



Reliable and Secure Space Communication Protocols

Reliable and effective ground-space communication is important for all NASA Missions. Security against malicious attacks has become a major issue. Our development tool-supported framework will enable the cost-effective, flexible development of correct and safe protocols for the specific needs of sustained Exploration Missions

Background

Reliable communication between ground and spacecraft is central to mission success, especially in the realms of digital communication (data and command links). Seen in the light of recent events, these communication links are vulnerable to malicious intrusion. If terrorists or hackers illegally listen to, or worse, modify communication content, disaster can occur. The consequences of a nuclear powered spacecraft under control of a hacker or terrorist could be devastating. Therefore, all communications to and between spacecraft must be extremely secure *and* reliable.

Although secure communication protocols are in wide use (e.g., on the Internet), history has shown that many errors and vulnerabilities exist and have been exploited. Such security flaws may be introduced (or fail to be detected) during all stages of the software development cycle, like vulnerable encryption algorithms (design) or buffer overrun errors during implementation. Mission specific requirements (low bandwidth, high latency [20 minutes to Mars], low on-board computational capabilities) pose additional severe challenges for secure communication software.

Research Overview

Reliable and secure space communication software can only be developed with a unified end-to-end approach for the design, analysis, implementation, and certification, which is based upon rigorous logical and mathematical foundations. We are proposing a set of tools integrated into a software process which, given an intuitive, yet concise definition of all protocol requirements (e.g., using the Unified Modeling Language UML), can automatically perform the necessary analyses, support simulation, and automatically generate all required artifacts (code, documentation, certificates).



Because all software development steps are derived from one high level specification of the protocol and its properties, results of all analyses and the generated code is always in sync, thus eliminating many errors yielding the communication software insecure. Formal-based tools for protocol optimization (e.g., to accommodate low bandwidths / low computational requirements), and automatic, tamper-proof certification can provide explicit guarantees about important reliability and security properties and the absence of implementation errors. Thus a tremendous increase in correctness and reliability of the communication software can be obtained which in turn leads to better security.

Relevance to Exploration Systems

CEV and other space vehicles require a reliable, safe and secure means of communication. Malicious attacks can jeopardize lives and mission success. Our approach enables the designer to cost-effectively develop verified and correct code for Code-T's specific communication requirements (e.g., 20 min latency in communications to Mars).

H&RT Program Elements:

This research capability supports the following H&RT program /elements:

ASTP/Software, Intelligent Systems & Modeling

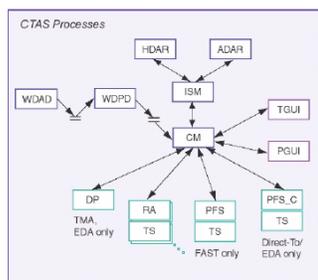
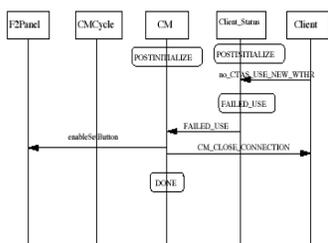
CCEI/Communications, Computing, Electronics and Imaging

Point of Contact:

Johann Schumann, RIACS/USRA

(650) 604-0941 schumann@email.arc.nasa.gov

<http://ase.arc.nasa.gov/schumann>



```
Send(char *buf){
int i;
for (i=0; i<n;i++)
{
```

