An Actionable Framework for Space Cyber Risk Management

Ekzhin Ear, Caleb Chang, and Shouhuai Xu
Laboratory for Cybersecurity Dynamics
Department of Computer Science
University of Colorado Colorado Springs

Problem Statement and Goals

Problem:

- There is a need to manage cyber risks in space infrastructures
- Existing cyber risk management frameworks either oversimplify things of are not geared toward space infrastructures

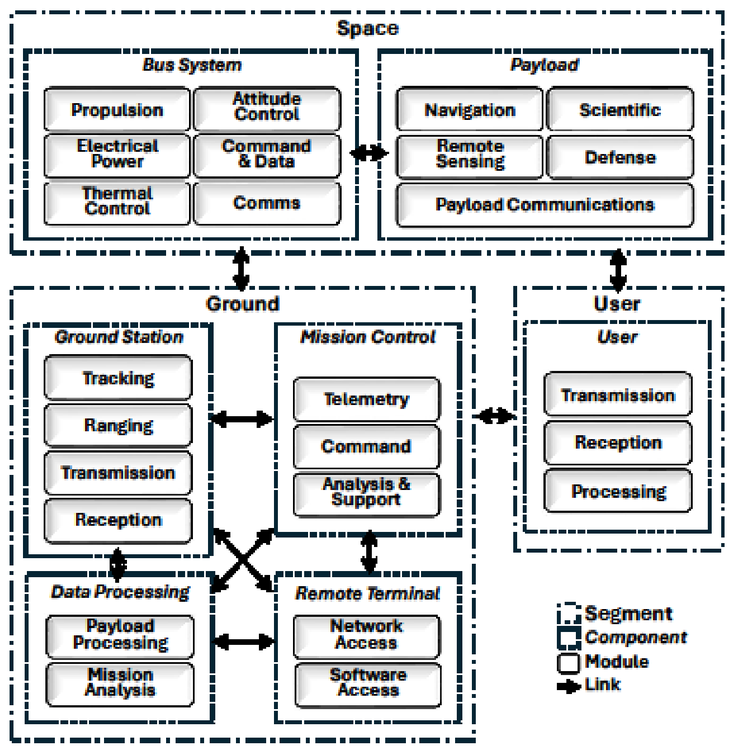
Goals:

- Propose a principled and actionable space cyber risk management framework
- Propose algorithms for quantitatively managing space cyber risks and for hardening against space cyber threats
- Apply the framework and algorithms to real-world space cyber attack scenarios

Note: The research results are patent-pending.

Approach

System Model:

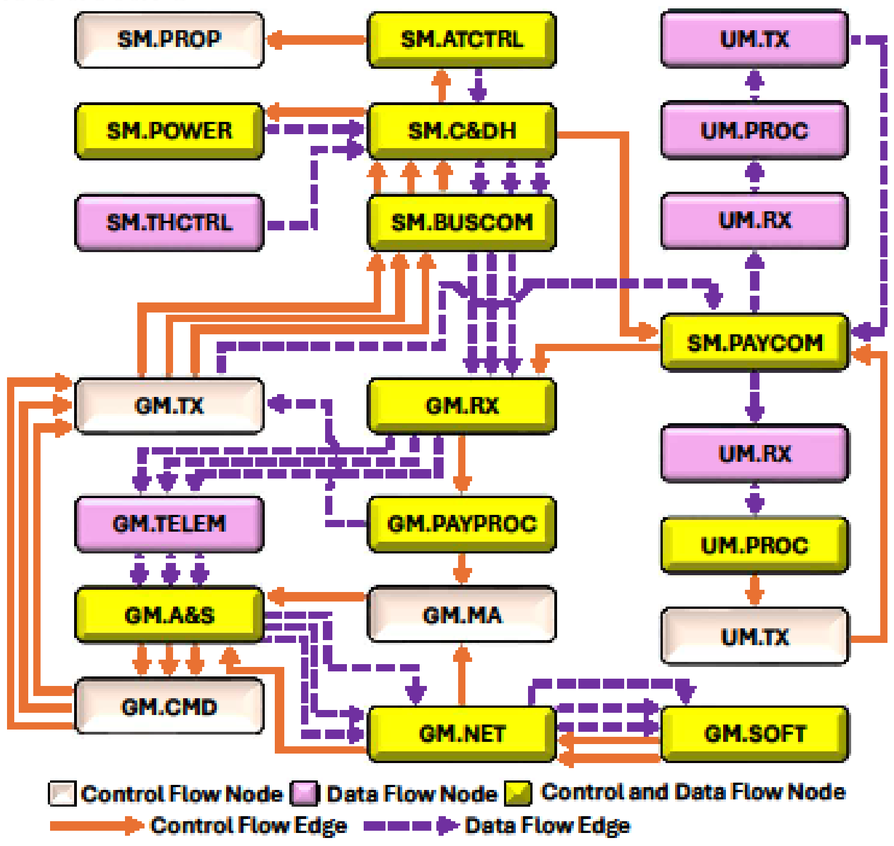


The framework can perform mission risk analysis and recommend security controls for mission hardening

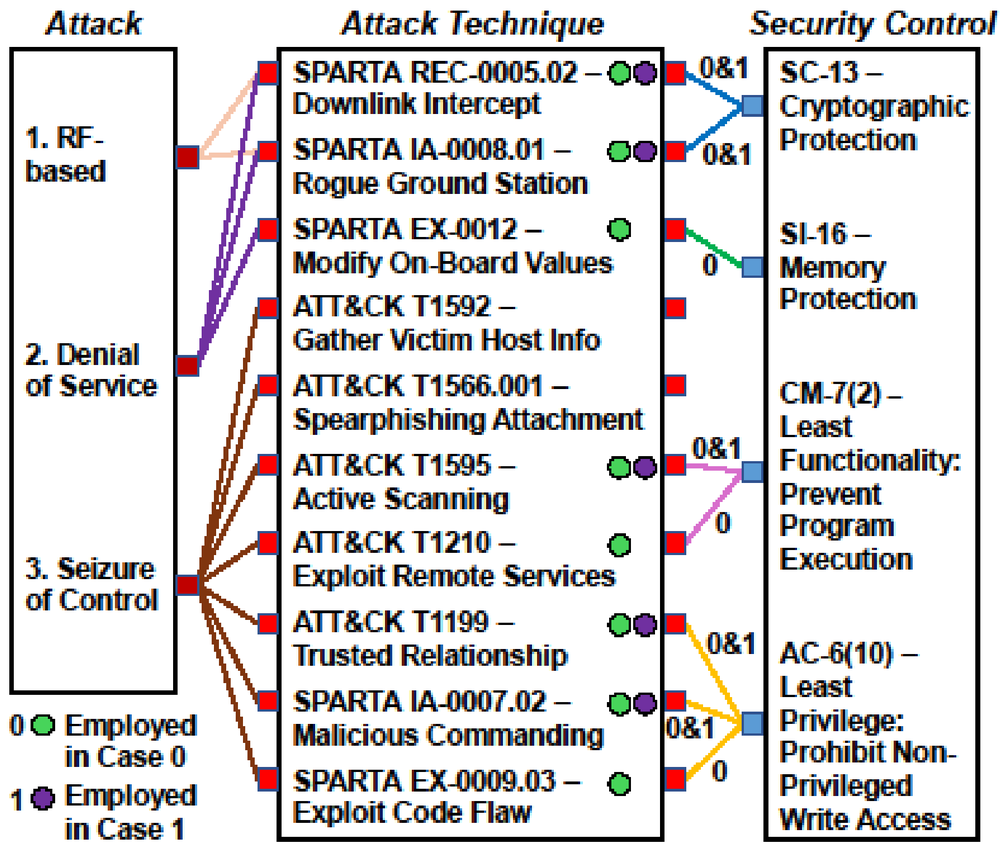
Results

Insight: Our framework can effectively harden missions by mitigating high risk attack techniques possessed by an attacker.

Mission Control and Data Flows in Space Infrastructure



3 Case Studies with Mapped Techniques and Controls



Future Research (Examples):

- Optimize hardening algorithms
- Apply system model to more case studies

Caleb Chang
University of Colorado Colorado Springs

An Actionable Framework for Space Cyber Risk Management

Abstract

Space infrastructures play critical roles in modern society, such as satellite communications (SATCOM). Like the Internet, space infrastructures are vulnerable to cyber attacks, dubbed *space cyber attacks*, highlighting the importance of managing cyber risks to space infrastructures, dubbed *space cyber risks*. However, adequately managing space cyber risks is an outstanding open problem. In this poster, we propose the first space cyber risk management framework to systematically analyze and mitigate space cyber risks. The framework models space infrastructures, space missions, and space cyber attacks, while offering algorithms for space mission risk analysis and hardening. We demonstrate its usefulness by conducting a case study on 3 real-world space cyber attacks against the SATCOM infrastructure implemented in our testbed. Our results show, among other things, that: (i) dealing with space cyber attack cascading effects is essential to space cyber risk management; (ii) the framework can effectively harden space missions; (iii) NIST security controls can effectively mitigate space cyber risks.

Caleb Chang
University of Colorado Colorado Springs

UCCS University of Colorado Colorado Springs