Formal Verification for Mission Assurance in Cyberspace: Education, Tools, and Results

Shiu-Kai Chin

Professor, Department of Electrical Engineering & Computer Science
Syracuse University
Senior Scientist, Serco, Inc.

The Colloquium for Information Systems Security Education

11 June 2012

Acknowledgments

This is joint work with:

- Erich Devendorf, Ph.D., Serco, Inc.
- Sarah Muccio, Ph.D., Air Force Research Laboratory
- Susan Older, Ph.D., Syracuse University, Serco, Inc.
- Jim Royer, Ph.D., Syracuse University

Dr. Kamal Jabbour, ST, Senior Scientist, Information Assurance, USAF

- Cyber Revolution in Military Affairs
- Cybercraft
- Impregnable Design

Leadership in Cyberspace

Abraham Lincoln

"If I had eight hours to chop down a tree, I'd spend six hours sharpening my ax."

FM 3-0, Operations, Chapter 5: Command and Control

"Commanders continuously combine **analytic** *and* **intuitive** *approaches to decision-making to exercise battle command."*

NASA

"Systems engineering is first and foremost about getting the **right design** *. . . A great systems engineer completely understands and applies the art of* **leadership** *and has the experience and scar tissue from trying to* **earn** *the badge of* **leader** *from his or her team."*

Orientation: Overall Objectives

Desired End State

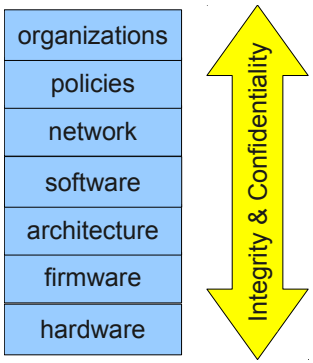
- Cyberspace leaders who have the combined knowledge and capabilities of military leadership and systems engineering

Critical Requirements

- Cyber engineering (computer engineering & science) research & education for contested environments to **reshape cyberspace to our advantage**
- Cyberspace leaders capable of solving operational and tactical problems, who refrain from magical thinking, and who can do the math while holding themselves and others accountable

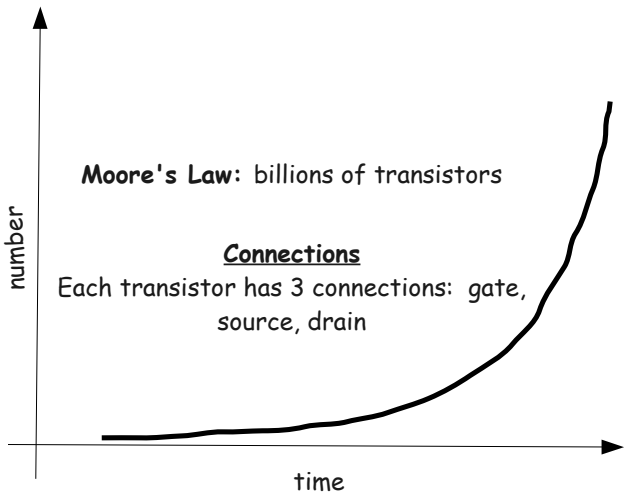
Orientation: Integrity of Command and Control

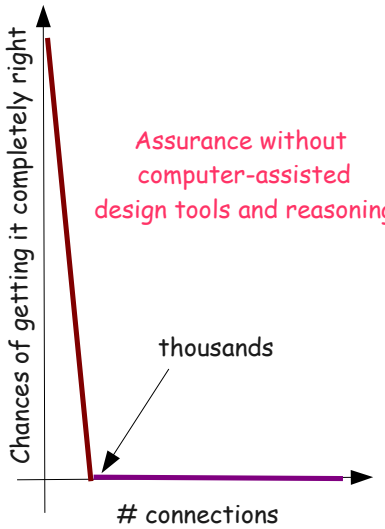
Security & integrity requirements span all levels of abstraction



- How do we account for integrity & security policies at each abstraction level?
- If you cannot secure physical memory all is lost at all levels above

Assurance: How do we know things are done correctly?





Computer-assisted reasoning tools?

Orientation: John Boyd

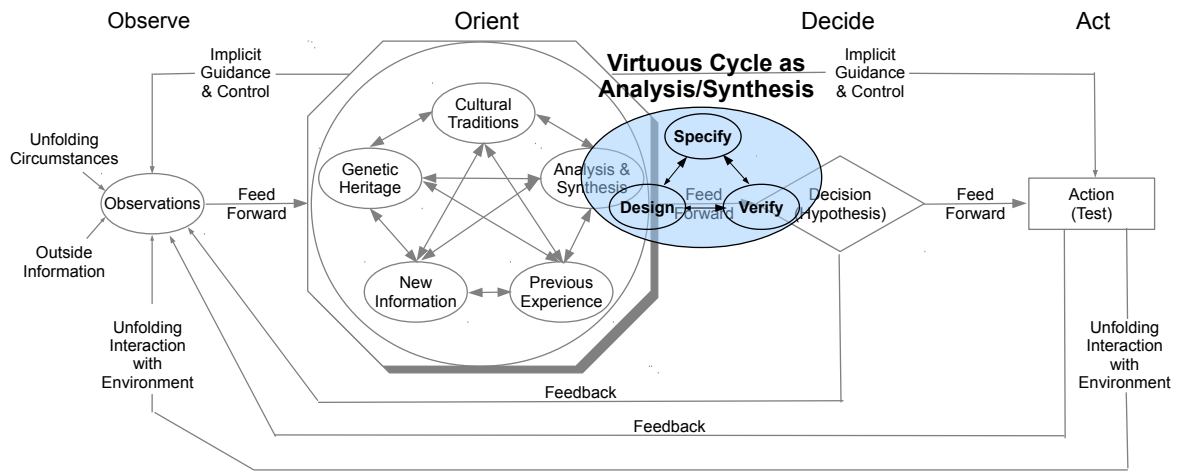
The Essence of Winning and Losing, 1995

"**Without analysis and synthesis** across a variety of domains or across a variety of competing/independent channels of information, we cannot evolve new repertoires to deal with unfamiliar phenomena or unforeseen change."

Implications for cyberspace

Mathematical analysis and synthesis for insight into why things work to achieve adaptability, not artificial certainty, as a counterweight to uncertainty

Where this talks fits



Purpose and Preview

Purpose

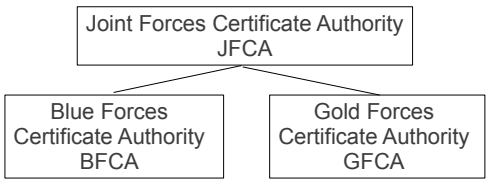
Show feasibility of equipping undergraduates to walk fully the virtuous cycle of formal specification, design, and verification in support of mission assurance in cyberspace

Preview

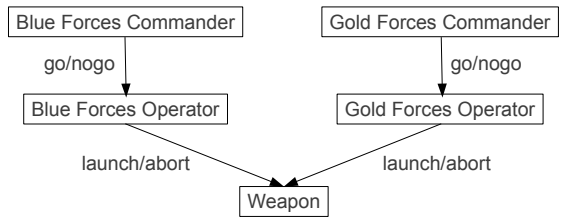
1. Examples of virtuous cycle achieved by undergraduates
2. Underlying educational basis
3. Educational research questions, lessons learned, & next steps
4. Conclusions & discussion

All Students Completed the Virtuous Cycle (1/4)

Specification of command and control

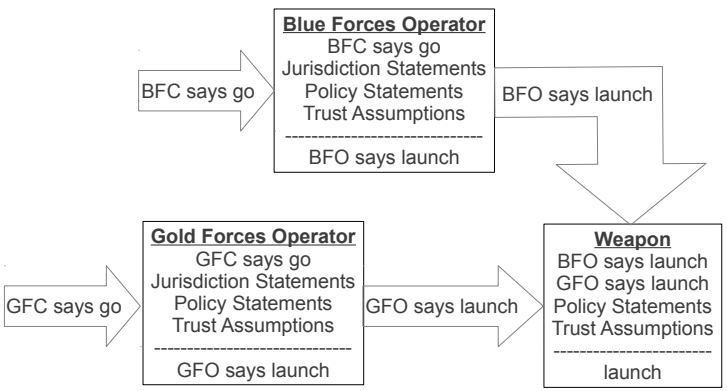


Certificate Authority Hierarchy

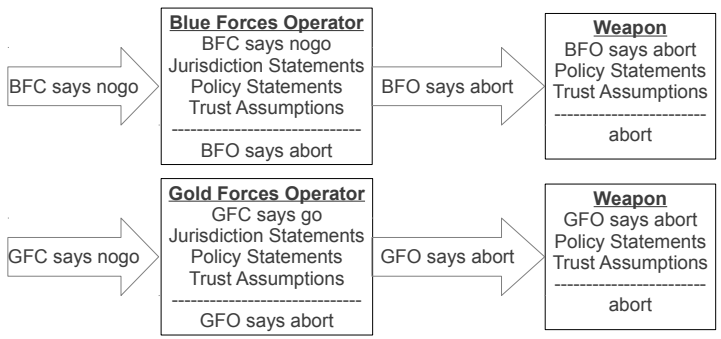


Flow of Command and Control

CONOPS Design with Access-Control Logic



Launch CONOPS



Abort CONOPS

Virtuous Cycle: Verified CONOPS (2/4)

Inference Rule in the access-control Calculus

$$\textit{BFO Launch Rule} \quad \frac{\textit{BFC says } \langle go \rangle \qquad \langle go \rangle \supset \langle launch \rangle \qquad \textit{BFC controls } \langle go \rangle}{\textit{BFO says } \langle launch \rangle}$$

Formally Verified HOL Theorem Corresponding to BFO Launch Rule

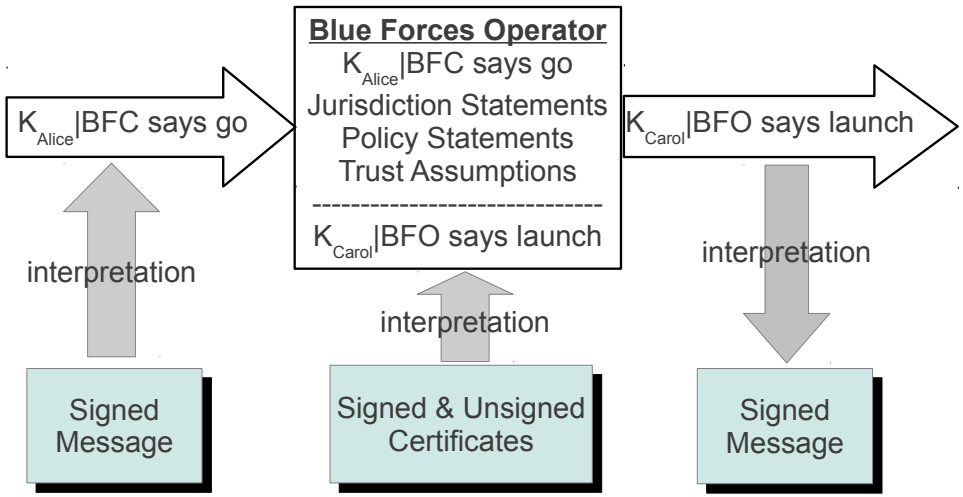
$$\begin{aligned} \vdash\ & (M, Oi, Os)\ \texttt{sat Name BFC says prop (MC go)} \Rightarrow \\ & (M, Oi, Os)\ \texttt{sat prop (MC go) impf prop (WC launch)} \Rightarrow \\ & (M, Oi, Os)\ \texttt{sat Name BFC controls prop (MC go)} \Rightarrow \\ & (M, Oi, Os)\ \texttt{sat Name BFO says prop (WC launch)} \end{aligned}$$

What this means

- Proves feasibility of teaching undergraduates to execute the virtuous cycle
- Previously thought to be impossible at the undergraduate level

Virtuous Cycle: Refinements (3/4)

Students Defined Formal Semantics of Message and Certificate Structures



Classification	Access-Control Statement
Signed Message:	$K_{Alice} \mid BFC$ says go
Signed Key Certificate:	K_{bfca} says $K_{Alice} \Rightarrow Alice$
Signed Key Certificate:	K_{jfca} says $K_{bfca} \Rightarrow BFCA$
Trusted Role Certificate:	$Alice$ reps BFC on go
Trusted Key Certificate:	$K_{jfca} \Rightarrow JFCA$
Jurisdiction Statement:	BFC controls go
Jurisdiction Statement:	$JFCA$ controls $K_{bfca} \Rightarrow BFCA$
Jurisdiction Statement:	$BFCA$ controls $K_{Alice} \Rightarrow Alice$
Policy Statement:	$go \supset launch$

Virtuous Cycle: Verified Refinements in HOL (4/4)

Students Formally Verified in HOL Theorems for Interpreting Messages

$$\vdash \forall \mathit{sender}\ \mathit{role}\ \mathit{recipient}\ \mathit{enDEK}\ \mathit{enCMDMsg}\ \mathit{Os}\ \mathit{Oi}\ \mathit{M}\ \mathit{CMDMsgSig}\ .$$

```
checkMSG
  (MSG (From sender) (As role) (To recipient) enDEK
     enCMDMsg CMDMsgSig) ⇒
((M,Oi,Os) msat
 MSG (From sender) (As role) (To recipient) enDEK enCMDMsg
   CMDMsgSig ⟺
 (M,Oi,Os) sat
 Name (MKey (pubK (KStaff sender))) quoting
 Name (MRole role) says
 prop
   (getCommand
      (MSG (From sender) (As role) (To recipient) enDEK
         enCMDMsg CMDMsgSig)))
```

Fall 2011 Cyber Engineering Semester

Demographics of Fall 2011 Program: Six students

- Minimum GPA $\geq$ 3.3
- 4 computer engineering, 2 computer science
- 4 SU, 1 Texas A&M, 1 Michigan Tech; 3 ROTC, 3 civilian

Schedule

	Monday	Tuesday	Wednesday	Thursday	Friday	
8am	Secure Hardware Laboratory	Secure Operating Systems	Secure Hardware Laboratory	Secure Operating Systems	Internship (AFRL)	8am
9am						9am
10am						10am
11am						11am
12pm						12pm
1pm	Secure Computer Architecture	Cyber Engineering Seminar	Secure Computer Architecture	Cyber Engineering Seminar		1pm
2pm						2pm
3pm	Engineering Assurance Laboratory		Engineering Assurance Laboratory			3pm
4pm						4pm

Col (ret) Fred Wieners: leadership case studies–**courage and competence**

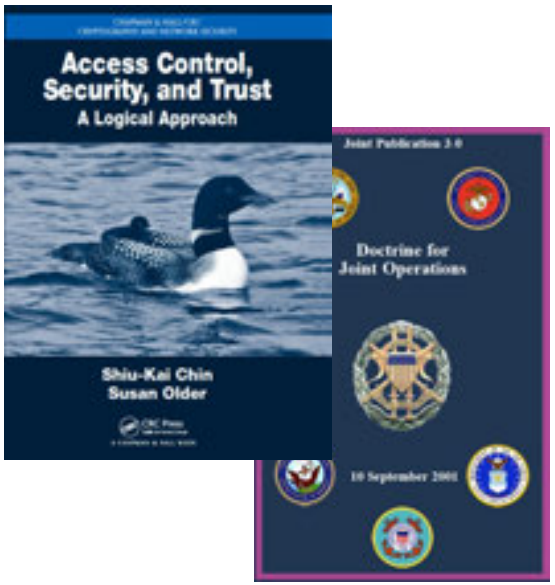
- Gettysburg Leadership Staff Ride
- Normal Accident Theory/Critical Decision Case Studies: Apollo 13, Space Shuttle Disasters, Black Hawk Shootdown
- Eastern Air Defense Sector tour & 9/11 Failure to Anticipate

Educational Basis

10 Years of Research, Education, and Experimentation

ACE Class of 2006

- 2003–2010: **226+ ACE graduates from 40+ universities**
- 2011–2012: **IA Internship: 13+25 students**
- 2011–2012: **Cyber Engineering Semester: 6 + 6+ students**



- Jointly taught by AFRL, Serco, Inc., & SU
- Access-control textbook written based on ACE
- Reasonable to link operational art with systems engineering **with mathematical rigor**

Research Questions and Lessons Learned

Educational Research Questions

Are **undergraduate** students able to rigorously comprehend, analyze, and synthesize the concepts put forth in Saltzer and Schroeder's *The Protection of Information in Computer Systems*?

- Q: Were we asking too much? A: *Almost*
- Q: Could the students "connect the dots"? A: *Mostly*
- Q: Could students use theorem provers? A: *Yes*

Lessons Learned

- Small size of pilot program allowed mid-course corrections across 5 courses to help students "connect the dots" and relieve time pressure
- Access-control logic across courses provided a common calculus for security and integrity
- Mutually reinforcing assignments across courses works
- Functional programming (Haskell) + access-control logic effective for developing programming skills and thinking logically about security and integrity
- HOL worked because of acquired functional programming skills, restricting use of HOL to the access-control logic, and students' familiarity with the access-control logic

Next Steps

Fall 2012 Cyber Engineering Semester

- Refinements in schedule and assignments over all courses for increased mutual support of common ideas and principles
- Reduction in intensity
- Eye toward 1-year, 2-year, and 4-year programs

Virtuous Cycle

- Compose (within HOL) access-control logic (ACL) with structural operational semantics (SOS) to account for operational policy changes in transition systems—*prototype demonstrated*
- Develop (within HOL) a refinement strategy where all operational policy changes and configuration changes are explicitly justified—*prototype demonstrated*
- Develop (within HOL) modal mu logic to augment ACL and SOS to reason about modal and temporal properties—*prototype almost complete*

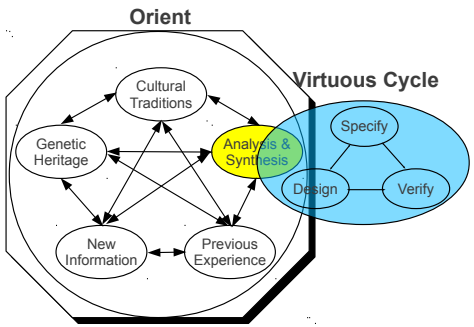
Conclusions and Discussion

There's no substitute for competence

Col. Henry Knox, 27 September 1776 on establishing artillery schools:

"... officers can never act with confidence until they are masters of their profession ..."

Orient future leaders by education and solving real problems



Developing courage and competence

- Establish culture & traditions
- Develop knowledge of self (heritage)
- Provide relevant information and experiences
- Teach analysis/synthesis using the virtuous cycle

Build a National Capability

Thousands of engineers and officers capable of mathematical analysis and leadership in support of designing, verifying, procuring, and operating cyber systems