Red Teaming Space

Hacking the Final Frontier

#: whoami (Never howami)

- Founder of ETHOS Labs and RBX Space
- Over a decade of experience in offensive security, red teaming, and penetration testing
- Former consultant for Fortune 100 financial institutions
- Specializes in space systems security, satellite operations, and embedded systems
- Creator of hands-on training platforms using real CubeSats and simulated space networks.
- Speaker at multiple security conferences nationwide

ETHOSLABS

RBX SPACE

Introduction

THE NEW SPACE RACE: COMMERCIALIZATION, INTERCONNECTIVITY, AND OPPORTUNITY

WHY CYBERSECURITY MATTERS IN SPACE

WHO THIS TALK IS FOR (PENTESTERS, RESEARCHERS, ENGINEERS, POLICYMAKERS)

The Space Revolution

Growth in satellites (LEO, MEO, GEO constellations)

Commercial and governmental players

Satellite's On Orbit (2023)

ETHOSLABS

RBX SPACE

What's at Stake?

Critical infrastructure: communications, navigation, defense, Earth observation

Economic and geopolitical implications

Visual: Icons representing key space services

The Expanding Attack Surface

Interconnectedness = more entry points

Ground, space, and supply chain vulnerabilities

Visual: Diagram of typical space system architecture

Space System Components

Space segment: satellites, payloads

Ground segment: control stations, mission ops

Communications: Unique Risks in Space

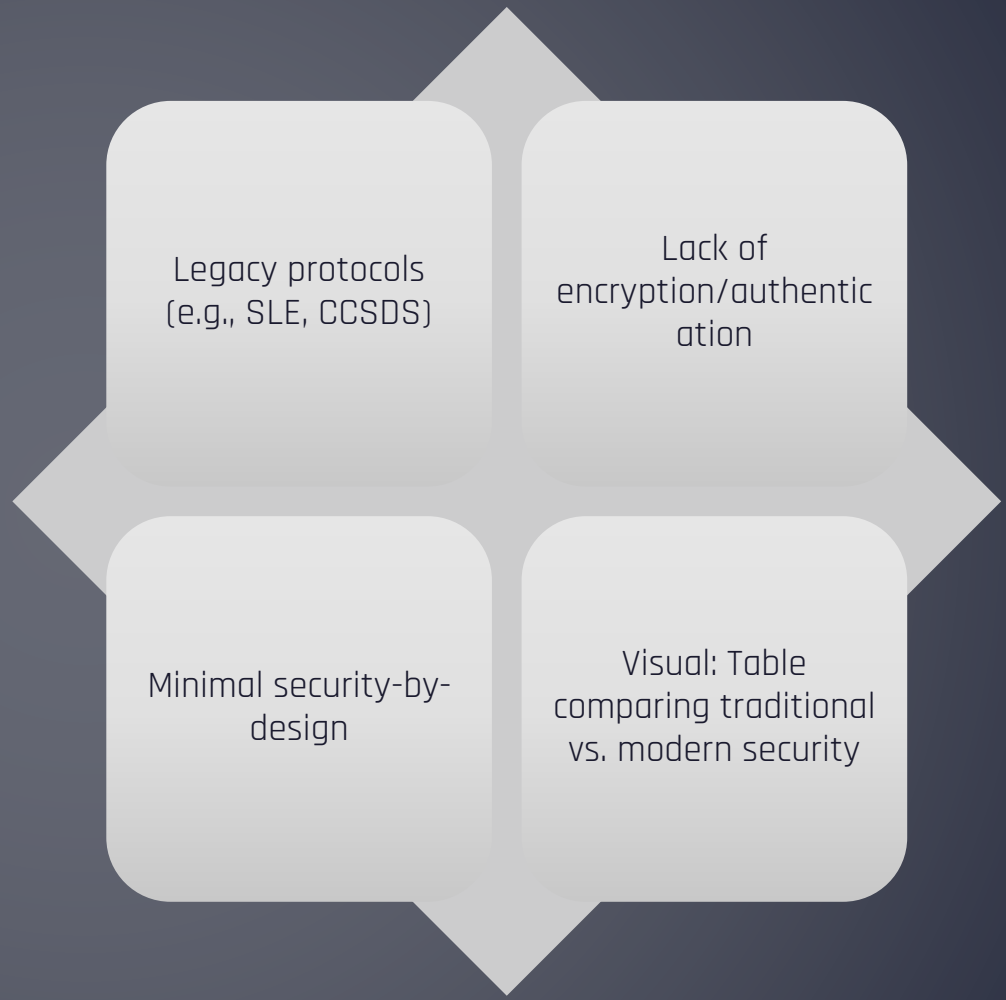
Uplinks, downlinks, relay

Visual: Labeled system diagram

Unique Risks in Space

- Physical inaccessibility
- Long asset lifetimes
- Limited patching/updating

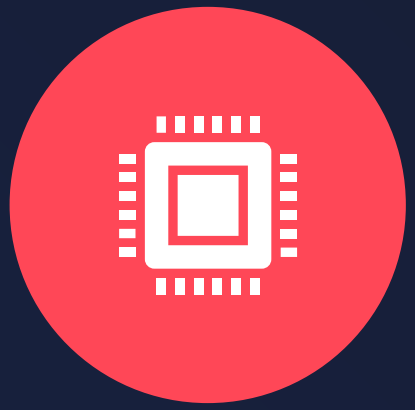
Traditional Security Models Fall Short



ETHOSLABS

RBX SPACE

Recent Space Cyber Incidents



2022: VIASAT KA-SAT HACK (UKRAINE)

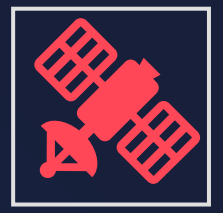
1998: ROSAT SATELLITE HACK

2023: STARLINK JAMMING/SPOOFING ATTEMPTS

ETHOSLABS

RBX SPACE

Anatomy of the Space Attack Surface



Spacecraft vulnerabilities: firmware, command channels

Radio link threats: jamming, spoofing, interception

Ground station risks: network, physical, insider

Visual: Attack surface map

ETHOSLABS

RBX SPACE

Attacker Motivations

- Nation-state espionage
- Criminal ransomware/extortion
- Hacktivism and disruption
- Visual: Icons or personas

Tactics, Techniques, and Procedures (TTPs)

Uplink-assisted attacks

Signal jamming/spoofing

Telemetry manipulation

Supply chain compromise

Insider threats

Visual: MITRE ATT&CK-style matrix

Case Study – ViaSat KA-SAT Hack

- How attackers exploited ground infrastructure
- Impact: communication blackout
- Lessons learned
- Visual: Incident flowchart

Introducing Space Red Teaming

DEFINITION: SIMULATED ADVERSARIAL TESTING FOR SPACE ASSETS

WHY IT'S NEEDED

VISUAL: RED TEAM/BLUE TEAM ILLUSTRATION

ETHOSLABS

RBX SPACE

Red Teaming Methodologies

Reconnaissance (OSINT, RF scanning)

Vulnerability assessment (protocol fuzzing, hardware analysis)

Exploitation (command injection, link hijacking)

Post-exploitation (persistence, exfiltration)

Visual: Red teaming workflow

Tools and Testbeds

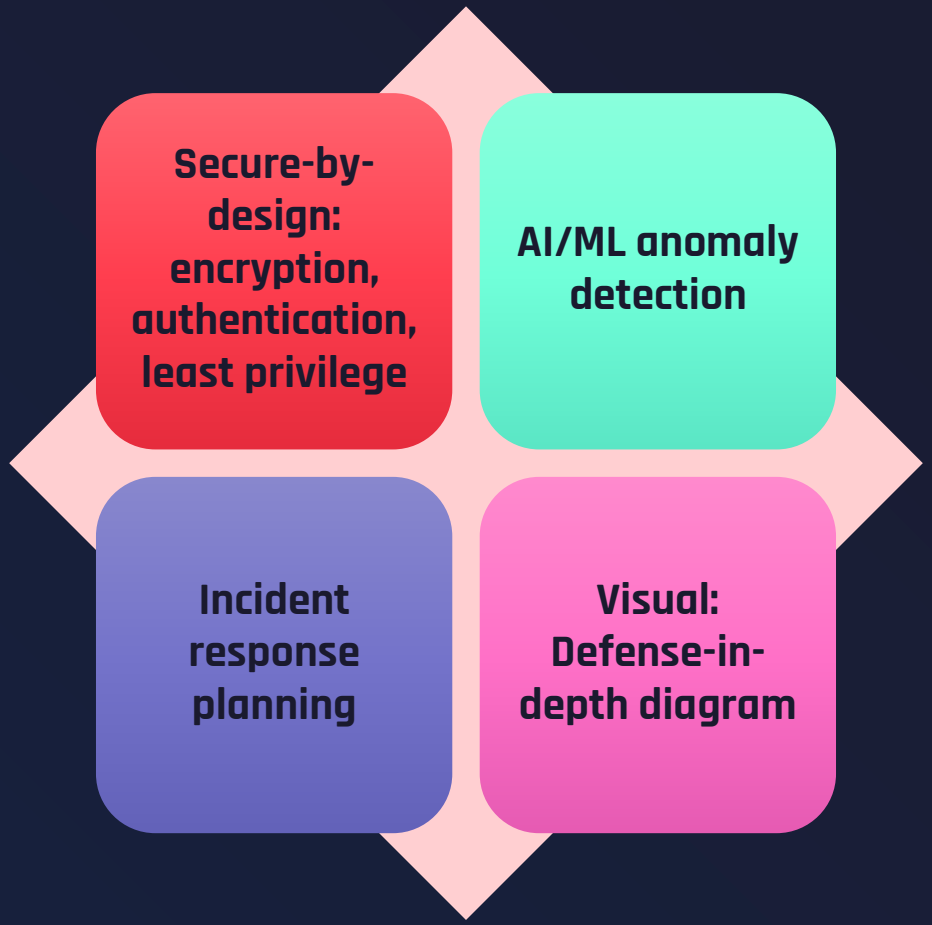
Space cyber ranges (digital twins, flat-sats)

RF testing equipment

Simulation platforms

Visual: Photos of testbeds or tools

Defensive Takeaways



Policy and Collaboration

Space ISAC, NIST, ENISA guidelines

Cross-sector information sharing

The Road Ahead

- Quantum-resistant comms
- Autonomous threat response
- Continuous red/blue teaming
- Visual: Futuristic satellite/space scene

Conclusion & Q&A