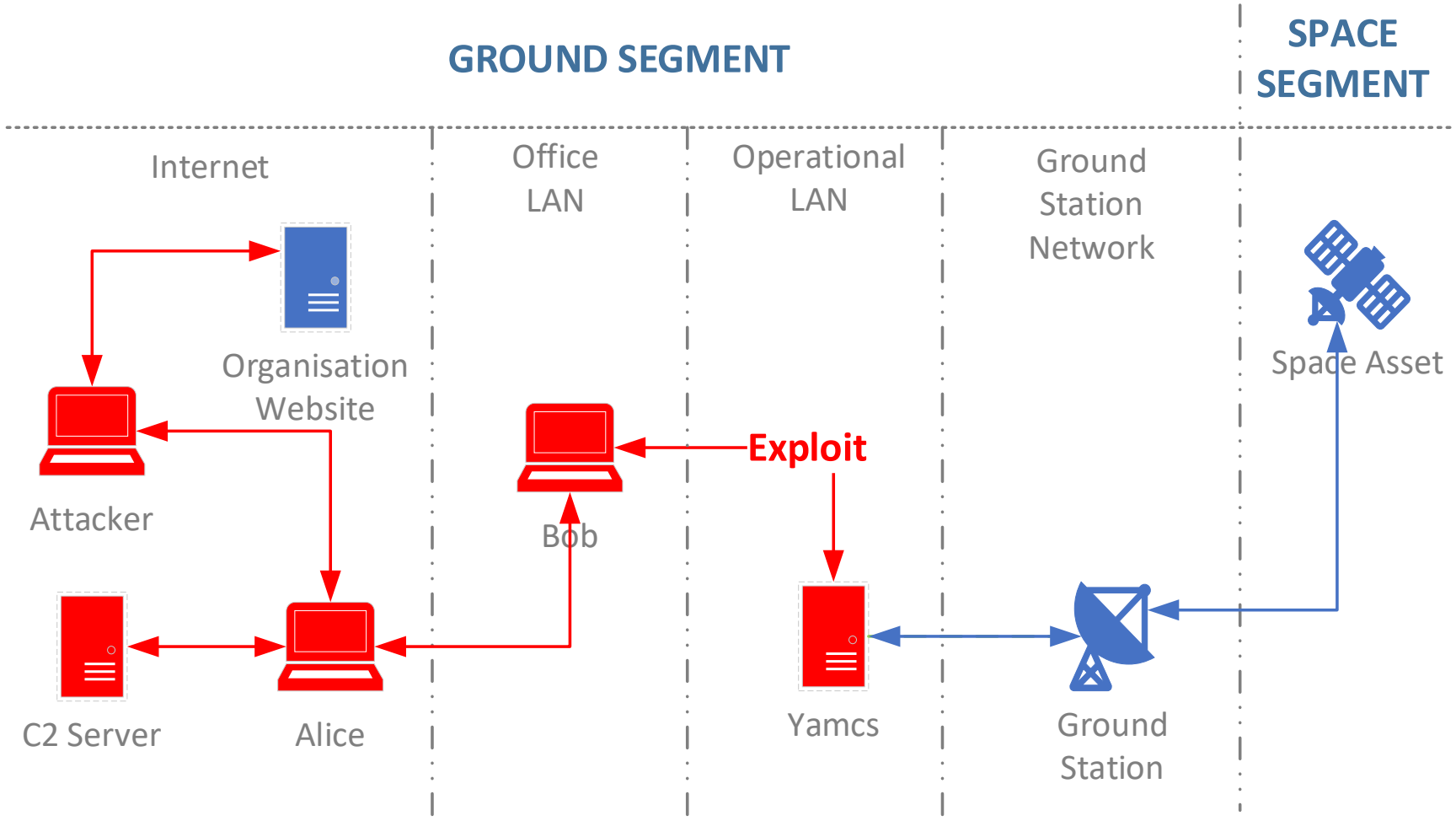
Attack Scenario – initial access



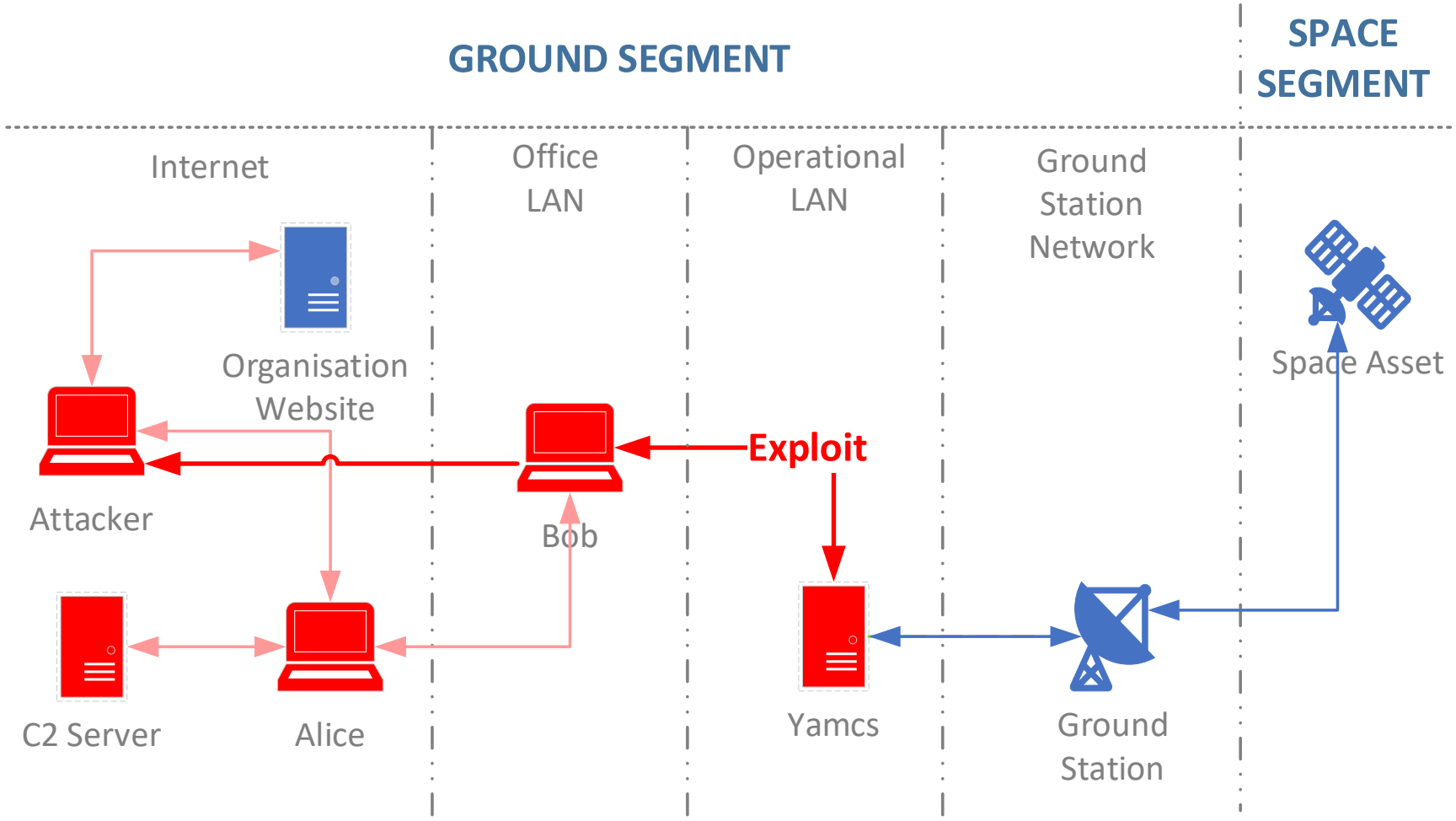
Attack Scenario – internal phishing



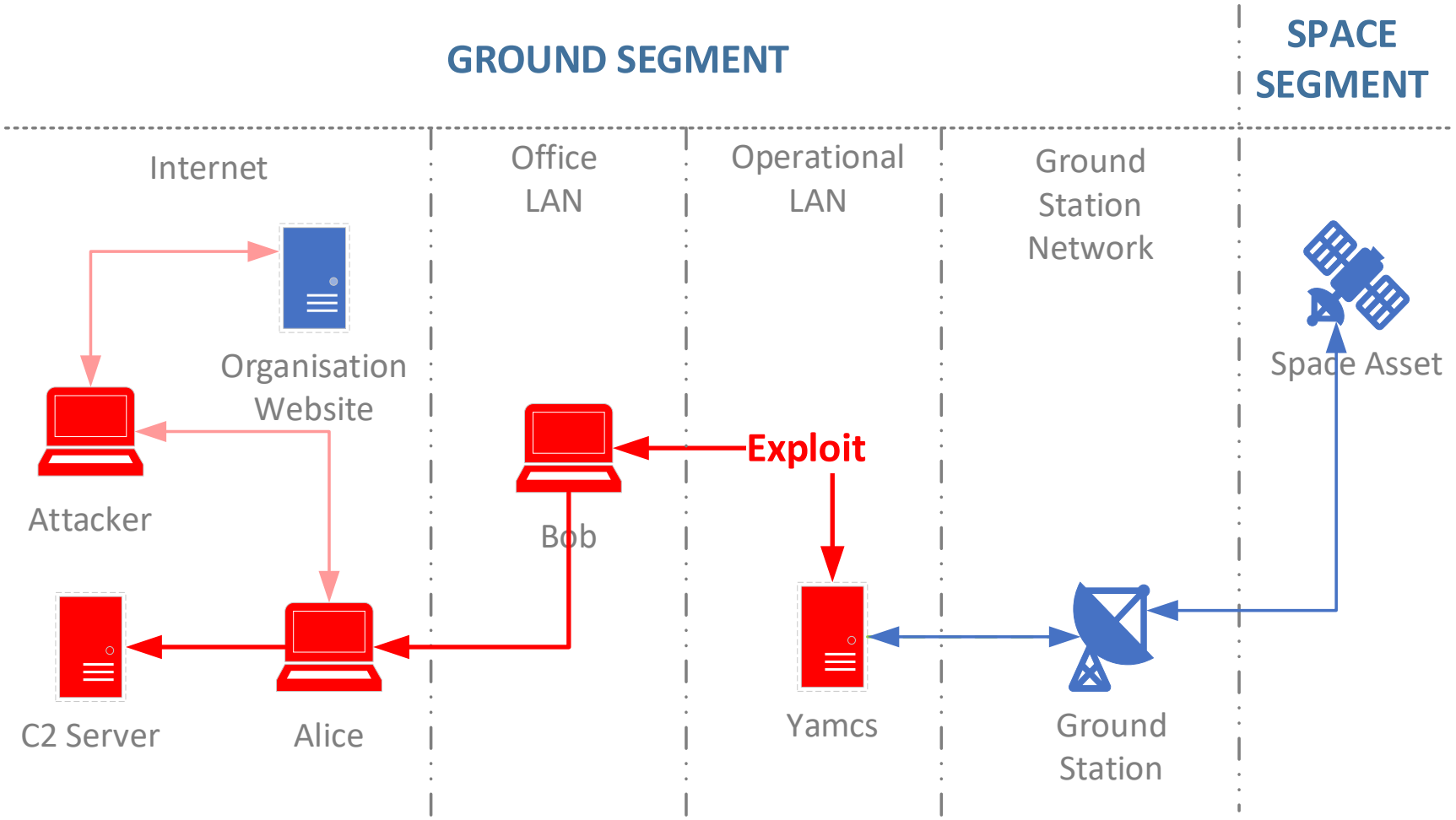
Attack Scenario – exploitation



Attack Scenario – information exfiltration (1)



Attack Scenario – information exfiltration (2)



Demo: yamcs-exploit.mkv

Static Code Analysis vs Offensive Security Testing

Static Analysis

CVE	Product	Type
CVE-2023-45884	OpenMCT	CSRF vulnerability
CVE-2023-45281	YaMCS	Session Hijacking
CVE-2023-46471	YaMCS	XSS Vulnerability
CVE-2023-46470	YaMCS	XSS Vulnerability
CVE-2023-47311	YaMCS	Clickjacking
CVE-2024-35056	AIT-Core	SQL Injection
CVE-2024-35057	AIT-Core	Local Code Execution
CVE-2024-35058	AIT-Core	Local Code Execution
CVE-2024-35059	AIT-Core	Local Code Execution
CVE-2024-35060	AIT-Core	Local Code Execution
CVE-2024-35061	AIT-Core	Missing Encryption

Dynamic Analysis + Exploitation

CVE	Product	Type
CVE-2023-45282	OpenMCT	Prototype Pollution
CVE-2023-45885	OpenMCT	XSS Vulnerability
CVE-2023-45277	YaMCS	Directory Traversal
CVE-2023-45278	YaMCS	Arbitrary File Deletion
CVE-2023-45279	YaMCS	XSS Vulnerability
CVE-2023-45280	YaMCS	XSS Vulnerability

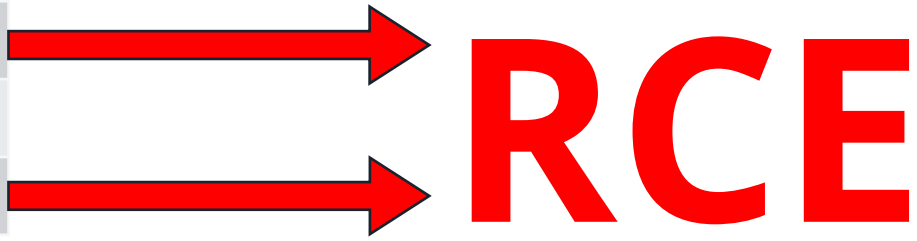
Static Code Analysis vs Offensive Security Testing

Static Analysis

CVE	Product	Type
CVE-2023-45884	OpenMCT	CSRF Vulnerability
CVE-2023-45281	YaMCS	Session Hijacking
CVE-2023-46471	YaMCS	XSS Vulnerability
CVE-2023-46470	YaMCS	XSS Vulnerability
CVE-2023-47311	YaMCS	Clickjacking
CVE-2024-35056	AIT-Core	SQL Injection
CVE-2024-35057	AIT-Core	Local Code Execution
CVE-2024-35058	AIT-Core	Local Code Execution
CVE-2024-35059	AIT-Core	Local Code Execution
CVE-2024-35060	AIT-Core	Local Code Execution
CVE-2024-35061	AIT-Core	Missing Encryption

Dynamic Analysis + Exploitation

CVE	Product	Type
CVE-2023-45282	OpenMCT	Prototype Pollution
CVE-2023-45885	OpenMCT	XSS Vulnerability
CVE-2023-45277	YaMCS	Directory Traversal
CVE-2023-45278	YaMCS	Arbitrary File Deletion
CVE-2023-45279	YaMCS	XSS Vulnerability
CVE-2023-45280	YaMCS	XSS Vulnerability



Demo: AIT-Core-MitM-RCE-comments.mp4

Static Code Analysis – SCOS-2000 Case

CWE ID	Count	Description
CWE-119	668	Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-120	2460	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CWE-126	548	Buffer Over-read
CWE-134	126	Use of Externally-Controlled Format String
CWE-190	590	Integer Overflow or Wraparound
CWE-327	36	Use of a Broken or Risky Cryptographic Algorithm
CWE-362	301	Concurrent Execution using Shared Resource with Improper Synchronization
CWE-367	6	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-377	4	Insecure Temporary File
CWE-676	11	Use of Potentially Dangerous Function
CWE-732	1	Incorrect Permission Assignment for Critical Resource
CWE-807	174	Reliance on Untrusted Inputs in a Security Decision

Resources and Further Research

YaMCS	OpenMCT	AIT-Core
Website	Website	Website
GitHub	GitHub	GitHub

Security Research:

- NASA OpenMCT part 1
- NASA OpenMCT part 2
- NASA AIT-Core
- YaMCS part 1
- YaMCS part 2



THANK YOU!

Andy Olchawa

andrzej.olchawa@visionspace.com

linkedin.com/in/andrzejolchawa

@0x4ndy

Milenko Starcik

milenko.starcik@visionspace.com

linkedin.com/in/milenko-starcik

Ayman Boulaich

ayman.boulaich@visionspace.com

linkedin.com/in/aymanblh

pwndside.github.io

