SafeDocs Transition to Operational Platforms

Secure parsers provide formal guarantees of security for input handling code for operational technologies

SafeDocs secure parsers are adoptable amongst a variety of platforms and enables conformance testing of open architecture systems. SafeDocs has a proven integration strategy and path for operational platforms and secures legacy systems for which the codebase is inaccessible, protecting against memory corruption vulnerabilities.

Adversarial injection attacks are possible using commodity hardware, as we have seen in contested environments such as Russia/Ukraine. Now, more than ever, is the time to practice security in depth by replacing vulnerable input handling code with secure parsers, stemming from DARPA SafeDocs.

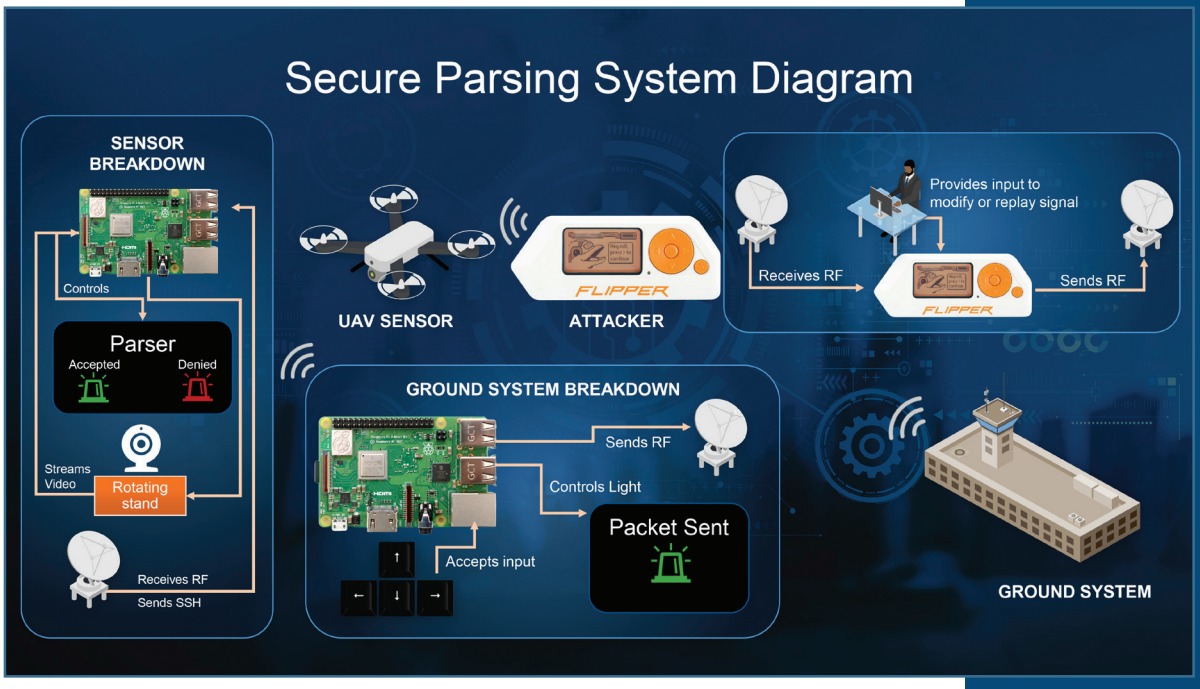
Procedure

- Identify relevant communication protocol(s) on platform
- Develop secure parser for protocol(s) using DARPA SafeDocs tooling
- Integrate secure parsers, replacing vulnerable input handling code; alternatively, wrap device interfaces with newly created secure parser
- Generate adversarial injection attack using Flipper Zero
- Thwart adversarial Flipper Zero attack by enabling Riverside-created secure parser
- Apply secure parser to real operational platform and beyond

RIVERSIDE RESEARCH

Key Features

- Secures legacy systems for which the codebase is inaccessible
- Has a proven integration strategy and path for operational platforms
- Enables conformance testing of open architecture systems
- Inspects packets at the bit level against a formal grammar
- Protects against a wide variety of memory corruption vulnerabilities



SafeDocs Transition to Operational Platforms

Observations

Our secure parser protects against all adversarial attacks that attempt to corrupt the default input handling code of the MORA protocol being used on the device. It does this by leveraging a SafeDocs-created secure parser tooling that covers all edge cases of input handling injection attacks.

We transitioned technology created by DARPA SafeDocs to open architecture frameworks. More specifically, we created a secure parser using the parser-combinator library Hammer (created under SafeDocs) to parse Modular Open Radio-Frequency Architecture (MORA) messages. MORA is used in over 20 DoD programs. In this demonstration, we show how SafeDocs secure parsing technologies can be transitioned to operational platforms using a candidate quadcopter with a camera that receives open architecture over-the-air radio frequency (RF) messages. Our secure parser can be turned on and off to demonstrate how an adversary can interfere with messages to cause mission failure, and how we can prevent these adversarial injection attacks. These same principles can be applied across operational platforms for security of military systems.

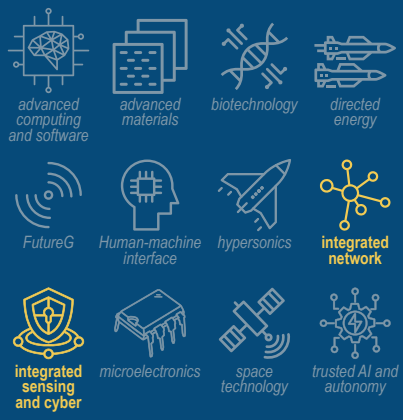
Next Steps

Updating our SafeDocs demonstration to include:

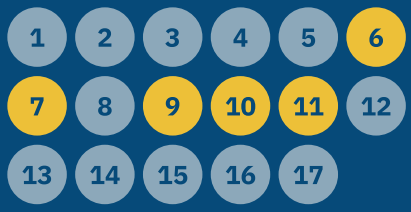
- A design with screens for monitoring network traffic and spikes
- Ability to interact with drone propellers
- Compass/position sensor on drone
- New camera gimbal to better show tracking
- New attacks to interact with the above components
- Sleeker, more compact form factor with new drone hardware

RIVERSIDE RESEARCH

Critical Tech Areas



DoD Priorities



1. Southwest Border Activities
2. Combating Transnational Criminal Organizations in the Western Hemisphere
3. Audit
4. Nuclear Modernization (including NC3)
5. Collaborative Combat Aircraft (CCAs)
6. Virginia-class Submarines
7. Executable Surface Ships
8. Homeland Missile Defense
9. One-Way Attack/Autonomous Systems
10. Counter-small UAS Initiatives
11. Priority Critical Cybersecurity
12. Munitions
13. Core Readiness, including full DRT funding
14. Munitions and Energetics Organic Industrial Bases
15. Executable INDOPACOM MILCON
16. Combatant Command support agency funding for INDOPACOM, NORTHCOM, SPACECOM, STRATCOM, CYBERCOM, and TRANSCOM
17. Medical Private-Sector Care