Cyber Attacks: An Emerging Threat to Satellites

This presentation does not contain any ITAR restricted material.

Paul Wood
Southwest Research Institute
paul.wood@swri.org

Agenda

- Cyber Security Threat Environment Evolution
- Requirements Management for Cyber Security Risks
- New Tools and Techniques to Mitigate Cyber Security Risks
- Questions/Comments

Traditional Cyber Threat Environment

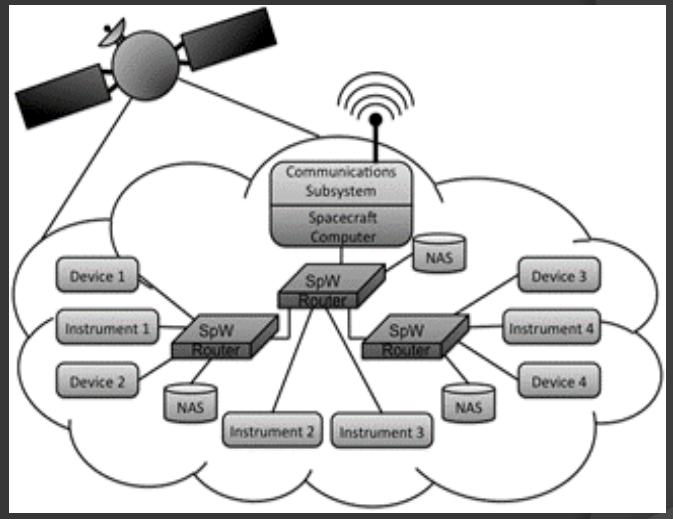
- Ground Segment was not networked
- S/C had obscure protocols & message formats
- Ground communications links were costly, large, and physically protected
- Assets were considered low value to attack
  - Easier, more desirable soft targets were available
  - Lightweight cyber attacks not practical

Current Cyber Threat Environment

- Ground Segment are networked
- S/C have better known protocols & message formats
- Lower cost, more portable communications links are possible
- All soft targets are on the radar

Emerging Cyber Threats

- Trends
  - Terrestrial-like networking on-board
  - S/C clusters with concepts for intra-cluster networking
  - S/C may be an extension of the ground network, with network links to relay satellites on orbit
- Provenance of software, firmware, and components increasingly in question,
  - Demand for capabilities exceeds budgets unless using lower provenance software/hardware



Requirements Management for Cyber Security Threats

- First: Need to recognize that threats exist
- Second: Need to analyze the risks
- Third: Need to develop requirements to address cyber security

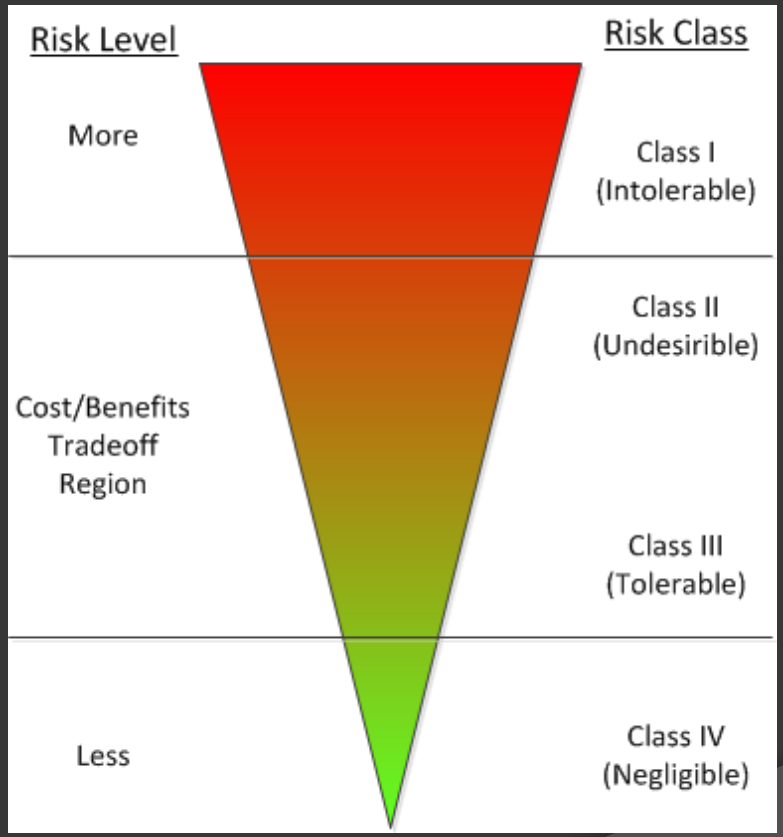
- Can use a model similar to safety risk analysis
- Build a security risk matrix to support analysis and prioritizing of risks

Cyber Security Risk Matrix (Consequence + Frequency = Risk Class)

Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Moderate	I	I	II	II
Occasional	I	II	III	III
Remote	II	III	III	IV
Unlikely	III	III	IV	IV
Impossible	IV	IV	IV	IV

Interpreting the Matrix

- Code from matrix shows risk class once frequency and consequence are known
- Class I risks must be addressed
- Class II/III risks require cost/benefits analysis
- Class IV risks are ignored



Cyber Security Requirements

- Cyber security risks require product requirements similar to safety or reliability
- Requirements need to have the following characteristics
  - Clear
  - Concise
  - Testable
  - Tracked in design & verification

Example Cyber Security Requirements

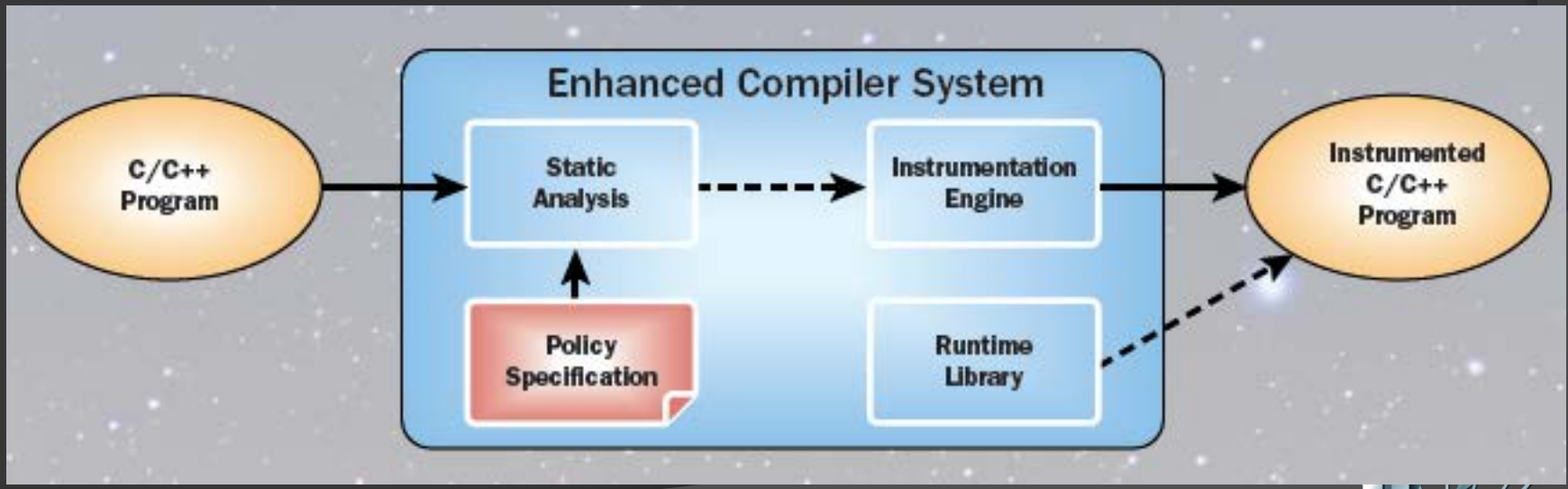
- Weak
  - The software shall incorporate a memory monitor that generates alerts in the event of abnormal memory use
  - The software shall be free of memory stack overflow vulnerabilities
- Better
  - The software shall incorporate a memory monitor that generates alerts in the event of increasing memory use once system initialization is complete
  - The software shall use counted functions for all string operations

New Tools & Techniques to Mitigate Risks

- Static Code Analysis
  - Many tools available
  - Open source and commercial
  - Greater focus on security in commercial tools
- Dynamic Analysis
  - Instrumentation of code
  - Test case generation
    - Code coverage
    - Boundary cases
- These tools generally focus on testing phase

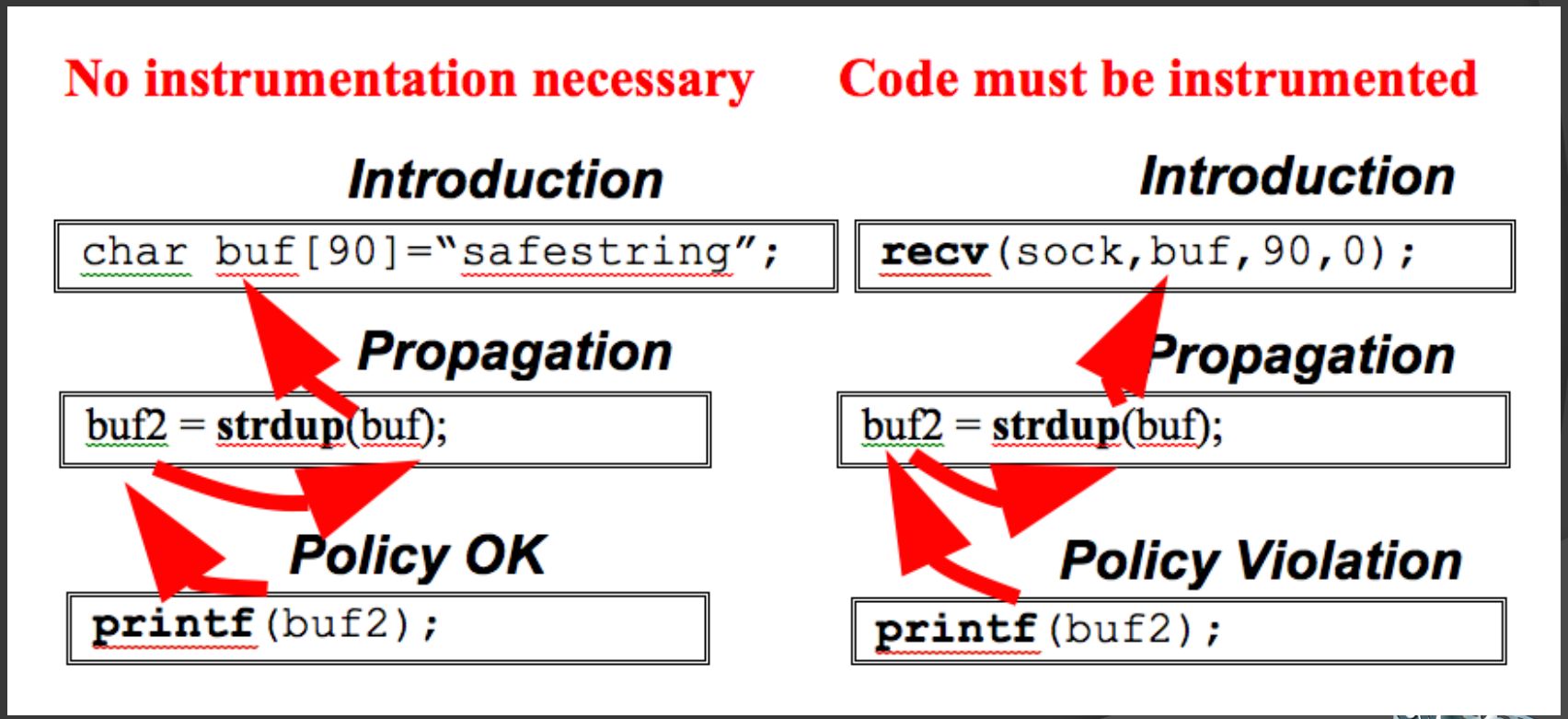
Enhanced Compiler (DDFA)

- Instrument code to enforce security policy at runtime
- Supports a “fight through” paradigm
- Can protect against code with limited provenance or history
- DDFA = Dynamic Data Flow Analysis



Code Instrumentation in DDFA

- Only code with potential vulnerabilities requires instrumentation



Detailed DDFA Example

Introduction

```
recv(sock, buf, 100, 0);
ddfa_insert(LTAINT, buf, strlen(buf), TAINTED);
```

Propagation

```
buf2 = strdup(buf);
ddfa_copy_flowval(LTAINT, buf2, buf, strlen(buf2));
```

Policy Violation

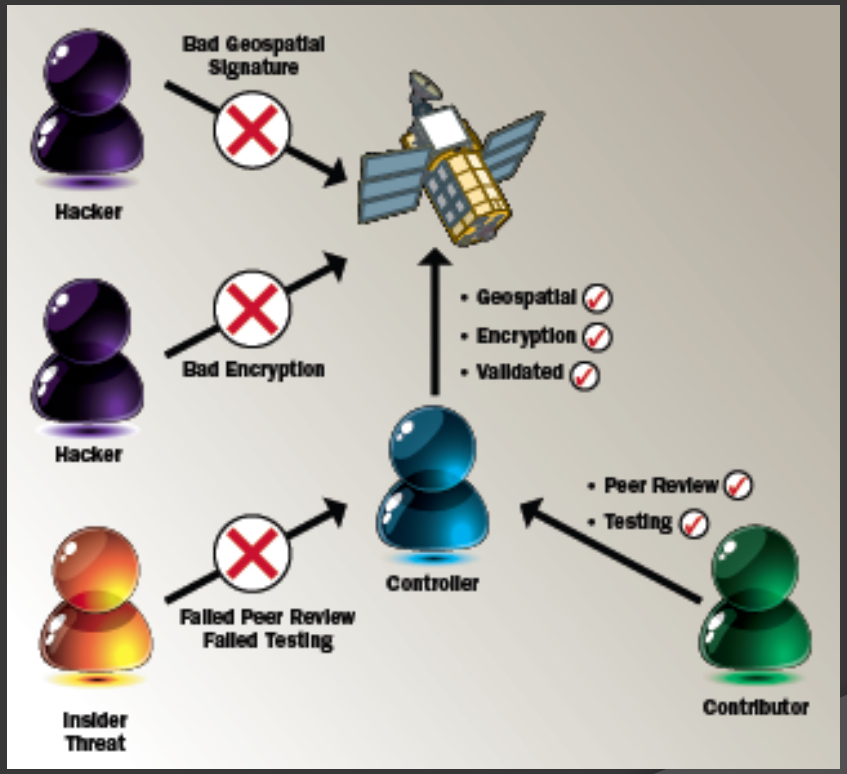
```
if (ddfa_check_flowval(LTAINT, buf2, TAINTED))
{
  if (! fsv_sanitize(buf2))
  {
    log_fsv_error(buf2);
  }
  else
  {
    printf(buf2);  // OK, buf2 sanitized
  }
else
{
  printf(buf2);   // OK, buf2 not tainted
}
```

Example Cyber Security Risks

- Loss of data (denial of service)
  - Resets, corruption of OFPs and control data
- Potential loss of asset
  - EEPROM write life exhausted
  - Propellant consumption
  - Orientation corruption (pointing, excess spin)
- Use as weapon
  - Compromise an orbit, hit another asset, deorbit

Examples for Mitigating Risks

- Encryption
- Geospatial Signatures
- Strong development processes
  - Peer reviews
  - Testing
- Active countermeasures
  - DDFA



Conclusion

- Cyber Security is a Concern
- Threats are Emerging Due To
  - Increasing networking of Space Systems
  - Use of low-provenance software and hardware
- Identify System Security Requirements & Fix
- New Techniques & Tools Can Help
  - Static & dynamic code analysis
  - Code augmentation to “fight through” attacks

Questions?

Acronyms

CCSDS	Consultative Committee for Space Data Systems
CFDP	CCSDS File Delivery Protocol
FTP	File Transfer Protocol
IETF	Internet Engineering Task Force
OSI	Open Systems Interconnection
RFC	Request For Comments
SCPS	Space Communications Protocol Specification
SCPS-FP	SCPS File Protocol
SCPS-TP	SCPS Transport Protocol
SMTP	Simple Mail Transfer Protocol
TFTP	Trivial File Transfer Protocol