Theorem Proving for Certified Mission Assurance

Shiu-Kai Chin Professor, Dept. of Electrical Engineering & Computer Science Syracuse University, Syracuse, New York Senior Scientist, Serco-NA, Rome, New York

Acknowledgements

This is joint work with:

- Susan Older, Ph.D., Syracuse University
- Sarah Muccio, Ph.D., Air Force Research Laboratory
- Thomas (TJ) Vestal, Air Force Research Laboratory
- Fred Wieners, Col. USAF (ret), Serco-NA
- Lockwood Morris, Ph.D., Syracuse University

Why Mission Assurance Matters

Major General Richard Webber, Commander, 24th Air Force

 "Mission assurance is the number one goal in current cyber operations, versus the old paradigm of information assurance."

Definitions

- Mission Assurance: assuring that critical system capabilities necessary to complete a mission successfully are available, correctly implemented, and secure
- Information Assurance: measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation

Eugene Spafford

• "There are limits to how much you can fireproof a cardboard box."

Why Certified & Verified Mission Assurance Matters

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

- "Modifying the cyberspace domain to eliminate vulnerabilities or make them inaccessible to an adversary through sound hardware and software development practices can eliminate beforehand vulnerabilities by designing them out of a system."
- "I want theorems!"

Need: A science & engineering for mission assurance

Purpose & Preview

Purpose

- Describe some of our efforts to develop and apply mathematical logic for mission assurance
- Show that the logic, proofs, and methods are well within the capabilities of practicing engineers

Preview

- Introduction: intended audience, focus, & viewpoint
- Overview of the logic
- Representation of CONOPS & an example
- Conclusions

Introduction

Intended audience

• Designers, builders, specifiers, buyers, and evaluators of secure and trustworthy computer and information systems

Focus: access policies and concepts of operation

- Hardware, virtual machines, networks
- Credentials, authority, delegation
- Confidentiality & integrity policies

Logic is a means to an end

- Means of description
- Inference rules
- Theorem-based design & verification (proofs)

イロト イヨト イヨト イヨト

Our Viewpoint



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

A Logical Approach to Access Control

Access-control logic as a tool

- Modification of multi-agent propositional modal logic created by Abadi, Burrows, Lampson, and Plotkin
- Implemented as a conservative extension to the Cambridge Higher Order Logic (HOL-4) Kananaskis 7 theorem prover (joint work with Lockwood Morris)
- Routinely taught to SU graduate students in *Principles of Distributed Access Control* course
- Used since 2003 by over 226 ROTC cadets from over 40 universities as part of Air Force Research Lab's *Advanced Course in Engineering for Cybersecurity Bootcamp*

Methods usable by practicing engineers and provide assurance

Our focus: Concept of Operations (CONOPS)

CONOPS definition

"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 ..."

JP 5-0, Joint Operation Planning

Why focus on CONOPS?

- Reveals the thinking of commanders in terms of mission requirements, critical capabilities, policies, jurisdiction, and trust assumptions
- Mission assurance requires commanders and implementers precisely and accurately agree on the CONOPS

Syntax

BNF

- Principals (actors) P ::= A / P&Q / P | Q
- Statements they $\varphi ::= P / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 /$ make $P \Rightarrow Q / P$ says φ / P controls φ / P reps Q on φ

Kripke structures

		<i>Е_М</i> [[р]]		
	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \vee \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
		$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q \rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
		$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
		$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
		$\mathcal{E}_{\mathcal{M}}$ [P reps Q on φ]		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \rrbracket$
			•	

Syntax

BNF

- Principals (actors) P ::= A / P&Q
- Statements they make

- = A / P & Q / P | Q $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 /$
 - $P \Rightarrow Q / P$ says φ / P controls φ / P reps Q on φ

Kripke structures

		€ _M [[p]]		
	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \lor \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q \rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
		$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
		$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
		$\mathcal{E}_{\mathcal{M}}$ [P reps Q on φ]		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi brace$
			۲	

Syntax

BNF

- Principals (actors)
- ::= A / P & Q / P |
- Statements they make

 $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 /$ $P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

		€ _М [[p]]		
	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W = \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
	PName $\rightarrow \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \lor \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
		$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q \rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
		$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w) \subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
		$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
		$\mathcal{E}_{\mathcal{M}}$ [P reps Q on φ]		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \rrbracket$
			•	

Syntax

BNF

- Principals (actors) P ::= A / P & Q / P | Q
- Statements they make

 $\begin{array}{l} p \ / \ \neg \varphi \ / \ \varphi_1 \land \varphi_2 \ / \ \varphi_1 \lor \varphi_2 \ / \ \varphi_1 \supset \varphi_2 \ / \ \varphi_1 \equiv \varphi_2 \ / \\ P \Rightarrow Q \ / \ P \text{ says } \varphi \ / \ P \text{ controls } \varphi \ / \ P \text{ reps } Q \text{ on } \varphi \end{array}$

Kripke structures

		$\mathcal{E}_{\mathcal{M}}\llbracket p rbracket$		
	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}} \llbracket \varphi_1 \wedge \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \vee \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
		$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q\rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
		$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
		$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
		$\mathcal{E}_{\mathcal{M}}$ [P reps Q on φ]		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \rrbracket$
			•	

Syntax

BNF

- Principals (actors) P ::=
- Statements they make

- = A / P & Q / P | Q $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 =$
 - $P \Rightarrow Q / P$ says φ / P controls φ / P reps Q on φ

Kripke structures

		$\mathcal{E}_{\mathcal{M}}\llbracket p rbracket$		
	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}} \llbracket \varphi_1 \wedge \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \vee \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q\rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
		$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
		$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
		$\mathcal{E}_{\mathcal{M}}[P \text{ reps } Q \text{ on } \varphi]$		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \rrbracket$
			•	

SyntaxBNF• Principals (actors)P ::= A / P & Q / P | Q• Statements they
make $\varphi ::= P / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supseteq \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

		$\mathcal{E}_{\mathcal{M}}\llbracket p rbracket$		
	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W = \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}} \llbracket \varphi_1 \wedge \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \lor \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q \rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
		$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
		$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}[(P \text{ says } \varphi) \supset \varphi]$
		$\mathcal{E}_{\mathcal{M}}[P \text{ reps } Q \text{ on } \varphi]$		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \rrbracket$
			4	□ ▶ < 클 ▶ < 클 ▶ < 클 ▶ 클 → 의 < @ 10 / 18



Krip	tructures	Semantics	
		$\mathcal{E}_{\mathcal{M}}\llbracket p rbracket$	
	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$	$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 \rrbracket$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 rbrace$
		$\mathcal{E}_{\mathcal{M}} \llbracket \varphi_1 \lor \varphi_2 \rrbracket$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$	$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
		$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q\rrbracket$	$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
		$\mathcal{E}_{\mathcal{M}}$ [P says φ]	$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
		$\mathcal{E}_{\mathcal{M}}$ [P controls φ]	$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
		$\mathcal{E}_{\mathcal{M}}$ [P reps Q on φ]	$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \rrbracket$
			□ ▶ < @ ▶ < 글 ▶ < 글 ▶ 글 ∽ ♀

Syntax

BNF

- Principals (actors) P ::= A / P&
- Statements they make

 $= A / P \otimes Q / P | Q$ $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ savs } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

		$\mathcal{E}_{\mathcal{M}}\llbracket p \rrbracket$		
	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W = \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 rbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \lor \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 brace$
		$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q \rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
		$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
		$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}[(P \text{ says } \varphi) \supset \varphi]$
		$\mathcal{E}_{\mathcal{M}}[P \text{ reps } Q \text{ on } \varphi]$		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \rrbracket$
			4	□ ▶ < 클 ▶ < 클 ▶ < 클 ▶ 클 → 의 < @ 10 / 18

Syntax

BNF

- Principals (actors) P ::= A / P & C
- Statements they make

 $= A / F \otimes Q / F | Q$ $= P / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

W	=	non-empty {worlds}
		$PropVar \to \mathcal{P}(W)$
		$PName \to \mathcal{P}(W \times W)$

€ _M [[p]]		
$\mathcal{E}_{\mathcal{M}}\llbracket \neg \varphi \rrbracket$		$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi rbracket$
$\left[\varphi_1 \wedge \varphi_2 \right]$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 rbracket \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 rbracket$
${}_{t}\llbracket \varphi_{1} \vee \varphi_{2}\rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket\varphi_1\rrbracket \cup \mathcal{E}_{\mathcal{M}}\llbracket\varphi_2\rrbracket$
$\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
$\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
$\mathcal{M}\llbracket P \Rightarrow Q\rrbracket$		$egin{cases} W, & ext{if } J(Q) \subseteq J(P) \ \emptyset, & ext{otherwise} \end{cases}$
P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
ntrols φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
$[Q \text{ on } \varphi]$		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi brace$
	4	

Syntax

BNF

- Principals (actors) P ::= A / P & C
- Statements they make

 $= A / P \otimes Q / P | Q$ $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

W	=	non-empty {worlds}	E _ [[p]]		
1	=	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W = \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
		$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 rbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 rbracket \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 rbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \lor \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 rbrace \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 rbrace$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 rbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
			$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q\rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
			$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
			$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
			$\mathcal{E}_{\mathcal{M}}$ [P reps Q on φ]		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q$ says $\varphi \supset Q$ says $\varphi brace$
				4	

Syntax

BNF

- Principals (actors) P ::= A / P&Q
- Statements they make

 $= A / P \otimes Q / P | Q$ $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ savs } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

W	=	non-empty {worlds}	$\mathcal{E}_{\mathcal{M}}\llbracket p rbracket$		
I	=	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi rbracket$
J	=	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 rbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 rbracket \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 rbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \vee \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
			$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q \rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
			$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
			$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
			$\mathcal{E}_{\mathcal{M}}[P \text{ reps } Q \text{ on } \varphi]$		${\mathcal E}_{\mathcal M}\llbracket P {\mathcal Q} {\sf says} arphi \supset {\mathcal Q} {\sf says} arphi rbracket$
				•	□ ▶ < ⓓ ▶ < 볼 ▶ < 볼 ▶ 월 - ⑦ Q (0 10/18

Syntax

BNF

- Principals (actors) P ::= A / P&Q /
- Statements they make

 $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 /$ $P \Rightarrow 0 / P \text{ savs } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

W	=	non-empty {worlds}	<i>Е</i> _М [[p]]		
1	=	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
J	=	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
\mathcal{M}	=	$\langle W, I, J \rangle$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \vee \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
			$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q \rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
			$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
			$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
			$\mathcal{E}_{\mathcal{M}}[P \text{ reps } Q \text{ on } \varphi]$		${\mathcal E}_{\mathcal M}\llbracket P \mid Q$ says $arphi \supset Q$ says $arphi rbracket$
				۲	□ ▶ 《圖 ▶ 《 볼 ▶ 《 볼 ▶ 《 볼 · ⑦ 역 10 / 1

Syntax

BNF

- Principals (actors) P ::= A / P&Q
- Statements they make

 $= A / P \otimes Q / P | Q$ = $P / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

			$\mathcal{E}_{\mathcal{M}}\llbracket p \rrbracket$	=	<i>I</i> (<i>p</i>)
		$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
		$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 rbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 brace$
\mathcal{M}	=	$\langle W, I, J \rangle$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \lor \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 brace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 brace$
			$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q\rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
			$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
			$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi\rrbracket$
			$\mathcal{E}_{\mathcal{M}}[P \text{ reps } Q \text{ on } \varphi]$		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi brace$
				۲	□ ▶ < @ ▶ < 볼 ▶ < 볼 ▶ ≧ ∽ Q (0 10/18

Syntax

 \mathcal{M}

BNF

- Principals (actors) P ::= A / P & G
- Statements they make

 $= A / F \otimes Q / F | Q$ $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

		E _ [[p]]		
	$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg\varphi]\!]$	=	$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi rbracket$
	$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 rbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 rbracket \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 rbracket$
=	$\langle W, I, J \rangle$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \lor \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 rbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
		$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q\rrbracket$		$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
		$\mathcal{E}_{\mathcal{M}}$ [P says φ]		$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
		$\mathcal{E}_{\mathcal{M}}$ [P controls φ]		$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
		$\mathcal{E}_{\mathcal{M}}[P \text{ reps } Q \text{ on } \varphi]$		$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi brace$

Syntax

BNF

- Principals (actors) P ::= A / P
- Statements they make

= A / P & Q / P | Q $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

Semantics

- W = non-empty {worlds}
- $I = \operatorname{PropVar} \rightarrow \mathcal{P}(W)$
- $J = \mathsf{PName} \to \mathcal{P}(W \times W)$
- $\mathcal{M} = \langle W, I, J \rangle$

$$\begin{split} \mathcal{E}_{\mathcal{M}}[\rho] &= I(\rho) \\ \mathcal{E}_{\mathcal{M}}[\neg\varphi] &= W - \mathcal{E}_{\mathcal{M}}[\varphi] \\ \mathcal{E}_{\mathcal{M}}[\varphi_{1} \land \varphi_{2}] &= \mathcal{E}_{\mathcal{M}}[\varphi_{1}] \cap \mathcal{E}_{\mathcal{M}}[\varphi_{2}] \\ \mathcal{E}_{\mathcal{M}}[\varphi_{1} \lor \varphi_{2}] &= \mathcal{E}_{\mathcal{M}}[\varphi_{1}] \cup \mathcal{E}_{\mathcal{M}}[\varphi_{2}] \\ \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} \supseteq \varphi_{2}] &= \mathcal{E}_{\mathcal{M}}[\varphi_{1} \supset \varphi_{2}] \cap \mathcal{E}_{\mathcal{M}}[\varphi_{2} \supset \varphi_{1}] \\ \mathcal{E}_{\mathcal{M}}[P \Rightarrow Q] &= \begin{cases} W, \text{ if } J(Q) \subseteq J(P) \\ \emptyset, \text{ otherwise} \end{cases} \\ \mathcal{M}[P \text{ says } \varphi] &= \{w|J(P)(w) \subseteq \mathcal{E}_{\mathcal{M}}[\varphi]\} \\ \text{ controls } \varphi] &= \mathcal{E}_{\mathcal{M}}[P \text{ says } \varphi \supset \varphi] \\ \mathbb{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi] \\ \mathcal{E}_{\mathcal{M}}[P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \cap Q \text{ says } \varphi \supset Q \text{ says } \varphi \supset Q \text{ says } \varphi \cap Q \text{ says$$

Syntax

BNF

- Principals (actors) P ::= A / P &
- Statements they make

= A / P & Q / P | Q $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

- - 10/18

Syntax

BNF

- Principals (actors) P ::= A / P &
- Statements they make

= A / P & Q / P | Q $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

- - 10/18

Syntax

BNF

- Principals (actors) P ::= A / P &
- Statements they make

= A / P & Q / P | Q $= p / \neg \varphi / \varphi_1 \land \varphi_2 / \varphi_1 \lor \varphi_2 / \varphi_1 \supset \varphi_2 / \varphi_1 \equiv \varphi_2 / P \Rightarrow Q / P \text{ says } \varphi / P \text{ controls } \varphi / P \text{ reps } Q \text{ on } \varphi$

Kripke structures

Semantics

			$\mathcal{E}_{\mathcal{M}}\llbracket p rbracket$		
		$PropVar \to \mathcal{P}(W)$	$\mathcal{E}_{\mathcal{M}}[\![\neg \varphi]\!]$		$W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi \rrbracket$
		$PName \to \mathcal{P}(W \times W)$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \wedge \varphi_2 rbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 rbrace$
\mathcal{M}	=	$\langle W, I, J \rangle$	$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \vee \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 \rrbracket$		$(W - \mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \rrbracket) \cup \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \rrbracket$
			$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \equiv \varphi_2 \rrbracket$		$\mathcal{E}_{\mathcal{M}}\llbracket \varphi_1 \supset \varphi_2 rbrace \cap \mathcal{E}_{\mathcal{M}}\llbracket \varphi_2 \supset \varphi_1 rbrace$
			$\mathcal{E}_{\mathcal{M}}\llbracket P \Rightarrow Q\rrbracket$	=	$\begin{cases} W, & \text{if } J(Q) \subseteq J(P) \\ \emptyset, & \text{otherwise} \end{cases}$
			$\mathcal{E}_{\mathcal{M}}$ [P says φ]	=	$\{w J(P)(w)\subseteq \mathcal{E}_{\mathcal{M}}\llbracket\varphi\rrbracket\}$
			$\mathcal{E}_{\mathcal{M}}$ [P controls φ]	=	$\mathcal{E}_{\mathcal{M}}\llbracket(P \text{ says } \varphi) \supset \varphi rbrace$
			$\mathcal{E}_{\mathcal{M}}$ [P reps Q on φ]	=	$\mathcal{E}_{\mathcal{M}}\llbracket P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \rrbracket$
					ロン (日) (日) (日) (日) (日) (日)

Core inference rules

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

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

> If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

	$Q \supset (P \text{ say})$	$\forall S \ arphi \supset Q \ S$	
Quoting $P \mid Q$		says Q s	
& Says P & Q S			
		$ \begin{array}{c} \overline{P \Rightarrow P} \\ P Q' \Rightarrow \\ Q' \Rightarrow P \mid Q \end{array} $	$\frac{Q}{Q}$
P controls			
P reps Q on g	o def ₽ @ 🗗	₩54 æ∋ Q	SELVS ⊘≣ 、

Core inference rules

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

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

> If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

	$\supset \varphi')) \supset (P :$		
	$Q \supset (P \text{ says})$	$\varphi \supset Q$ S	
Quoting $P \mid Q$	says $\varphi \equiv P$ s	says Q s	
& Says P & Q Sa		ys φΛG	
	$y \text{ of } \frac{P' \Rightarrow P'}{P' \mid Q}$	$P Q' \Rightarrow \\ Q' \Rightarrow P \mid Q \mid$	$\frac{Q}{2}$
	y of $ = \frac{P (Q Q)}{(P Q)}$		
P controls			
P reps Q on g	o def Del @ Bay	/5∙ເ≣∋ (3	Senter State

Core inference rules

Rules

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

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

> If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

	$Q \supset (P \text{ says})$	$\varphi \supset Q$ S		
Quoting $P \mid Q$		says Q s		
& Says P & Q Sa				
		$\begin{array}{ccc} P & Q' \Rightarrow \\ P' \Rightarrow P \mid Q \end{array}$	<u>Q</u> 2	
	y of $ = \frac{P (Q }{(P Q)}$			
P controls				
P reps Q on Q	o def PI O BAV	′S• æ⊃ G	seavs ⊘≣	¢

Core inference rules

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

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

> If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

Speaks For $P \Rightarrow Q \supset (P \text{ says } \varphi \supset Q \text{ says } \varphi)$
Quoting $P \mid Q$ says $\varphi \equiv P$ says Q says φ
& Says $P \& Q$ says $\varphi \equiv P$ says $\varphi \land Q$ says φ
Monotonicity of $ $ $P' \Rightarrow P Q' \Rightarrow Q$ $P' Q' \Rightarrow P Q$
Associativity of $ \frac{P (Q R) \text{ says } \varphi}{(P Q) R \text{ says } \varphi}$
$P \ controls \ \varphi \ \stackrel{\mathrm{def}}{=} \ (P \ says \ \varphi) \supset \varphi$
Preps Q on a def planavs(Em Q Savs a so

Core inference rules

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

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

> If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

	$\Rightarrow Q \supset (P \text{ say})$	/S φ ⊃ Q S	
Quoting P 0	$\varphi \equiv P$	says Q s	
& Says P & Q		says $\varphi \wedge Q$	
		$ \begin{array}{c} \hline P \Rightarrow P \\ P & Q' \Rightarrow \end{array} \\ \hline Q' \Rightarrow P & Q' \Rightarrow \end{array} $	Q
		Q R) says Q) R says	
P control			
P reps Q on	φ def P @ 3	avs∙æ∋ Q	SBIVS ⊘≣ ✓

CORE INFERENCE RULES

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

 $\frac{H_1 \cdots H_n}{C} \text{ is sound if } for \\ all Kripke structures <math>\mathcal{M}$ and each $i \in \{1, \dots, n\}$:

> If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

	$Q \supset (P \text{ says})$	$\varphi \supset Q$ S	
Quoting P Q S		says q sa	
& Says P & Q Say		iys $\varphi \wedge Q$	
		$\begin{array}{c} P Q' \Rightarrow P \\ Q' \Rightarrow P \mid Q \end{array}$	Q
	of $ \frac{P (Q)}{(P Q)}$		
P controls			
P reps Q on φ	def P @ 50	/S¶∉⊇ Q	SEIVS φ≣ ∖

CORE INFERENCE RULES

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

 $\frac{H_1 \cdots H_n}{C} \text{ is sound if } for \\ all Kripke structures <math>\mathcal{M}$ and each $i \in \{1, \dots, n\}$:

If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

	$P \Rightarrow Q \supset (P \text{ say})$	$(S \varphi \supset Q S)$	
Quoting – P	$\varphi \mid Q$ says $\varphi \equiv F$	says q s	
	Q says $\varphi \equiv P$ s	says $\varphi \wedge Q$	
		$P \Rightarrow P \\ P Q' \Rightarrow \\ Q' \Rightarrow P \mid Q$	
		Q R) says Q) R says	
P conti			
P reps Q C	on 🦁 🏜 🗛 🛛 🖉	avs∙æ∋ Q	⊊avs ⊘≣ ৺

CORE INFERENCE RULES

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

 $\frac{H_1 \cdots H_n}{C} \text{ is sound if } for \\ all Kripke structures <math>\mathcal{M}$ and each $i \in \{1, \dots, n\}$:

If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

		$\rho \supset Q$ S	
Quoting P Q Sa		ays q s	
& Says P & Q SAY		$S \ \varphi \land Q$	
	ency of $\Rightarrow {P}$ of $ \frac{P' \Rightarrow P}{P' Q'}$	$\overrightarrow{P} = \begin{array}{c} P \\ Q' \Rightarrow \\ \Rightarrow P \mid Q \end{array}$	$\frac{Q}{Q}$
	of $\left \frac{P \left \left(Q \right R}{\left(P \right Q \right) \right $		
P controls φ			
<i>P</i> reps <i>Q</i> on φ	lef ⊫⊡ p• @ ∰avs	<	SEIVS ⊘≣ ✓

CORE INFERENCE RULES

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

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

> If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

	$Q \supset (P \text{ says } \varphi \supset G)$	
Quoting P Q	says $\varphi \equiv P$ says G	
& Says P & Q Sa		Q says φ
	otency of \Rightarrow $\overrightarrow{P \Rightarrow P}$ \downarrow of $ $ $\overrightarrow{P' \Rightarrow P Q'}$ $\overrightarrow{P' \mid Q' \Rightarrow P}$	$\Rightarrow Q$
	$r of \mid \frac{P \mid (Q \mid R) \text{ say}}{(P \mid Q) \mid R \text{ say}}$	Υ S φ ΥS φ
P controls		
P reps Q on q	def_₽ @∄ ₽\\$(建⊃	Q 5995 07 4

Core inference rules

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

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

> If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

	$P Q \supset (P \text{ says})$	$\varphi \supset Q$ S		
Quoting $P \mid Q$		says Q s		
& Says P & Q S		ays $\varphi \wedge \zeta$		
		$ \frac{P \Rightarrow P}{P Q' \Rightarrow} $ $ \frac{Q' \Rightarrow P \mid Q}{Q' \Rightarrow P \mid Q} $	Q 2	
	ty of $\left \frac{P \left \left(Q \right) \right }{\left(P \left Q \right) \right }$			
P controls	$\varphi \stackrel{\mathrm{def}}{=} (P$			
P reps Q on a	φ def ₽ @ ∰ ∂	VS•∉∋ Q	seanys φ≣	4

Core inference rules

RULES

- Inconvenient to use Kripke semantics
- Use inference rules $\frac{H_1 \cdots H_n}{C}$ instead

Soundness

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

> If all $\mathcal{E}_{\mathcal{M}}\llbracket H_i \rrbracket = W$ then $\mathcal{E}_{\mathcal{M}}\llbracket C \rrbracket = W$

- All rules are sound
- All verified in HOL-4 K-7 theorem prover

$\begin{array}{cc} \text{ Taut } & \underset{\varphi}{ & } & \text{ if } \varphi \text{ is an instance of a prop-logic tau-} \\ & \text{ tology } \end{array}$
$\begin{array}{ccc} \textit{Modus Ponens} & \frac{\varphi & \varphi \supset \varphi'}{\varphi'} & & \textit{Says} & \frac{\varphi}{\textit{P says } \varphi} \end{array}$
$\frac{MP \text{ Says }}{(P \text{ says } (\varphi \supset \varphi')) \supset (P \text{ says } \varphi \supset P \text{ says } \varphi')}$
Speaks For $\overline{P \Rightarrow Q \supset (P \text{ says } \varphi \supset Q \text{ says } \varphi)}$
$Quoting \overline{P \mid Q \text{ says } \varphi \equiv P \text{ says } Q \text{ says } \varphi}$
$\& Says \hline P \& Q \text{ says } \varphi \equiv P \text{ says } \varphi \land Q \text{ says } \varphi$
Idempotency of $\Rightarrow {P \rightarrow P}$
Monotonicity of $ \frac{P' \Rightarrow P Q' \Rightarrow Q}{P' \mid Q' \Rightarrow P \mid Q}$
Associativity of $ \frac{P (Q R) \text{ says } \varphi}{(P Q) R \text{ says } \varphi}$
$P \text{ controls } \varphi \stackrel{\text{def}}{=} (P \text{ says } \varphi) \supset \varphi$
P reps Q on $\varphi \stackrel{\mathrm{def}}{=} P Q $ says $\varphi \supset Q$ says $\varphi \ge -$

Examples

A simple proof

- 1. $P \text{ controls } \varphi$ Ass2. $P \text{ says } \varphi$ Ass3. $P \text{ says } \varphi \supset \varphi$ 1 de4. φ 2, 3
 - Assumption Assumption 1 def'n controls 2, 3 Modus Ponens

Derived inference rule

$$\frac{P \text{ controls } \varphi \quad P \text{ says } \varphi}{\varphi}$$

All derived rules are sound

In HOL

Controls Proof

```
- val a1 = ACL ASSUM ``(P:'c Princ) controls (f:('a,'c,'d,'e)Form)``:
> val al = [.] |- (M.Oi.Os) sat P controls f : thm
- val a2 = ACL ASSUM ``(P:'c Princ) says (f:('a,'c,'d,'e)Form)``;
> val a2 = [.] |- (M,0i,0s) sat P says f : thm
- val th3 = REWRITE RULE (Controls Eq) a1:
> val th3 = [.] |- (M.0i.0s) sat P says f impf f : thm

    val th4 = ACL MP a2 th3;

> val th4 = [..] |- (M,01,0s) sat f : thm
. val th5 -
        (DISCH ALL th4):
> val th5 =
   I- VM 01 0s P f.
        (M.Oi.Os) sat P says f -
        (M.Oi.Os) sat P controls f →
        (M.Oi.Os) sat f : thm
```

Controls Inference Rule

```
1**
                      * CONTROLS
* CONTROLS : thm->thm -> thm
* SYNOPSTS
* Deduces formula f if the principal who says f also controls f.
* DESCRIPTION
    A1 |- (M,Oi,Os) sat P controls f A2 |- (M,Oi,Os) sat P says f
    CONTROLS
                     A1 u A2 I- (M.Oi.Os) sat f
* FATLURE
* Fails unless the theorems match in terms of principals and formulas
* in the access-control logic.
*****************
                                             *****)
fun CONTROLS th1 th2 = MATCH MP (MATCH MP (SPEC ALL Controls) th2) th1:
```

General Form of CONOPS

"The CONOPS ... describes how the actions of ... components and supporting organizations will be integrated, synchronized, and phased to accomplish the mission ..."



- Principals are actors
- Assumptions about jurisdiction, policy, and trust are explicit
- Each step in CONOPS is a derived inference rule



Joint Terminal Air Controller



-

Remotely Piloted Vehicle



Airborne Early Warning & Control





Joint Terminal Air Controller



Remotely Piloted Vehicle



Airborne Early Warning & Control



Air Operations Center

イロト 不得 とくまとう ほう

3





Remotely Piloted Vehicle



Airborne Early Warning & Control





Joint Terminal Air Controller



Remotely Piloted Vehicle



Airborne Early Warning & Control





Joint Terminal Air Controller



And the second s

Remotely Piloted Vehicle



Airborne Early Warning & Control





Statement	Formal Representation
request 1	(Token _{Alice} JTAC) SAYS <i>(strike, target)</i>
relay 1	(K _{JTAC-MVA} JTAC) SAYS (strike, target)
authenticated request 1	JTAC SAYS (strike, target)
request 2	(Token _{Bob} Controller) SAYS (JTAC SAYS (strike, target))
relay 2	(K _{Controller-MVA} Controller) SAYS (JTAC SAYS (strike, target))
authenticated request 2	Controller SAYS (JTAC SAYS <strike, target="">)</strike,>



Statement	Formal Representation
request 1	(Token _{Alice} JTAC) SAYS (strike, target)
relay 1	(K _{JTAC-MVA} JTAC) SAYS (strike, target)
authenticated request 1	JTAC SAYS (strike, target)
request 2	(Token _{Bob} Controller) SAYS (JTAC SAYS (strike, target))
relay 2	(K _{Controller-MVA} Controller) SAYS (JTAC SAYS (strike, target))
authenticated request 2	Controller SAYS (JTAC SAYS <strike, target="">)</strike,>



Statement	Formal Representation
request 1	(Token _{Alice} JTAC) SAYS (strike, target)
relay 1	(K _{JTAC-MVA} JTAC) SAYS (strike, target)
authenticated request 1	JTAC SAYS (strike, target)
request 2	(Token _{Bob} Controller) SAYS (JTAC SAYS (strike, target))
relay 2	(K _{Controller-MVA} Controller) SAYS (JTAC SAYS (strike, target))
authenticated request 2	Controller SAYS (JTAC SAYS <strike, target="">)</strike,>



Statement	Formal Representation
request 1	(Token _{Alice} JTAC) SAYS <i>(strike, target)</i>
relay 1	(K _{JTAC-MVA} JTAC) SAYS (strike, target)
authenticated request 1	JTAC SAYS (strike, target)
request 2	(Token _{Bob} Controller) SAYS (JTAC SAYS (strike, target))
relay 2	(K _{Controller-MVA} Controller) SAYS (JTAC SAYS (strike, target))
authenticated request 2	Controller SAYS (JTAC SAYS <strike, target="">)</strike,>



Statement	Formal Representation
request 1	(Token _{Alice} JTAC) SAYS <i>(strike, target)</i>
relay 1	(K _{JTAC-MVA} JTAC) SAYS (strike, target)
authenticated request 1	JTAC SAYS (strike, target)
request 2	(Token _{Bob} Controller) SAYS (JTAC SAYS (strike, target))
relay 2	(K _{Controller-MVA} Controller) SAYS (JTAC SAYS (strike, target))
authenticated request 2	Controller SAYS (JTAC SAYS (strike, target))



Statement	Formal Representation
request 1	(Token _{Alice} JTAC) SAYS <i>(strike, target)</i>
relay 1	(K _{JTAC-MVA} JTAC) SAYS (strike, target)
authenticated request 1	JTAC SAYS (strike, target)
request 2	(Token _{Bob} Controller) SAYS (JTAC SAYS (strike, target))
relay 2	(K _{Controller-MVA} Controller) SAYS (JTAC SAYS (strike, target))
authenticated request 2	Controller SAYS (JTAC SAYS (strike, target))



Statement	Formal Representation
request 1	(Token _{Alice} JTAC) SAYS (strike, target)
relay 1	(K _{JTAC-MVA} JTAC) SAYS (strike, target)
authenticated request 1	JTAC SAYS (strike, target)
request 2	(Token _{Bob} Controller) SAYS (JTAC SAYS (strike, target))
relay 2	(K _{Controller-MVA} Controller) SAYS (JTAC SAYS (strike, target))
authenticated request 2	Controller SAYS (JTAC SAYS (strike, target))

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

Transmitting MVA:

Receiving MVA

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

Input (Token or Key | Role) says φ

Transmitting MVA:

Receiving MVA

 $(K_{MVA_{1}} | Role) \text{ Says } \varphi$ $K_{Auth} \text{ Says } (MVA_{1} \text{ reps } Role \text{ On } \varphi)$ $K_{Auth} \text{ Says } (K_{MVA_{1}} \Rightarrow MVA_{1})$ Auth controls $(MVA_{1} \text{ reps } Role \text{ On } \varphi)$ $Auth \text{ controls } (K_{MVA_{1}} \Rightarrow MVA_{1})$ $K_{Auth} \Rightarrow Auth$ $Role \text{ Says } \varphi$ $(\Box \Rightarrow \langle \Box \Rightarrow \langle \Xi \Rightarrow \langle \Xi \Rightarrow \langle \Xi \Rightarrow \rangle \langle \Xi \rangle \rangle \langle C \rangle$ 17/18

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

nput (Token or Key | Role) says φ

Delegation Cert K_{Auth} says (*Person or Object* reps *Role* on φ)

Key Certificate K_{Auth} says (Token or Key \Rightarrow Person or Object)JurisdictionAuth controls (Person or Object reps Role on φ)JurisdictionAuth controls (Token or Key \Rightarrow Person or Object)Frust Assumption $K_{Auth} \Rightarrow Auth$

Transmitting MVA:

Receiving MVA

 $(K_{MVA_1} | Role) \operatorname{Says} \varphi$ $K_{Auth} \operatorname{Says} (MVA_1 \operatorname{reps} Role \ \operatorname{On} \varphi)$ $K_{Auth} \operatorname{Says} (K_{MVA_1} \Rightarrow MVA_1)$ Auth controls (MVA_1 reps Role \ \operatorname{On} \varphi) Auth controls (K_{MVA_1} \Rightarrow MVA_1) $K_{Auth} \Rightarrow Auth$ $Role \operatorname{Says} \varphi$ $(\Box \triangleright \langle \Box \rangle \land \langle \Xi \rangle \land \langle \Xi \rangle \land \langle \Xi \rangle \land \langle \Xi \rangle$ 17/18

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

nput (Token or Key | Role) says φ

Delegation Cert K_{Auth} says (*Person or Object* reps *Role* on φ)

Key Certificate K_{Auth} says (Token or Key \Rightarrow Person or Object)

JurisdictionAuth controls (Person or Object reps Role on φ)JurisdictionAuth controls (Token or Key \Rightarrow Person or Object)ust Assumption $K_{Auth} \Rightarrow Auth$

Transmitting MVA:

Receiving MVA

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

Input(Token or Key | Role) says φ Delegation Cert K_{Auth} says (Person or Object reps Role on φ)Key Certificate K_{Auth} says (Token or Key \Rightarrow Person or Object)JurisdictionAuth controls (Person or Object reps Role on φ)JurisdictionAuth controls (Token or Key \Rightarrow Person or Object)rust Assumption $K_{Auth} \Rightarrow Auth$

Transmitting MVA:

Receiving MVA

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

Input (Token or Key | Role) says φ Delegation Cert K_{Auth} says (Person or Object reps Role on φ) Key Certificate K_{Auth} says (Token or Key \Rightarrow Person or Object) Jurisdiction Auth controls (Person or Object reps Role on φ) Jurisdiction Auth controls (Token or Key \Rightarrow Person or Object) ust Assumption $K_{Auth} \Rightarrow Auth$

Transmitting MVA:

Receiving MVA

 $\begin{array}{c} (\textit{Token} \mid \textit{Role}) \; \texttt{Says} \; \varphi \\ K_{Auth} \; \texttt{Says} \; (\textit{Person reps Role ON } \varphi) \\ K_{Auth} \; \texttt{Says} \; (\textit{Token} \Rightarrow \textit{Person}) \\ Auth \; \texttt{Controls} \; (\textit{Person reps Role On } \varphi) \\ Auth \; \texttt{Controls} \; (\textit{Token} \Rightarrow \textit{Person}) \\ K_{Auth} \; \Rightarrow \textit{Auth} \\ \hline \\ MVA \; 1 \; \hline \\ \hline \\ K_{MVA_1} \mid \textit{Role Says} \; \varphi \end{array}$

 $(K_{MVA_{1}} | Role) \text{ says } \varphi$ $K_{Auth} \text{ says } (MVA_{1} \text{ reps } Role \text{ on } \varphi)$ $K_{Auth} \text{ says } (K_{MVA_{1}} \Rightarrow MVA_{1})$ $Auth \text{ controls } (MVA_{1} \text{ reps } Role \text{ on } \varphi)$ $Auth \text{ controls } (K_{MVA_{1}} \Rightarrow MVA_{1})$ $K_{Auth} \Rightarrow Auth$ $Role \text{ says } \varphi$ $(\Box \triangleright \langle \Box \rangle \land \langle \Box \rangle \land \langle \Xi \rangle \land \langle \Xi \rangle \land \langle \Xi \rangle \land \langle \Xi \rangle$ 17/18

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

Input(Token or Key | Role) says φ Delegation Cert K_{Auth} says (Person or Object reps Role on φ)Key Certificate K_{Auth} says (Token or Key \Rightarrow Person or Object)JurisdictionAuth controls (Person or Object reps Role on φ)JurisdictionAuth controls (Token or Key \Rightarrow Person or Object)

Trust Assumption

 $K_{Auth} \Rightarrow Auth$

```
Transmitting MVA:
```

Receiving MVA

 $\begin{array}{c} (\textit{Token} \mid \textit{Role}) \; \texttt{Says} \; \varphi \\ K_{Auth} \; \texttt{SayS} \; (\textit{Person repS Role ON } \varphi) \\ K_{Auth} \; \texttt{SayS} \; (\textit{Token} \Rightarrow \textit{Person}) \\ Auth \; \texttt{Controls} \; (\textit{Person repS Role ON } \varphi) \\ Auth \; \texttt{Controls} \; (\textit{Token} \Rightarrow \textit{Person}) \\ K_{Auth} \; \texttt{Controls} \; (\textit{Token} \Rightarrow \textit{Person}) \\ K_{Auth} \; \texttt{Controls} \; (\textit{Token} \Rightarrow \textit{Person}) \\ K_{Auth} \; \Rightarrow \; Auth \\ \hline K_{MVA_1} \mid \textit{Role SayS} \; \varphi \\ \end{array}$

 $(K_{MVA_{1}} | Role) \operatorname{Says} \varphi$ $K_{Auth} \operatorname{Says} (MVA_{1} \operatorname{reps} Role \operatorname{On} \varphi)$ $K_{Auth} \operatorname{Says} (K_{MVA_{1}} \Rightarrow MVA_{1})$ $Auth \operatorname{Controls} (MVA_{1} \operatorname{reps} Role \operatorname{On} \varphi)$ $Auth \operatorname{controls} (K_{MVA_{1}} \Rightarrow MVA_{1})$ $K_{Auth} \Rightarrow Auth$ $Role \operatorname{Says} \varphi$ $\Box \triangleright \langle \Box \triangleright \langle \Box \triangleright \langle \Xi \triangleright \langle \Xi \land \Box E \rangle \langle \Xi \rangle \langle \Xi \rangle$ 17/18

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

Transmitting MVA:

Receiving MVA

 $\begin{array}{c} (Token \mid Role) \text{ Says } \varphi & (K_{MVA_1} \mid Role) \text{ Says } \varphi \\ K_{Auth} \text{ Says } (Person \; \text{reps } Role \; \text{On } \varphi) \\ K_{Auth} \text{ Says } (Token \Rightarrow Person) \\ Auth \; \text{ controls } (Person \; \text{reps } Role \; \text{On } \varphi) \\ Auth \; \text{ controls } (Token \Rightarrow Person) \\ Auth \; \text{ controls } (Token \Rightarrow Person) \\ Auth \; \text{ controls } (Token \Rightarrow Person) \\ K_{Auth} \Rightarrow Auth \\ \hline \\ K_{Auth} \Rightarrow Auth \\ \hline \\ K_{MVA_1} \mid Role \; \text{ Says } \varphi \end{array} \qquad MVA 2 \qquad \begin{array}{c} (K_{MVA_1} \mid Role) \; \text{ Says } \varphi \\ K_{Auth} \; \text{ says } (MVA_1 \; \text{ reps } Role \; \text{On } \varphi) \\ Auth \; \text{ controls } (K_{MVA_1} \Rightarrow MVA_1) \\ Auth \; \text{ controls } (K_{MVA_1} \Rightarrow MVA_1) \\ K_{Auth} \Rightarrow Auth \\ \hline \\ K_{MVA_1} \mid Role \; \text{ Says } \varphi \end{array}$

 $17 \, / \, 18$

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

Transmitting MVA:

Receiving MVA

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

Input(Token or Key | Role) says φ Delegation Cert K_{Auth} says (Person or Object reps Role on φ)Key Certificate K_{Auth} says (Token or Key \Rightarrow Person or Object)JurisdictionAuth controls (Person or Object reps Role on φ)JurisdictionAuth controls (Token or Key \Rightarrow Person or Object)Frust Assumption $K_{Auth} \Rightarrow Auth$

Transmitting MVA:

Receiving MVA

Common *form* of requests, delegations, key certificates, jurisdiction, and trust assumptions

Transmitting MVA:

Receiving MVA

(Token | Role) Says φ $(K_{MVA_1} \mid Role)$ Says φ K_{Auth} says (Person reps Role On φ) K_{Auth} says ($\hat{M}VA_1$ reps Role On φ) K_{Auth} Says (Token \Rightarrow Person) K_{Auth} says $(K_{MVA_1} \Rightarrow MVA_1)$ Auth controls (Person reps Role on φ) Auth controls (MVA₁ reps Role on φ) Auth controls (Token \Rightarrow Person) Auth controls $(K_{MVA_1} \Rightarrow MVA_1)$ $K_{Auth} \Rightarrow Auth$ $K_{Auth} \Rightarrow Auth$ MVA 1 MVA 2 $K_{MVA_1} \mid Role \text{ says } \varphi$ Role Savs φ イロト イポト イヨト イヨト

Findings & Conclusions

226+ ACE cadets, captains, & lieutenants from 40+ universities



Formal approach to access control and CONOPS is feasible (with adequate education)

- 21 hours of instruction
- Kripke semantics, basic & distributed access control, delegation, hardware, and confidentiality/integrity policies

Textbook based on accesscontrol logic taught in ACE



Shiu-Kai Chin Susan Older

18/18

Increased their capabilities to design, specify, evaluate, and procure critical systems