Steal This Drone: High-Assurance Cyber Military Systems (HACMS)

AFRL S5
1 August 2017

Dr. Darren Cofer
Advanced Technology Center
darren.cofer@rockwellcollins.com
Abbie Hoffman

steal this drone
Securing Cyber-Physical Systems: State of the Art

IT Systems

- Anti-virus scanning, intrusion detection systems, patching infrastructure
- This approach cannot solve the problem
  - Not convergent with the threat
  - Focused on known vulnerabilities; can miss zero-day exploits
  - Can introduce new vulnerabilities and privilege escalation opportunities

Control Systems

- Air gaps & obscurity?
  Forget the myth of the air gap – the control system that is completely isolated is history.
  – Stefan Woronka, 2011
  Siemens Director of Industrial Security Services

- Trying to adopt IT approaches, but technology is not a good fit:
  - Resource constraints, real-time deadlines
  - Extreme cost pressures
  - Patches may have to go through lengthy verification/certification processes
  - Patches could require recalls

October 2010 Vulnerability Watchlist

1/3 of the vulnerabilities are in security software!

We need a fundamentally different approach
The Dream...
Formal Methods: Complete Exploration of Design

\[ 3^2 + 4^2 = 5^2 \]
Formal Methods: Complete Exploration of Design

\[3^2 + 4^2 = 5^2\]
Formal Methods: Complete Exploration of Design

Testing can only show the presence of bugs (and only if you are lucky)
Formal Methods: Complete Exploration of Design

Testing can only show the presence of bugs (and only if you are lucky)
Formal Methods: Complete Exploration of Design

Testing can only show the presence of bugs (and only if you are lucky)
Formal Methods: Complete Exploration of Design

Testing can only show the presence of bugs (and only if you are lucky)

Analysis can show the absence of bugs (with evidence of correctness)
High-Assurance Cyber Military Systems (HACMS)

Architectural-Level
Rockwell Collins, University of Minnesota
Compositional Reasoning

Application-Level Software
Galois, CMU, Draper Labs, MIT, Oxford, Princeton, SpiralGen, University of Illinois, University of Pennsylvania
Generate from Specification, Correct by Construction, Software Verification, Robust Algorithms

Low-Level Software
Data61 (NICTA), Yale
Verified OS Kernels

Ground Vehicle
HRL
Integrate on TARDEC Autonomous Systems

Air Vehicle
Boeing
Integrate on Unmanned Little Bird

HACMS program:
Technology for the construction of high-assurance cyber-physical systems

Use formal methods to build systems that are resilient against cyber-attack because they can be proven not to have typical security vulnerabilities

Evaluation & Penetration Testing
Draper, AIS
High-Assurance Cyber Military Systems (HACMS)

HACMS program:
Technology for the construction of high-assurance cyber-physical systems

Use formal methods to build systems that are resilient against cyber-attack because they can be proven not to have typical security vulnerabilities.
HACMS in the News...

https://www.youtube.com/watch?v=DofZ9TickKA
High-Assurance Cyber Military Systems

- **Final Demonstrations**
  - Boeing Unmanned Little Bird (ULB): Mesa AZ, Feb 2017
  - Quadcopter: Sterling VA, Apr 2017
- **Demonstrated cyber-resiliency of both vehicles**
  - "Before" and "after" flight demonstrations
  - *Attacked in-flight*
  - Comprehensive evaluation by HACMS Red Team
- **Cyber-resiliency achieved through application of formal methods**
  - Model checking of architecture properties
  - Synthesis/verification of software components
  - Comprehensive proof of correctness of operating system

*Formal Methods are practical and effective for achieving cybersecurity in real aerospace systems*
Approach: Architecture-Driven Assurance

- Architecture model is correct
  - Properties, structure, behavior, interaction of components, interfaces, contracts
  - Analyzable
Approach: Architecture-Driven Assurance

- Architecture model is correct
  - Properties, structure, behavior, interaction of components, interfaces, contracts
  - Analyzable
- Components are correct
  - Consistent/realizable contracts
  - Components verified to implement contracts
Approach: Architecture-Driven Assurance

- Architecture model is correct
  - Properties, structure, behavior, interaction of components, interfaces, contracts
  - Analyzable
- Components are correct
  - Consistent/realizable contracts
  - Components verified to implement contracts
- System does what the model says
  - No other information flows (memory safety, isolation)
  - OS executes model correctly (incl. timing)
Approach: Architecture-Driven Assurance

- Architecture model is correct
  - Properties, structure, behavior, interaction of components, interfaces, contracts
  - Analyzable
- Components are correct
  - Consistent/realizable contracts
  - Components verified to implement contracts
- System does what the model says
  - No other information flows (memory safety, isolation)
  - OS executes model correctly (incl. timing)
- System implementation corresponds to model
  - Automatic build from component and architecture models
HACMS Accomplishments: Technologies

- **Open source tools, languages, software**
- seL4 formally verified OS kernel
  - Isabelle/HOL proof of correctness
  - Security properties proven to binary level
- Ivory/Tower embedded DSLs
  - Memory safe component software
  - Code generation from high-level specification
- Architecture modeling and analysis tools (AADL)
  - Assume-Guarantee Reasoning Environment (AGREE)
  - Architecture-based assurance cases (Resolute)
- Automated build from models
  - Support for seL4, eChronos, VxWorks, Linux
HACMS Accomplishments:
Demonstrations

- Practical and effective
- Quadcopter
- Boeing Unmanned Little Bird helicopter
- Army TARDEC autonomous HET (HRL)
HACMS Accomplishments: Transition plans

- Army: JMR/FVL
- Navy: PIMCS
- Marines: RQ-21
Unverified Unsecure Quadcopter
Remote Data Link Attack
Verified Secure Quadcopter
Remote Data Link Attack
**Verified Secure Quadcopter**

Remote Data Link Attack (Fork Bomb)
VIDEO: FLIGHT 2
Unmanned Little Bird – Baseline
USB Maintenance Device Attack
Unmanned Little Bird – Secure USB Maintenance Device Attack
Unmanned Little Bird – Secure
Supply Chain Attack (COTS SW)
VIDEO: ULB
Conclusions

• Formal Methods are *practical* and *effective* for building and verifying high-assurance aerospace systems
  – Applied and demonstrated in two aircraft
  – Transition to other platforms in-progress
  – Withstood cyberattacks both in lab and in flight
  – Usable by engineers (Boeing and Rockwell Collins)

• What next?
  – Supply Side: Research to reduce cost of development and integration by continuing to improve tools and technology
  – Demand Side: Customer (government/military) demand for comprehensive evidence of correctness, especially for cybersecurity requirements (negative requirements)
Further Reading/Viewing

• HACMS final demo videos

• DARPA Blocks Cyberattacks on Unmanned Little Bird In Flight (Aviation Week)

• Cybersecurity Skeptics Now Embracing Formal Methods (ACM Ubiquity)
  – http://ubiquity.acm.org/article.cfm?id=3081880
Code, papers, videos available at:

Loonwerks.com