Mission Assurance in Cyberspace:
Formal Methods and Tools for Security

Shiu-Kai Chin
Professor, Dept. of Electrical Engineering & Computer Science
Syracuse University, Syracuse, New York

This is joint work done by a team whose members will be disclosed in this talk

5 February 2013
2nd *Workshop on Formal Methods and Tools for Security*
Microsoft Research, Cambridge, UK

version 1.2

A Logical Approach to Access Control

Formal Method: an access-control logic

- Modification of multi-agent propositional modal logic with Kripke semantics created by Abadi, Burrows, Lampson, and Plotkin
  - Our mods: added delegation, redefined roles, added security and integrity labels, and inference rules
- Textbook: *Access Control, Security, and Trust: A Logical Approach*, Chin & Older, CRC Press, 2011

Tool: HOL theorem prover

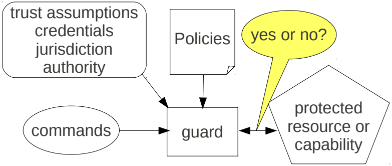
- Implemented as a conservative extension to HOL (joint work with Lockwood Morris) used by 30+ undergrads from 26 US universities
- Supports proof style in textbook used by 277+ undergrads from 50+ universities

Security Applications

- JP Morgan Chase: Partner Key Management (PKM)—credentials management for high-value commercial transactions (SWIFT)
- US Air Force: command and control (C2) and secure messaging

Our Viewpoint

The central task



When given a command/request, trust assumptions, credentials, jurisdiction, authority, and policy

- Logically justify if the command/request is honored or not
- Anything less is regarded as a don't know, don't care, or incompetence

No different for hardware designers and verifiers

Access-Control Logic Syntax & Semantics

Access-Control Logic Syntax & Semantics

Syntax	BNF

Access-Control Logic Syntax & Semantics

Syntax

- Principals (actors)

BNF

Access-Control Logic Syntax & Semantics

Syntax	BNF
- Principals (actors)	$P ::= A \;/\; P \,\&\, Q \;/\; P \mid Q$

Access-Control Logic Syntax & Semantics

Syntax

BNF

- Statements they make

Access-Control Logic Syntax & Semantics

Syntax

- Statements they make

BNF

$$\varphi \quad ::= \quad p \ / \ \neg\varphi \ / \ \varphi_1 \wedge \varphi_2 \ / \ \varphi_1 \vee \varphi_2 \ / \ \varphi_1 \supset \varphi_2 \ / \ \varphi_1 \equiv \varphi_2 \ /$$

Access-Control Logic Syntax & Semantics

- Statements they make $\varphi ::= P \Rightarrow Q \;/\; P \text{ says } \varphi \;/\; P \text{ controls } \varphi \;/\; P \text{ reps } Q \text{ on } \varphi$

Access-Control Logic Syntax & Semantics

Kripke structures

Semantics

Access-Control Logic Syntax & Semantics

Kripke structures

$W = \text{non-empty } \{\text{worlds}\}$

Semantics

Access-Control Logic Syntax & Semantics

Kripke structures

$$\begin{array}{rcl} W & = & \text{non-empty } \{\text{worlds}\} \\ I & = & \textbf{PropVar} \to \mathcal{P}(W) \end{array}$$

Semantics

Access-Control Logic Syntax & Semantics

Kripke structures

$$\begin{aligned} W &= \text{non-empty } \{\text{worlds}\} \\ I &= \textbf{PropVar} \to \mathcal{P}(W) \\ J &= \textbf{PName} \to \mathcal{P}(W \times W) \end{aligned}$$

Semantics

Access-Control Logic Syntax & Semantics

Kripke structures

$$\begin{aligned} W &= \text{non-empty } \{\text{worlds}\} \\ I &= \textbf{PropVar} \rightarrow \mathcal{P}(W) \\ J &= \textbf{PName} \rightarrow \mathcal{P}(W \times W) \\ \mathcal{M} &= \langle W, I, J \rangle \end{aligned}$$

Semantics

Access-Control Logic Syntax & Semantics

Kripke structures

$$\mathcal{M} = \langle W, I, J \rangle$$

Semantics

$$\mathcal{E}_{\mathcal{M}}[\![p]\!] = I(p)$$

Access-Control Logic Syntax & Semantics

Kripke structures

Semantics

$$\mathcal{E}_{\mathcal{M}}[\![\neg\varphi]\!] \quad = \quad W - \mathcal{E}_{\mathcal{M}}[\![\varphi]\!]$$

$$\mathcal{M} \quad = \quad \langle W, I, J \rangle$$

Access-Control Logic Syntax & Semantics

Kripke structures

$$\mathcal{M} = \langle W, I, J \rangle$$

Semantics

$$\mathcal{E}_{\mathcal{M}}[\![\varphi_1 \wedge \varphi_2]\!] = \mathcal{E}_{\mathcal{M}}[\![\varphi_1]\!] \cap \mathcal{E}_{\mathcal{M}}[\![\varphi_2]\!]$$

Access-Control Logic Syntax & Semantics

Kripke structures

$$\mathcal{M} = \langle W, I, J \rangle$$

Semantics

$$\mathcal{E}_{\mathcal{M}}[\![\varphi_1 \vee \varphi_2]\!] = \mathcal{E}_{\mathcal{M}}[\![\varphi_1]\!] \cup \mathcal{E}_{\mathcal{M}}[\![\varphi_2]\!]$$

Access-Control Logic Syntax & Semantics

Kripke structures

Semantics

$$\mathcal{M} \quad = \quad \langle W, I, J \rangle$$

$$\begin{array}{rcl} \mathcal{E}_{\mathcal{M}}[\![\varphi_1 \supset \varphi_2]\!] & = & (W - \mathcal{E}_{\mathcal{M}}[\![\varphi_1]\!]) \cup \mathcal{E}_{\mathcal{M}}[\![\varphi_2]\!] \\ \mathcal{E}_{\mathcal{M}}[\![\varphi_1 \equiv \varphi_2]\!] & = & \mathcal{E}_{\mathcal{M}}[\![\varphi_1 \supset \varphi_2]\!] \cap \mathcal{E}_{\mathcal{M}}[\![\varphi_2 \supset \varphi_1]\!] \end{array}$$

Access-Control Logic Syntax & Semantics

Kripke structures

Semantics

$$\mathcal{M} = \langle W, I, J \rangle$$

$$\begin{aligned}
\mathcal{E}_{\mathcal{M}}[\![P \Rightarrow Q]\!] &= \begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases} \\
\mathcal{E}_{\mathcal{M}}[\![P \text{ says } \varphi]\!] &= \{w \mid J(P)(w) \subseteq \mathcal{E}_{\mathcal{M}}[\![\varphi]\!]\} \\
\mathcal{E}_{\mathcal{M}}[\![P \text{ controls } \varphi]\!] &= \mathcal{E}_{\mathcal{M}}[\![(P \text{ says } \varphi) \supset \varphi]\!] \\
\mathcal{E}_{\mathcal{M}}[\![P \text{ reps } Q \text{ on } \varphi]\!] &= \mathcal{E}_{\mathcal{M}}[\![P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi]\!]
\end{aligned}$$

Inference Rules

Inference Rules

Rules

Inference Rules

Rules

- Inconvenient to use Kripke semantics

Inference Rules

Rules

- Use inference rules $\dfrac{H_1 \cdots H_n}{C}$ instead

Inference Rules

SOUNDNESS

Inference Rules

Soundness

$\dfrac{H_1 \cdots H_n}{C}$ is sound if *for all Kripke structures* $\mathcal{M}$ and each $i \in \{1, \ldots, n\}$:

Inference Rules

Soundness

$\dfrac{H_1 \cdots H_n}{C}$ is sound if *for all Kripke structures* $\mathcal{M}$ and each $i \in \{1, \ldots, n\}$:

If all $\mathcal{E}_{\mathcal{M}}[\![H_i]\!] = W$

Inference Rules

Soundness

$\dfrac{H_1 \cdots H_n}{C}$ is sound if *for all Kripke structures* $\mathcal{M}$ and each $i \in \{1, \ldots, n\}$:

$$\text{If all } \mathcal{E}_{\mathcal{M}}[\![H_i]\!] = W$$
$$\text{then } \mathcal{E}_{\mathcal{M}}[\![C]\!] = W$$

Inference Rules

Soundness

- All rules are sound

Inference Rules

SOUNDNESS

- All verified in HOL

Inference Rules

Core inference rules

Taut $$\frac{}{\varphi}$$ if φ is an instance of a prop-logic tautology

Modus Ponens $$\frac{\varphi \qquad \varphi \supset \varphi'}{\varphi'}$$

Says $$\frac{\varphi}{P \text{ says } \varphi}$$

MP Says $$\frac{}{(P \text{ says } (\varphi \supset \varphi')) \supset (P \text{ says } \varphi \supset P \text{ says } \varphi')}$$

Speaks For $$\frac{}{P \Rightarrow Q \supset (P \text{ says } \varphi \supset Q \text{ says } \varphi)}$$

Quoting $$\frac{}{P \mid Q \text{ says } \varphi \equiv P \text{ says } Q \text{ says } \varphi}$$

& Says $$\frac{}{P \,\&\, Q \text{ says } \varphi \equiv P \text{ says } \varphi \wedge Q \text{ says } \varphi}$$

Idempotency of $\Rightarrow$ $$\frac{}{P \Rightarrow P}$$

Monotonicity of $\mid$ $$\frac{P' \Rightarrow P \quad Q' \Rightarrow Q}{P' \mid Q' \Rightarrow P \mid Q}$$

Associativity of $\mid$ $$\frac{P \mid (Q \mid R) \text{ says } \varphi}{(P \mid Q) \mid R \text{ says } \varphi}$$

$$P \text{ controls } \varphi \quad \stackrel{\text{def}}{=} \quad (P \text{ says } \varphi) \supset \varphi$$

$$P \text{ reps } Q \text{ on } \varphi \stackrel{\text{def}}{=} P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi$$

Purpose and Preview

Purpose

Describe an ongoing 10-year experiment by DoD, industry, and academia whose purpose is to develop the next generation of cyberspace leaders

Why would 4-star generals listen to a briefing on access-control and HOL?

- Rest of presentation taken (mostly) from *Cyberspace Operations Executive Course*
- 6 times since 2010

Preview

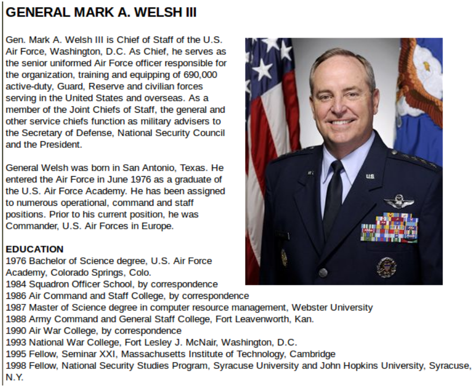
1. The challenge
2. Historical lessons (military view of why math matters)
3. Approach and overview of programs
4. Examples
5. Why we are hopeful
6. Concluding remarks

What Military Leaders Worry About

Mission Assurance

Assurance that critical system capabilities necessary to complete a mission successfully are available, correctly implemented, and secure.

Unknown → Misunderstanding → Uncertainty → Surprise → Defeat



GENERAL MARK A. WELSH III

Gen. Mark A. Welsh III is Chief of Staff of the U.S. Air Force, Washington, D.C. As Chief, he serves as the senior uniformed Air Force officer responsible for the organization, training and equipping of 690,000 active-duty, Guard, Reserve and civilian forces serving in the United States and overseas. As a member of the Joint Chiefs of Staff, the general and other service chiefs function as military advisers to the Secretary of Defense, National Security Council and the President.

General Welsh was born in San Antonio, Texas. He entered the Air Force in June 1976 as a graduate of the U.S. Air Force Academy. He has been assigned to numerous operational, command and staff positions. Prior to his current position, he was Commander, U.S. Air Forces in Europe.

EDUCATION
1976 Bachelor of Science degree, U.S. Air Force Academy, Colorado Springs, Colo.
1984 Squadron Officer School, by correspondence
1986 Air Command and Staff College, by correspondence
1987 Master of Science degree in computer resource management, Webster University
1988 Army Command and General Staff College, Fort Leavenworth, Kan.
1990 Air War College, by correspondence
1993 National War College, Fort Lesley J. McNair, Washington, D.C.
1995 Fellow, Seminar XXI, Massachusetts Institute of Technology, Cambridge
1998 Fellow, National Security Studies Program, Syracuse University and John Hopkins University, Syracuse, N.Y.

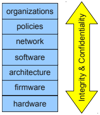
Their concerns:

- *"Will my weapon work?"*
- *"Will my command and control disappear?"*
- *"Will I lose situational awareness?"*
- Many do not have technical education
- Engineers are not generals, and vice versa
- What to do about cyberspace?

1. The challenge

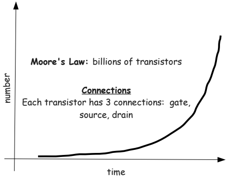
Integrity of Command and Control is Everything

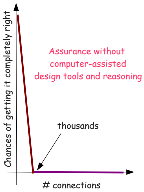
Security & integrity requirements span all levels of abstraction



- 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?





Goals

- Rigorous assurance of integrity & security spanning all abstraction levels
- Policy-based design and verification

Implication for Cyberspace

There is no assurance without computer-assisted reasoning

2. Historical Lessons
(Military View of Why Math Matters)

Military View (of why math matters): John Boyd (1/4)

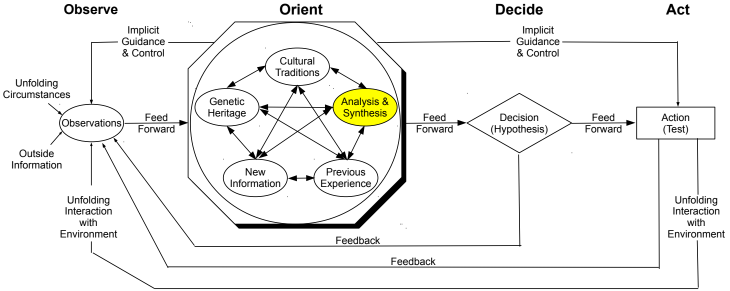
Forty Second Boyd

- Defeated any opposing pilot in air combat maneuvering in under 40 seconds
- Revered military strategist (maneuver, moral, mental, and physical warfare)
- General Charles Krulak, Marine Corps Commandant on Boyd's strategy for 1991 Gulf War:

  > *"The Iraqi army collapsed morally and intellectually under the onslaught of American and Coalition forces. John Boyd was an architect of that victory as surely as if he'd commanded a fighter wing or a maneuver division in the desert."*

Military View (of why math matters): John Boyd (2/4)

The Need for Speed and Maneuverability & How to Achieve It



Illumination: Organic Design for Command and Control, 1987

"The second O, orientation—as the repository of our genetic heritage, cultural tradition, and previous experiences—is the **most important part** of the O-O-D-A loop since it shapes the way we observe, the way we decide, the way we act."

Military View (of why math matters): John Boyd (3/4)

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."

What Boyd Did with Analysis & Synthesis

Analysis: doing the math at Georgia Tech

- Thermodynamics + Entropy + fighter pilot experience ⇒ **Energy-Maneuverability Theory**
- **Insight** into shortcomings of swing-wing aircraft

Synthesis: design with precision, accuracy, and insight

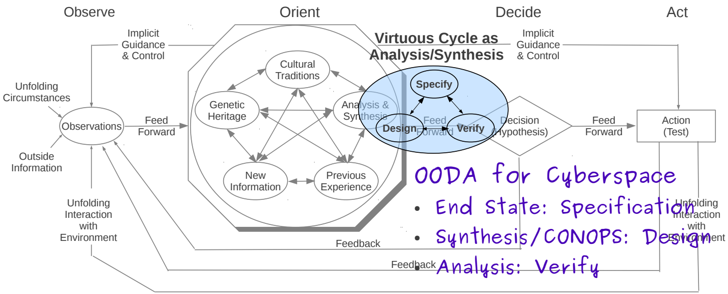
- New tactics: *Aerial Attack Study*, 1964
- New aircraft to meet mission requirements: F-16

Military View (of why math matters): John Boyd (4/4)

Implications for cyberspace (real value of formal methods)

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

Where this talk fits



OODA for Cyberspace

- End State: Specification
- Synthesis/CONOPS: Design
- Analysis: Verify

3. Team & Approach:
Focus on Connecting the Dots

- *Subject matter experts: military, operational, systems, semantics*
- *Trade breadth for depth to link specific policies and concepts of operation to particular implementations*
- *Formal specification and verification using HOL for assurance by third-parties*

The Team

Leader: Dr. Kamal Jabbour, ST, USAF Senior Scientist for IA

Principal scientific authority and independent researcher in IA, defensive information warfare, and offensive information warfare technology. He conceives, plans, and advocates major research and development activities for the Air Force, DoD, universities, and industry.

Military Subject Matter Experts (all with Serco-NA, Inc)

Col (ret) William Gray, Jr., USAF
Director Intelligence & Reconnaissance, AFRL; Asst Deputy Chief of Staff, Intelligence, USAFE; Chief, Intelligence Planning Division, HQ USAF

Col (ret) Frederick Wieners, USAF
4,200 hours as crew commander & instructor pilot B-52G, FB-111, B-1 aircraft; 1st commander Air Force Weapons School B-1B Division; Pentagon Air Staff, Joint Staff, OSD; Chairman Dept of Military Strategy and Operations, National War College

Lt Col (ret) Ken Chaisson, USAF
23 years of command, leadership, and supervisory expertise in USAF, Intelligence Community, Joint Cyber, and Defense Contracting environments

The Team

Air Force Research Lab Technical Staff

Dr. Sarah Muccio, USAF
DR-II, USAF, PhD Applied Math, Information Assurance Director, mission assurance, mission mapping

Dr. Erich Devendorf, Serco Inc
Serco Inc, Research Engineer, PhD Mechanical Engineering, risk in cyber operations, optimization, design of complex systems

Thomas N.J. Vestal, USAF
DR-II, USAF, secure computer architectures, cyber threat analysis, trusted hardware design, formal verification, cyber intelligence, cyber law

Michael Muccio, USAF
DR-II, USAF, wireless tactical mesh networks, self-healing and adaptive wireless networks, advanced routing protocols

The Team

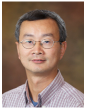
Syracuse University

Dr. Sue Older
CES Program Director, Associate Professor, semantics, concurrency

Dr. Steve Chapin
Associate Professor, Operating Systems, Security, Networking, Assurance

Dr. Qinru Qiu
Associate Professor, IC Power Management, Performance Optimization

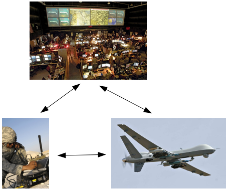
Dr. Shiu-Kai Chin
Professor, formal methods, security, access control



Dr. Kevin Du
Professor, Computer & Network Security, Data Mining, Privacy

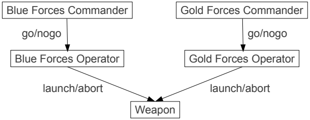
Approach: Derive Principles from Real Missions

Distributed Control of Remotely Piloted Aircraft (RPAs)



- Visits to 3rd Air Force and 174 FW
- Talks with JTACs, AOC staff, RPA pilots
- Description of C2 CONOPS in access-control logic
- Verification of C2 CONOPS by machine-checked formal proofs

Principles and Examples



Blue Forces Commander

go/nogo

Blue Forces Operator

launch/abort

Gold Forces Commander

go/nogo

Gold Forces Operator

launch/abort

Weapon

- Dual command & control structure
- Dual control of a weapon with accountability down to individual operators
- Formal description & verification of all
  - commands, jurisdiction, authorizations
  - personnel assignments, crypto operations, certificate authorities
  - message structure, trust assumptions

Approach: Apply Principles to Problems

2011 & 2012: RPA Mini-Hack

2011: 2 teams hacked RPAs in under 2 hours

2012: All 4 teams hacked RPAs in under 2 hours

2012 Experiments

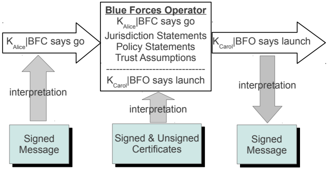
GPS spoofing & mitigation; Android mobile platforms

2012 Exercise: Secure C2 Operations in Clouds

- 4 simultaneous chess matches against Dr. Jabbour
- Teams physically isolated
- Each in 2 matches: command role & relay role
- Teams created own cloud & message structure on VM
- Operate and attack command clouds & relay clouds

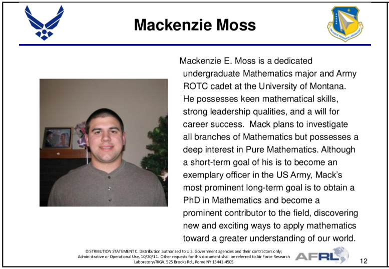
Approach: Top-to-Bottom Mission Assurance

Access-Control Logic for Conceptual Unity and Clarity



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

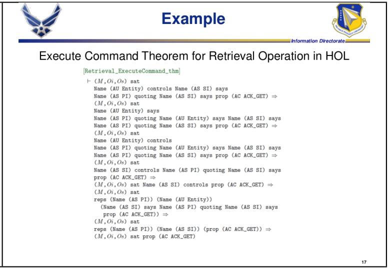
US Army ROTC Cadet Mackenzie Moss: 2012 IA Intern



Mackenzie Moss

Mackenzie E. Moss is a dedicated undergraduate Mathematics major and Army ROTC cadet at the University of Montana. He possesses keen mathematical skills, strong leadership qualities, and a will for career success. Mack plans to investigate all branches of Mathematics but possesses a deep interest in Pure Mathematics. Although a short-term goal of his is to become an exemplary officer in the US Army, Mack's most prominent long-term goal is to obtain a PhD in Mathematics and become a prominent contributor to the field, discovering new and exciting ways to apply mathematics toward a greater understanding of our world.

DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government agencies and their contractors only; Administrative or Operational Use, 10/20/11. Other requests for this document shall be referred to Air Force Research Laboratory/RIGA, 525 Brooks Rd., Rome NY 13441-4505



Example

Execute Command Theorem for Retrieval Operation in HOL

```
[Retrieval_ExecuteCommand_thm]
 ⊢ (M,Oi,Os) sat
   Name (AU Entity) controls Name (AS SI) says
   Name (AS PI) quoting Name (AS SI) says prop (AC ACK_GET) ⇒
   (M,Oi,Os) sat
   Name (AU Entity) says
   Name (AS PI) quoting Name (AU Entity) says Name (AS SI) says
   Name (AS PI) quoting Name (AS SI) says prop (AC ACK_GET) ⇒
   (M,Oi,Os) sat
   Name (AU Entity) controls
   Name (AS PI) quoting Name (AU Entity) says Name (AS SI) says
   Name (AS PI) quoting Name (AS SI) says prop (AC ACK_GET) ⇒
   (M,Oi,Os) sat
   Name (AS SI) controls Name (AS PI) quoting Name (AS SI) says
   prop (AC ACK_GET) ⇒
   (M,Oi,Os) sat Name (AS SI) controls prop (AC ACK_GET) ⇒
   (M,Oi,Os) sat
   reps (Name (AS PI)) (Name (AU Entity))
     (Name (AS SI) says Name (AS PI) quoting Name (AS SI) says
      prop (AC ACK_GET)) ⇒
   (M,Oi,Os) sat
   reps (Name (AS PI)) (Name (AS SI)) (prop (AC ACK_GET)) ⇒
   (M,Oi,Os) sat prop (AC ACK_GET)
```

Approach: Computer-Assisted Reasoning Tools

CONOPS determines methods taught

- Devise a CONOPS
- Formalize it in the access-control logic
- Verify its validity in HOL
- Implement it in Haskell

Assurance claims verified by HOL-4 theorem prover

- Implemented in ML functional language
- Inference rules are functional programs
- Extensive library of theories
- Access-control logic conservative extension of HOL
- Each step in CONOPS is a valid inference rule

Execution using Haskell functional programming language

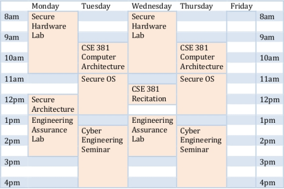
- Implementation of CONOPS described in HOL
- Message structure and crypto operations

Third parties can rapidly reproduce & verify CONOPS

- All proofs & documentation easily recreated & re-verified in minutes
- Formulas typeset by HOL–no typos!
- **Clarity & conceptual unity quickly**
- Miscommunication causes 80% aircraft mishaps—cyber?

Cyber Engineering Semester & IA Internship

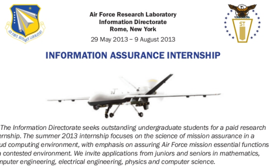
Cyber Engineering Semester: 18 credit hours



	Monday	Tuesday	Wednesday	Thursday	Friday	
8am	Secure Hardware Lab		Secure Hardware Lab			8am
9am						9am
		CSE 381 Computer Architecture		CSE 381 Computer Architecture		
10am						10am
11am		Secure OS		Secure OS		11am
			CSE 381 Recitation			
12pm	Secure Architecture					12pm
1pm	Engineering Assurance Lab		Engineering Assurance Lab			1pm
		Cyber Engineering Seminar		Cyber Engineering Seminar		
2pm						2pm
3pm						3pm
4pm						4pm

- Seminar (3): Access control, mission-based projects
- Hardware Lab (3): CPU w/virtual memory
- Secure Architecture (1): access control, HOL, operational semantics
- Computer Architecture (3): standard
- Secure Operating Systems (4): access control, micro-kernels
- Assurance Lab (4): HOL & Haskell

Information Assurance Internship: 10 weeks



Air Force Research Laboratory
Information Directorate
Rome, New York

29 May 2013 – 9 August 2013

INFORMATION ASSURANCE INTERNSHIP

The Information Directorate seeks outstanding undergraduate students for a paid research internship. The summer 2013 internship focuses on the science of mission assurance in a cloud computing environment, with emphasis on assuring Air Force mission essential functions in a contested environment. We invite applications from juniors and seniors in mathematics, computer engineering, electrical engineering, physics and computer science.

- Focus on mission assurance in a cloud computing environment
- Same team in CES and IA Internship
- CES material foundation for internship
- No grades in summer enables freedom to experiment to generate new CES material

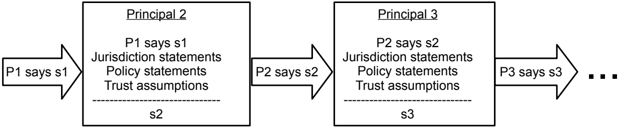
4. Examples

Concepts of Operation in the Access-Control Logic

JP 5-0, Joint Operation Planning

"The CONOPS clearly and concisely expresses what [is to be] accomplish[ed] and how it will be done using available resources. It describes how the actions of . . . components and supporting organizations will be integrated, synchronized, and phased to accomplish the mission . . ."

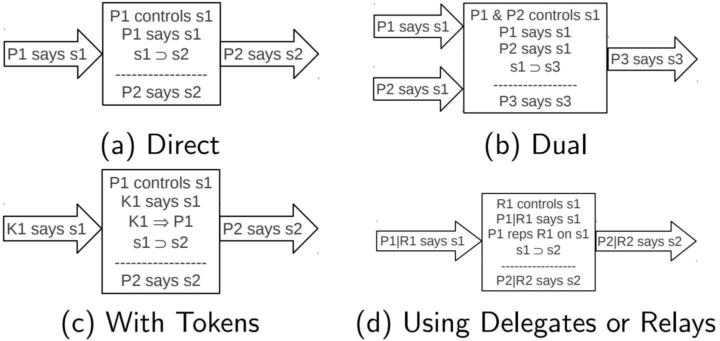
Flow of Control in CONOPS



Each CONOPS step has a corresponding inference rule

Types of Command and Control

Common Patterns



P1 says s1

P1 controls s1
P1 says s1
$s1 \supset s2$

P2 says s2

P2 says s2

(a) Direct

P1 says s1

P2 says s1

P1 & P2 controls s1
P1 says s1
P2 says s1
$s1 \supset s3$

P3 says s3

P3 says s3

(b) Dual

K1 says s1

P1 controls s1
K1 says s1
$K1 \Rightarrow P1$
$s1 \supset s2$

P2 says s2

P2 says s2

(c) With Tokens

P1|R1 says s1

R1 controls s1
P1|R1 says s1
P1 reps R1 on s1
$s1 \supset s2$

P2|R2 says s2

P2|R2 says s2

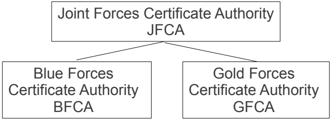
(d) Using Delegates or Relays

Significance

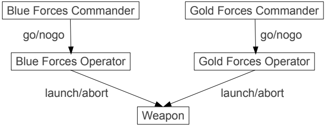
Analysis of C2 Patterns for Insight and Assurance

Example: Dual Control of a Weapon by Coalition Forces

Flow of Control



(a) Certificate Authority Hierarchy



(b) Flow of Command and Control

Informal description: top level roles only

- Blue and Gold Forces Commanders have authority on go/nogo mission commands
- Blue and Gold Forces Operators have authority on launch/abort weapon commands
- Weapon requires both Blue and Gold Forces Operators to order launch
- Any operator can abort

All Verified in HOL

Top-Level Weapons Launch Theorem in HOL

```
⊢ (M,Oi,Os) sat
  Name BFO meet Name GFO controls prop (WC launch) ⇒
  (M,Oi,Os) sat Name BFO says prop (WC launch) ⇒
  (M,Oi,Os) sat Name GFO says prop (WC launch) ⇒
  (M,Oi,Os) sat prop (WC launch)
```

Significance

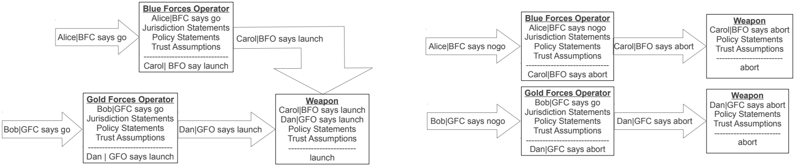
Theorems correspond to verified checklists showing how actions taken depend on orders given, policies, and trust infrastructure

Refinement: CONOPS Refined to Include Personnel

Role Assignments and Authorizations

Role	Person	Authenticated By	Formal Description of Delegation of Authority
BFC	Alice	pre-distributed prior to mission	*Alice* reps *BFC* on φ *Alice* reps *BFC* on (*Carol* reps *BFO* on φ)
GFC	Bob	pre-distributed prior to mission	*Bob* reps *GFC* on φ *Bob* reps *GFC* on (*Dan* reps *GFO* on φ)
BFO	Carol	Alice as BFC	*Carol* reps *BFO* on φ
GFO	Dan	Bob as GFC	*Dan* reps *GFO* on φ

Launch and Abort CONOPS with Assigned Personnel



Alice|BFC says go

Blue Forces Operator
Alice|BFC says go
Jurisdiction Statements
Policy Statements
Trust Assumptions
Carol| BFO say launch

Carol|BFO says launch

Bob|GFC says go

Gold Forces Operator
Bob|GFC says go
Jurisdiction Statements
Policy Statements
Trust Assumptions
Dan | GFO says launch

Dan|GFO says launch

Weapon
Carol|BFO says launch
Dan|GFO says launch
Policy Statements
Trust Assumptions
launch

Alice|BFC says nogo

Blue Forces Operator
Alice|BFC says nogo
Jurisdiction Statements
Policy Statements
Trust Assumptions
Carol|BFO says abort

Carol|BFO says abort

Weapon
Carol|BFO says abort
Policy Statements
Trust Assumptions
abort

Bob|GFC says nogo

Gold Forces Operator
Bob|GFC says go
Jurisdiction Statements
Policy Statements
Trust Assumptions
Dan|GFC says abort

Dan|GFC says abort

Weapon
Dan|GFC says abort
Policy Statements
Trust Assumptions
abort

(a) Launch CONOPS

(b) Abort CONOPS

Sample HOL Theorem/Verified Checklist

Refinement: Weapons Launch Linked to Personnel

```
⊢ (M,Oi,Os) sat
  Name (Role BFO) meet Name (Role GFO) controls
  prop (WC launch) ⇒
  (M,Oi,Os) sat
  Name (Staff Carol) quoting Name (Role BFO) says
  prop (WC launch) ⇒
  (M,Oi,Os) sat
  Name (Staff Dan) quoting Name (Role GFO) says
  prop (WC launch) ⇒
  (M,Oi,Os) sat
  reps (Name (Staff Carol)) (Name (Role BFO))
    (prop (WC launch)) ⇒
  (M,Oi,Os) sat
  reps (Name (Staff Dan)) (Name (Role GFO))
    (prop (WC launch)) ⇒
  (M,Oi,Os) sat prop (WC launch)
```

Next Refinement: CONOPS with Cryptographic Keys

Key and Role Certificates

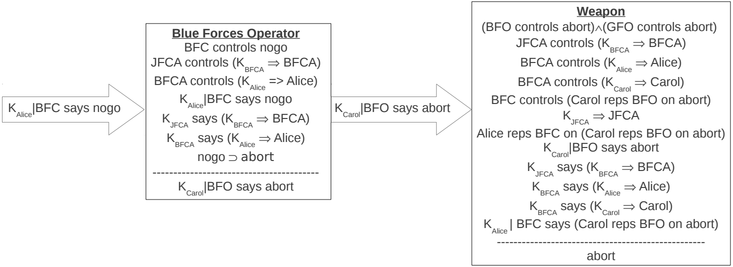
Key Certificate	
Issuer	Certificate Authority
Principal Name	P
Cryptographic Key	K_P
Digital signature	K_{CA} says ($K_P \Rightarrow P$)

(a) Key Certificate

Role Certificate	
Issuer	Role Authority
Principal Name	P
Role	$Role$
Jurisdiction	$\varphi_1 \cdots \varphi_n$
Digital signature	K_{RA} says (P reps $Role$ on φ_i)

(b) Role Certificate

Weapons Abort from BFO with Keys and Authorizations



K_{Alice}|BFC says nogo

Blue Forces Operator

BFC controls nogo
JFCA controls ($K_{BFCA} \Rightarrow$ BFCA)
BFCA controls (K_{Alice} => Alice)
K_{Alice}|BFC says nogo
K_{JFCA} says ($K_{BFCA} \Rightarrow$ BFCA)
K_{BFCA} says ($K_{Alice} \Rightarrow$ Alice)
nogo ⊃ abort

K_{Carol}|BFO says abort

K_{Carol}|BFO says abort

Weapon

(BFO controls abort)∧(GFO controls abort)
JFCA controls ($K_{BFCA} \Rightarrow$ BFCA)
BFCA controls ($K_{Alice} \Rightarrow$ Alice)
BFCA controls ($K_{Carol} \Rightarrow$ Carol)
BFC controls (Carol reps BFO on abort)
$K_{JFCA} \Rightarrow$ JFCA
Alice reps BFC on (Carol reps BFO on abort)
K_{Carol}|BFO says abort
K_{JFCA} says ($K_{BFCA} \Rightarrow$ BFCA)
K_{BFCA} says ($K_{Alice} \Rightarrow$ Alice)
K_{BFCA} says ($K_{Carol} \Rightarrow$ Carol)
K_{Alice} | BFC says (Carol reps BFO on abort)

---

abort

Verified HOL Theorem/Checklist for Abort

Orders, authorizations, trust infrastructure fully accounted for

$$\begin{array}{l}
\vdash (M,Oi,Os)\ \texttt{sat}\ R_2\ \texttt{controls}\ s\ \texttt{andf}\ R_3\ \texttt{controls}\ s \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ CA_1\ \texttt{controls}\ Kca_2\ \texttt{speaks\_for}\ CA_2 \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ CA_2\ \texttt{controls}\ Kp_1\ \texttt{speaks\_for}\ P_1 \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ CA_2\ \texttt{controls}\ Kp_2\ \texttt{speaks\_for}\ P_2 \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ R_1\ \texttt{controls}\ \texttt{reps}\ P_2\ R_2\ s \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ Kca_1\ \texttt{speaks\_for}\ CA_1 \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ \texttt{reps}\ P_1\ R_1\ (\texttt{reps}\ P_2\ R_2\ s) \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ Kp_2\ \texttt{quoting}\ R_2\ \texttt{says}\ s \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ Kca_1\ \texttt{says}\ Kca_2\ \texttt{speaks\_for}\ CA_2 \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ Kca_2\ \texttt{says}\ Kp_1\ \texttt{speaks\_for}\ P_1 \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ Kca_2\ \texttt{says}\ Kp_2\ \texttt{speaks\_for}\ P_2 \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ Kp_1\ \texttt{quoting}\ R_1\ \texttt{says}\ \texttt{reps}\ P_2\ R_2\ s \Rightarrow \\
\quad (M,Oi,Os)\ \texttt{sat}\ s
\end{array}$$

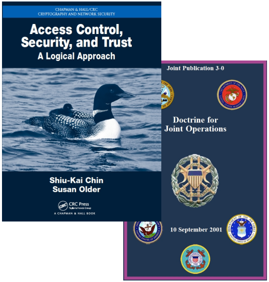
5. Why we are hopeful

10 Years of Teamwork, Research, and Experimentation

277+ graduates from 50+ universities

ACE Class of 2006

- AFRL & SU Education Partnership Agreement
- 2003–2010: **226+ ACE graduates from 40+ universities**
- 2011–2012: **IA Internship: 13+25 students**
- 2011–2012: **Cyber Engineering Semester: 6 + 7 students**



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

6. Concluding remarks

Concluding Remarks

Approach Works in Other Domains

- Credentials management for high-value commercial transactions, with JP Morgan Chase
- Distributed control of electric vehicles as power *sources* (V2G) on smart grids

Related Work in HOL (connecting more dots)

- Compose access-control logic (ACL) with structural operational semantics (SOS) to account for operational policy changes at the instruction-set architecture level—*prototype demonstrated*
- Embed modal mu logic (Stirling) to augment ACL and SOS to reason about modal and temporal properties—*HOL theories complete*

Educational Outcomes for Formal Verification are Repeatable

- Feasible to teach security and theorem proving to undergraduates
- Students can complete virtuous cycle of specification, design, and verification

Formal Methods and Tools for Security

Access-Control Logic in HOL available in HOL distribution