Game Theory for Homeland Security:
Lessons Learned from Deployed Applications

Chris Kiekintveld
UTEP

Janusz Marecki
IBM Watson

Milind Tambe
USC Teamcore

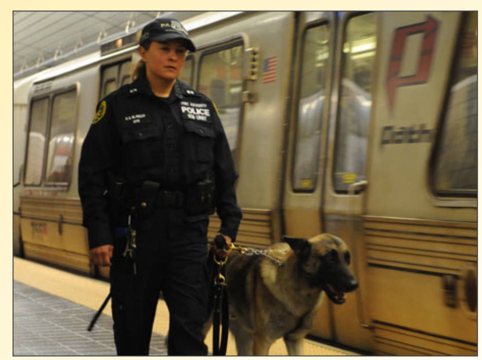
TEAMCORE
USC

Outline

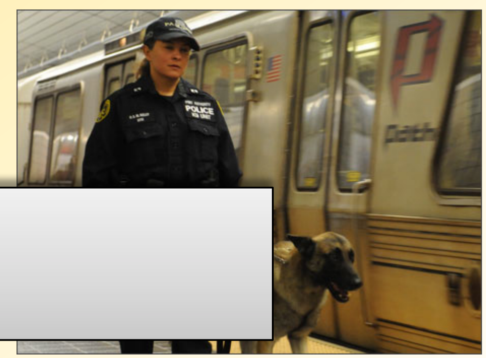
- Deployed real world applications
  - *LAX, FAMS, TSA, …*
- Research highlights
  - *Uncertainty:* Algorithms for Bayesian games
  - *Scaling Up:* Efficient algorithms for massive games
  - …
- Transitioning from theory to practice

  - *Algorithms:* AAMAS(06,07,08,09,10); AAAI (08,10)
  - *Behavioral game theory*: AAMAS'09, AI Journal (2010)
  - *Applications:* AAMAS Industry track (08,09), AI Magazine (09), Interfaces (10), Informatica (10)

Many Targets   Few Resources



Many Targets Few Resources



How to assign limited resources to defend the targets?

ARMOR: Deployed at LAX August 2007

- LAWA: Los Angeles World Airports police
  - *Randomized checkpoints & K9 allocation?*
- Assistant for randomized monitoring over routes
  - *Reward matrices: Embed with LAX, get data*

ARMOR-Checkpoints

ARMOR-K9

More Real-World Deployments

- *IRIS for Federal Air Marshals*: **Deployed** Oct 2009
- *GUARDS for TSA*: Pittsburgh deployed and in full use
  - *All airports Fall'2010?*
- *Coast Guard (Boston)*: Getting started next

IRIS

GUARDS

PROTECT

Key Issues

- Unpredictable schedules
  - *Intelligent, adaptive adversaries*
  - *Surveillance, insider threats*
- Diverse targets
  - *Varying consequences, vulnerabilities*
  - *Non-uniform randomization*
- Uncertainty about attackers
  - *Multiple groups with different capabilities*
  - *Uncertain preferences and motivations*

Bayesian Stackelberg Games

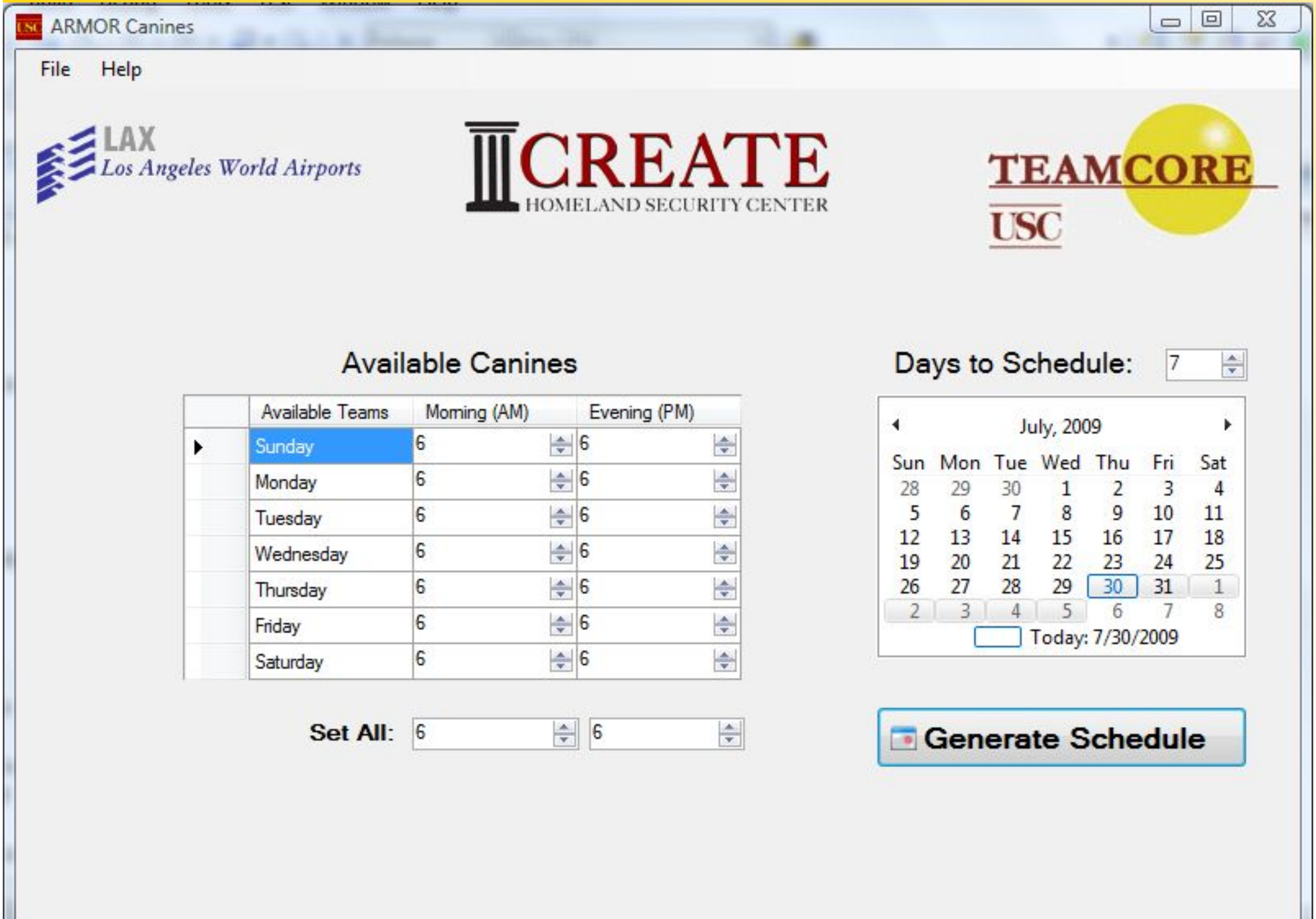
- Limited resources, targets different weights
- *Stackelberg*: Security commits, adversary responds
- *Bayesian*: Uncertain adversary types
- *Optimal security allocation:* Weighted random
- Strong Stackelberg Equilibrium (Bayesian)
  - *NP-hard*

Adversary

Police

	Terminal #1	Terminal #2
Terminal #1	5, -3	-1, 1
Terminal #2	-5, 5	2, -1

ARMOR Canine: Interface



Efficient Algorithms

Challenges: Combinatorial explosions due to:

- *Adversary types*: Adversary strategy combination
- *Defender strategies*: Allocations of resources to targets
  - *E.g. 100 flights, 10 FAMS*
- *Attacker strategies*: Attack paths
  - *E.g. Multiple attack paths to targets in a city*

SCALE-UP			Domain structure exploited	Exact or Approx	Type of equilibrium	Algorithm
Defender actions	Attacker actions	Attacker types				
Low	Low	Medium	None	Approx	SSE	ARMOR 2007
Low	Low	Medium	None	Exact	SSE	ARMOR 2008
Low	Low	Medium	None	Exact	rationality, observation	COBRA 2009
Medium	Low	Low	High (Security game, 1 target)	Exact	SSE	IRIS-I 2009
Medium	Low	Low	High (Security game, 2 targets)	Approx	SSE	IRIS-II 2009
Medium	Low	Low	Med (Security game, N targets)	Exact	SSE	IRIS-III 2010
Medium	Medium	Low	High (zero-sum, graph)	Approx	SSE	RANGER 2010

ARMOR: Multiple Adversary Types

- *NP-hard*
  - *Previous work: Linear programs using Harsanyi transformation*

P=0.3

	Term #1	Term #2
Term#1	5, -3	-1, 1
Term#2	-5, 5	2, -1

P=0.5

	Term #1	Term #2
Term#1	2, -1	-3, 4
Term#2	-[illegible]1	3, -3

P=0.2

	Term #1	Term #2
Term#1	4, -2	-1,0.5
Term#2	-4, 3	1.5, -0.5

	111	121	112	211	…	…	…	222
Terminal #1	3.3,-2.2	2.3,…						
Terminal #2	-3.8,2.6	…,…						

Multiple Adversary Types: Decomposition for Bayesian Stackelberg Games

- Mixed-integer programs
- No Harsanyi transformation

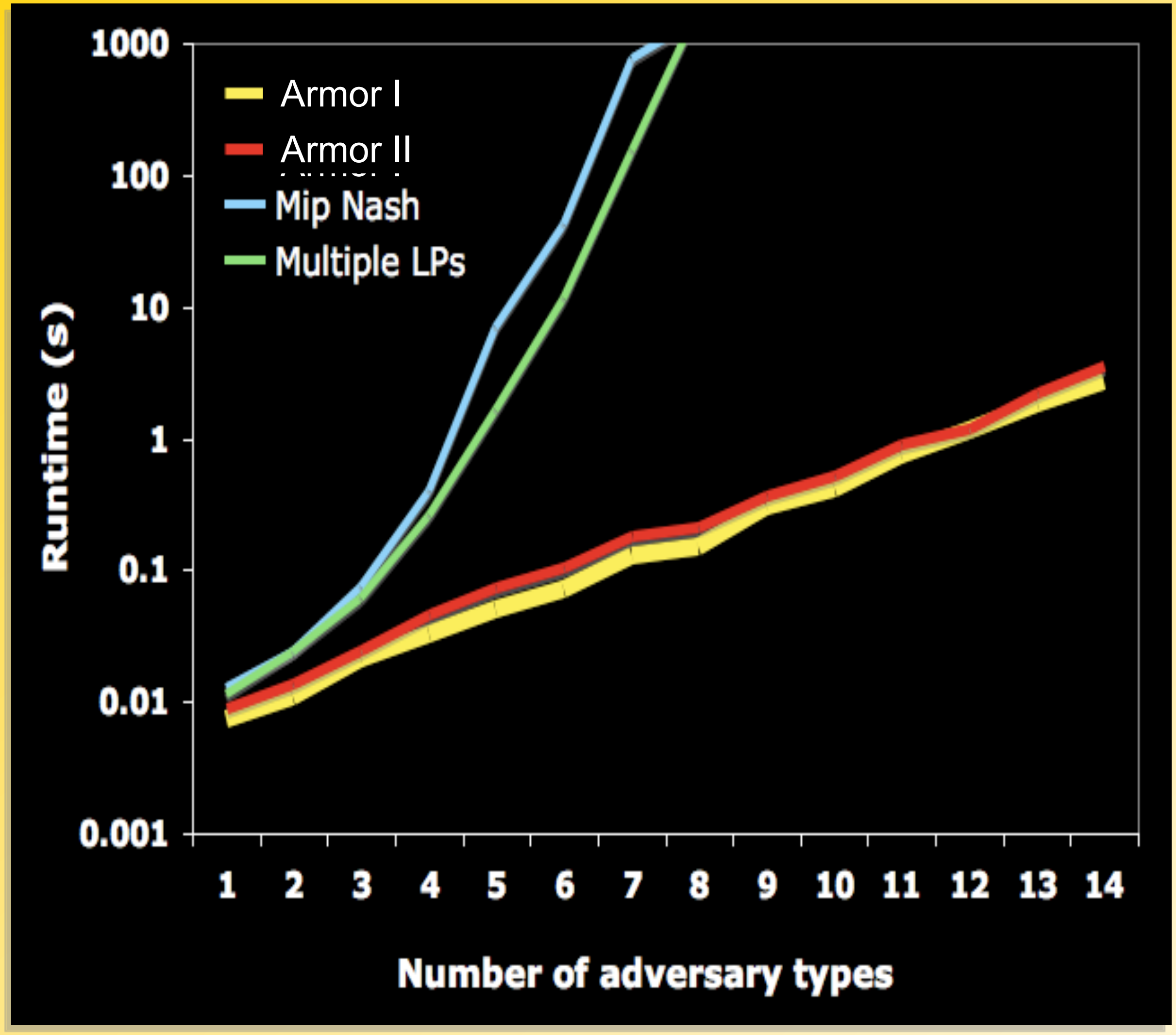
$$\max_{x,q} \sum_{i \in X} \sum_{l \in L} \sum_{j \in Q} p^l R_{ij}^l x_i q_j^l$$

$$s.t. \sum_i x_i = 1, \sum_{j \in Q} q_j^l = 1$$

$$0 \leq (a^l - \sum_{i \in X} C_{ij}^l x_i) \leq (1 - q_j^l) M$$

$$x_i \in [0 \ldots 1], q_j^l \in \{0,1\}$$

ARMOR: Run-time Results



- *Multiple LPs (Conitzer & Sandholm'06)*
- *MIP-Nash (Sandholm et al'05)*
- *Sufficient for LAX*

SCALE-UP						
Defender actions	Attacker actions	Attacker types	Domain structure exploited	Exact or Approx	Type of equilibrium	Algorithm
Low	Low	Medium	None	Approx	SSE	ARMOR 2007
Low	Low	Medium	None	Exact	SSE	ARMOR 2008
Low	Low	Medium	None	Exact	rationality, observation	COBRA 2009
Medium	Low	Low	High (Security game, 1 target)	Exact	SSE	IRIS-I 2009
Medium	Low	Low	High (Security game, 2 targets)	Approx	SSE	IRIS-II 2009
Medium	Low	Low	Med (Security game, N targets)	Exact	SSE	IRIS-III 2010
Medium	Medium	Low	High (zero-sum, graph)	Approx	SSE	RANGER 2010

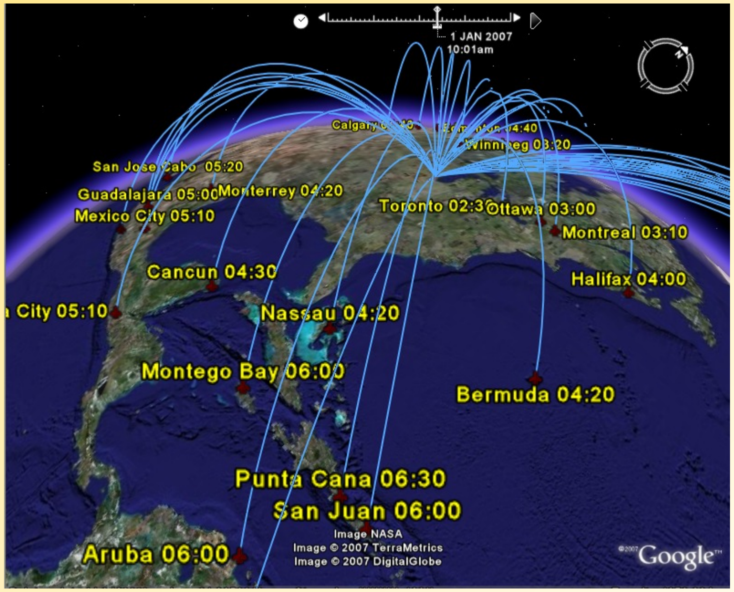
Federal Air Marshals Service

<u>Flights (each day)</u>
~27,000 domestic flights
~2,000 international flights

Estimated 3,000-4,000 air marshals

Massive scheduling problem:
How to assign marshals to flights?

International Flights from Chicago O'Hare



IRIS Scheduling Tool

IRIS Scheduling Tool

Flight Information

Resources

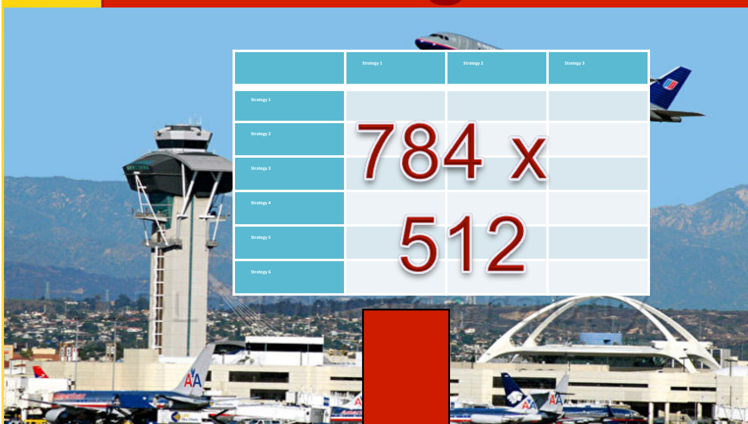
Risk Information

Game Model

Solution Algorithm

Randomized Deployment Schedule

IRIS: Large Numbers of Defender Strategies



*FAMS: **Joint** Strategies*

4 Flight tours
2 Air Marshals → 6 Schedules

100 Flight tours
10 Air Marshals → 17 ***trillion*** Schedules: ARMOR out of memory

Addressing Scale-up in Defender Strategies

- *Security game:Payoffs depend on attacked target covered or not*
  - *Target independence*

- *Avoid enumeration of all joint strategies:*
  - *Marginals*: Probabilities for individual strategies/schedules
    - Sample required joint strategies: IRIS I and IRIS II
      - *But:* Sampling may be difficult if schedule conflicts
    - *IRIS I (single target/flight), IRIS II (pairs of targets)*
  - *Branch & Price*: Probabilities on joint strategies
    - Enumerates required joint strategies, handles conflicts
    - *IRIS III (arbitrary schedules over targets)*

Explosion in Defender Strategies: Marginals for Compact Representation

ARMOR: 10 tours, 3 air marshals

ARMOR Actions	Tour combos	Prob
1	1,2,3	x1
2	1,2,4	x2
3	1,2,5	x3
…	…	…
120	8,9,10	x120

Compact Action	Tour	Prob
1	1	y1
2	2	y2
3	3	y3
…	…	…
10	10	y10

Payoff duplicates: Depends on target covered

		Attack 2	Attack …
1,2,3		4,-8	…
1,2,4		4,-8	…
1,3,5		-9,5	…
…		…	…

$$\max_{x,q} \sum_{i\in X}\sum_{l\in L}\sum_{j\in Q} p^l R^l_{ij} x_i q^l_j$$

$$s.t. \sum_i x_i = 1, \sum_{j\in Q} q^l_j = 1$$

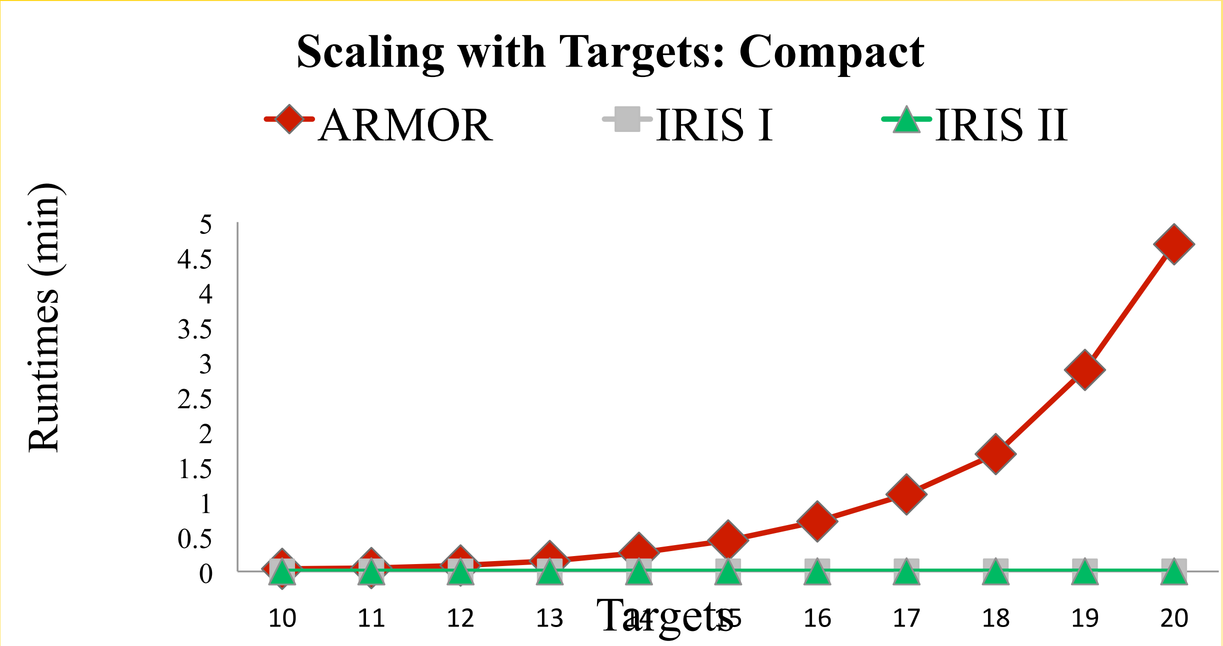
$$0 \le (a^l - \sum_{i\in X} C^l_{ij} x_i) \le (1 - q^l_j) M$$

$$x_i \in [0...1], q^l_j \in \{0,1\}$$

IRIS MILP similar to ARMOR

- 10 instead of 120 variables
- y1+y2+y3…+y10 = 3
- Construct samples over tour combos

IRIS Speedups: Efficient Algorithms II



	ARMOR Actions	ARMOR Runtime	IRIS Runtime
FAMS Ireland	6,048	4.74s	0.09s
FAMS London	85,275	----	1.57s

IRIS III

- Next generation of IRIS
- General scheduling constraints
  - *Schedules can be any subset of targets*
  - *Resource can be constrained to any subset of schedules*
  - *Problem is NP hard (Conitzer et al.)*
- Branch and Price Framework
  - *Techniques for large-scale optimization*
  - *Not an "out of the box" solution*

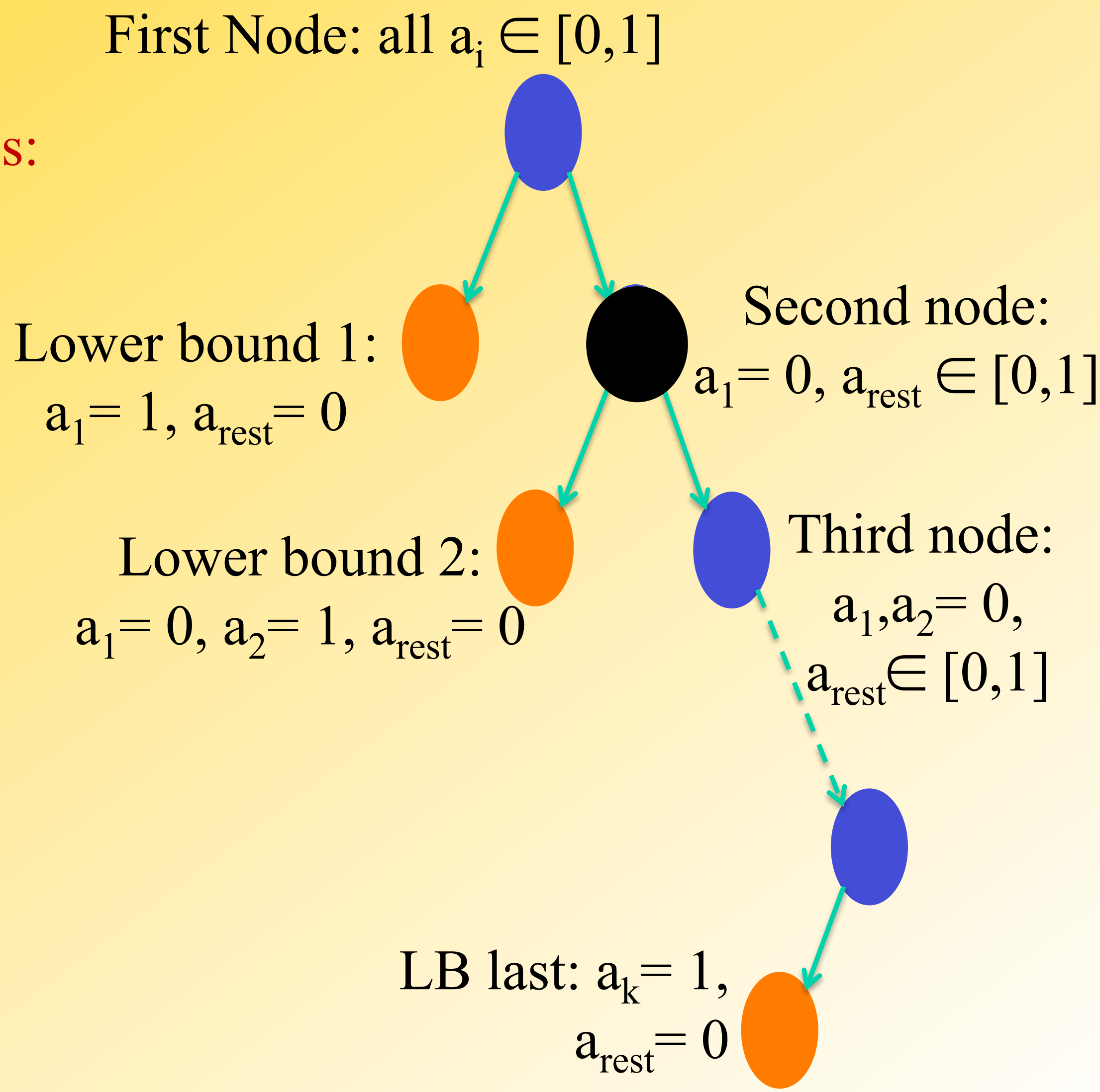
IRIS III Master Problem

$$
\begin{aligned}
\max \quad & & d \\
\text{s.t.} \quad & \mathbf{d} - & \mathbf{DPx} - \mathbf{U}_d^u \leq (\mathbf{1} - \mathbf{a})M \\
& \mathbf{k} - & \mathbf{APx} - \mathbf{U}_a^u \leq (\mathbf{1} - \mathbf{a})M \\
& & \mathbf{APx} + \mathbf{U}_a^u \leq \mathbf{k} \\
& & \sum_{j \in J} x_j = 1 \\
& & \mathbf{x}, \mathbf{a} \geq 0
\end{aligned}
$$

IRIS III: Branch and Price: Branch & Bound + Column Generation

Not “out of the box”

- Upper bounds: IRIS I
- Column generation leaf nodes: Network flow



Branching and Bounding

- Standard approach: LP Relaxation
  - *Allow integers to take on any value*

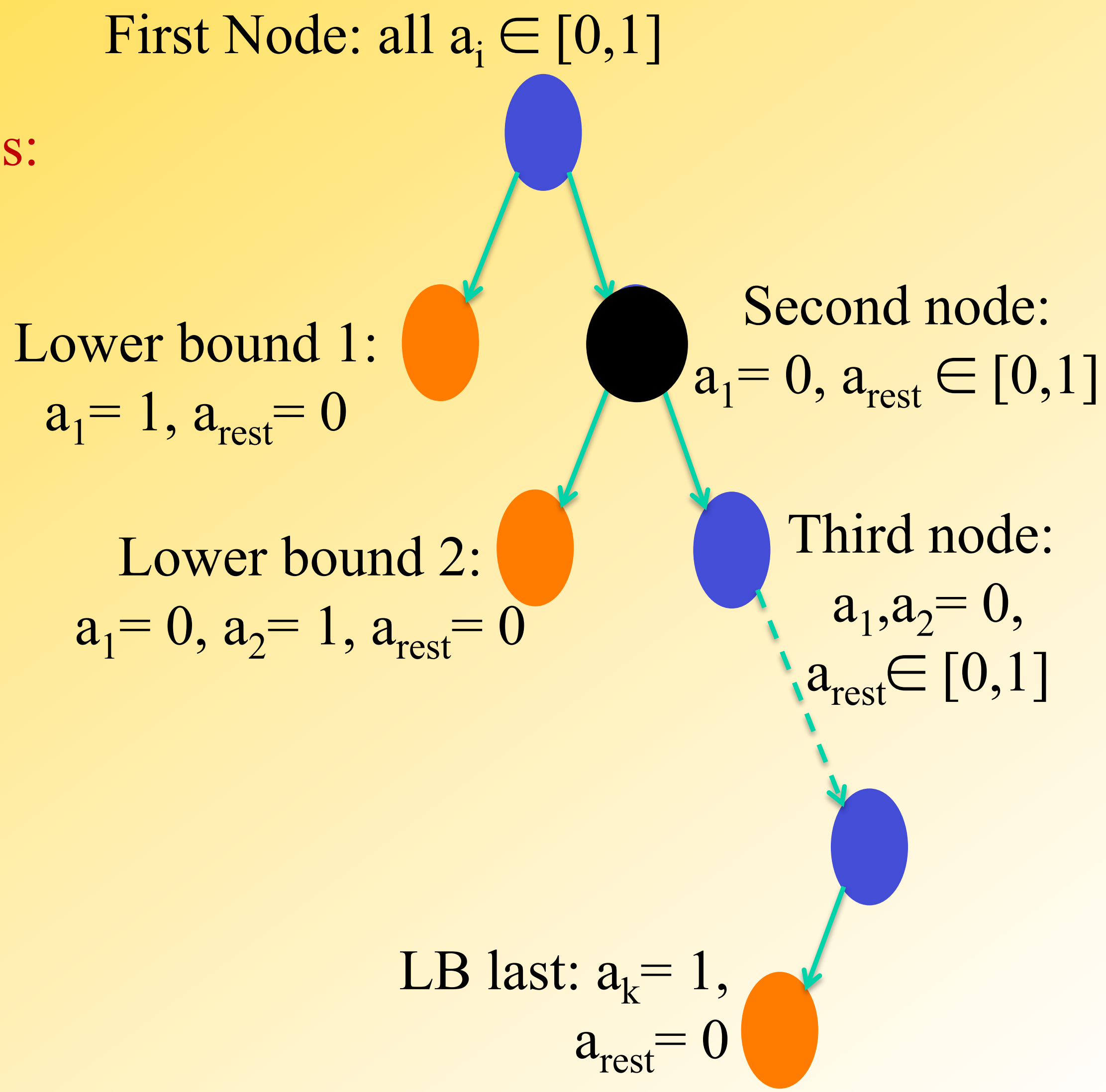
- Problem-specific relaxation
  - *Resources ignore scheduling constraints*
  - *Resources cover the maximum number of possible targets*

Can be solved extremely fast using IRIS I

IRIS III: Branch and Price: Branch & Bound + Column Generation

Not "out of the box"

- Upper bounds: IRIS I
- Column generation leaf nodes: Network flow



Column Generation

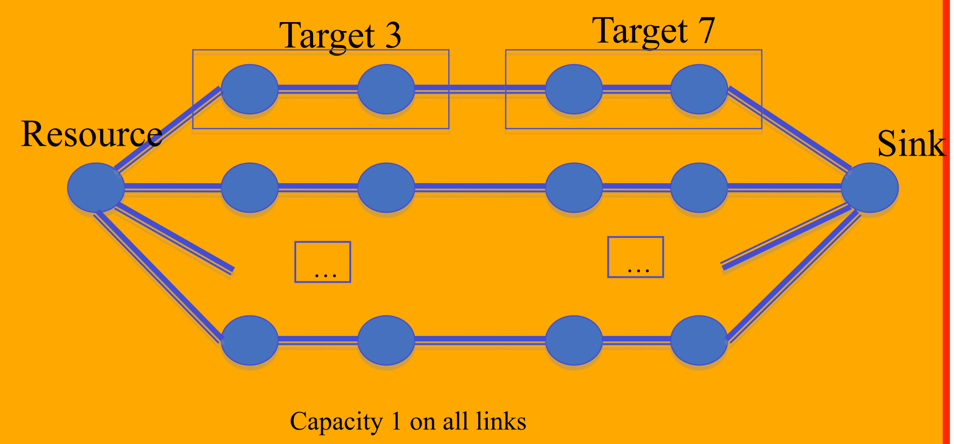
"Master" Problem (linear program)

Restricted set of joint schedules

Solution with N joint schedules

$(N+1)^{th}$ joint schedule

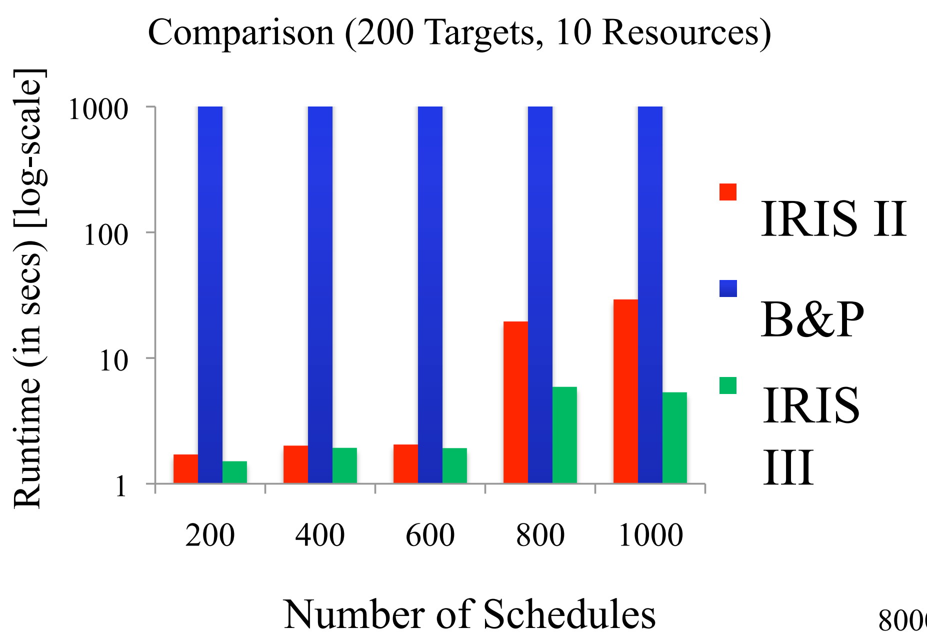
"Slave" Problem

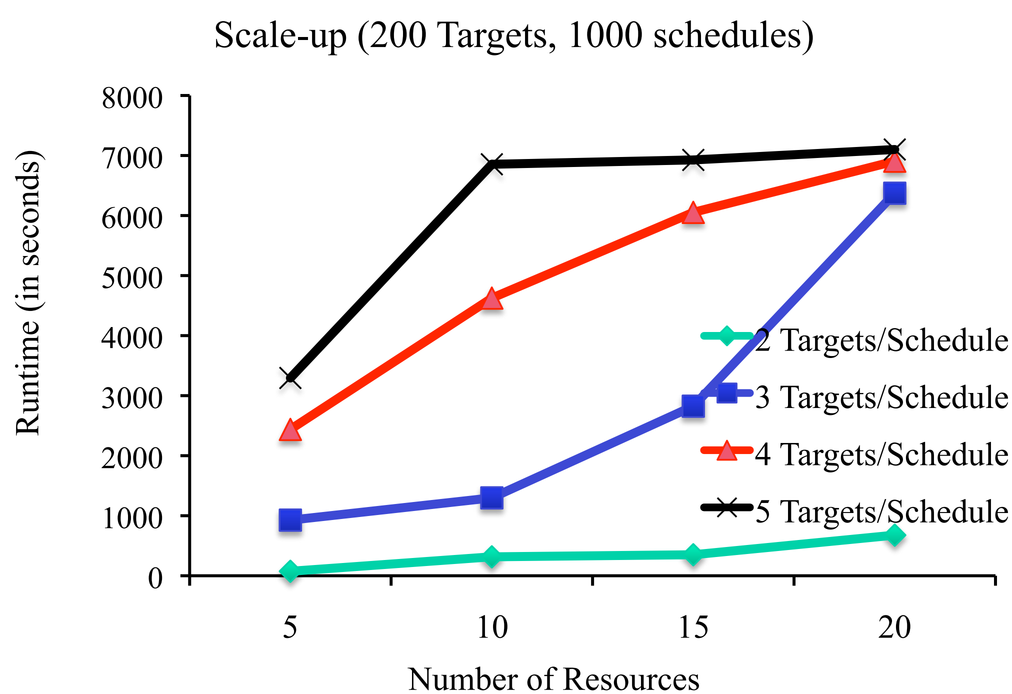


Return the "best" joint schedule to add

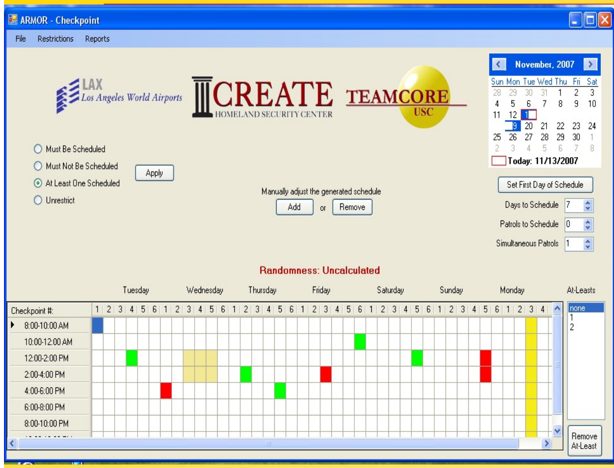
Minimum cost network flow: Identifies joint schedule to add

Results: IRIS III



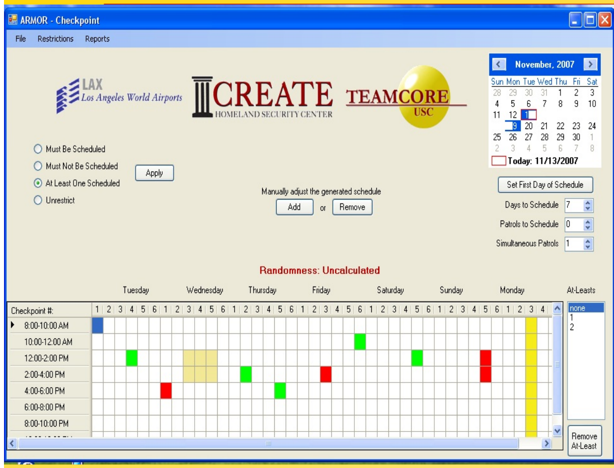


Deployed Applications: ARMOR, IRIS, GUARDS



- Research challenges
  - *Efficient algorithms:* Scale-up to real-world problems
  - *Observability:* Adversary surveillance capabilities
  - *Human adversary:* Bounded rationality, observation power
  - *Payoff uncertainty:* New algorithms, models

Deployed Applications: ARMOR, IRIS, GUARDS



- Transitioning from theory to practice
  - *Defining and validating models*
  - *Explaining models and output*
  - *Supporting fielded applications*
  - *Evaluating deployed systems*

Modeling Security Games

- Approach: domain experts supply the model
  - *Experts must understand necessary game inputs*
  - *What information is available? Sensitive?*
  - *Number of inputs must be reasonable (tens, not thousands)*
  - *What models can we solve computationally?*
- Uncertainty is ubiquitous
  - *Outcomes are inherently unpredictable*
  - *How do we accurately assess attacker capabilities and preferences?*
  - *New challenge: scalable, robust algorithms*

Explaining Results

- Organizational acceptance/trust
  - *End users up to senior managers*
  - *Most will not understand game theory*
- Finding the right level of abstraction
  - *LAX: detailed patrol instructions vs. general time/place*
- Providing options for analysis/modification:
  - *LAX: provided "edit" capability, never used*
- Explaining outputs of large "black box" game models
  - *Is the model correct?*
  - *Is the software correct?*
  - *New challenge: intuitive explanations for game theory*

Supporting Fielded Applications

- Deployed applications require ongoing support
  - *Debugging*
  - *New feature requests/updates*
  - *Use beyond the original scope*

- Students graduate
- Grant support ends
- Lots of "non-research" work

Evaluation of Real-World Applications

- Beyond run-time and optimality proofs

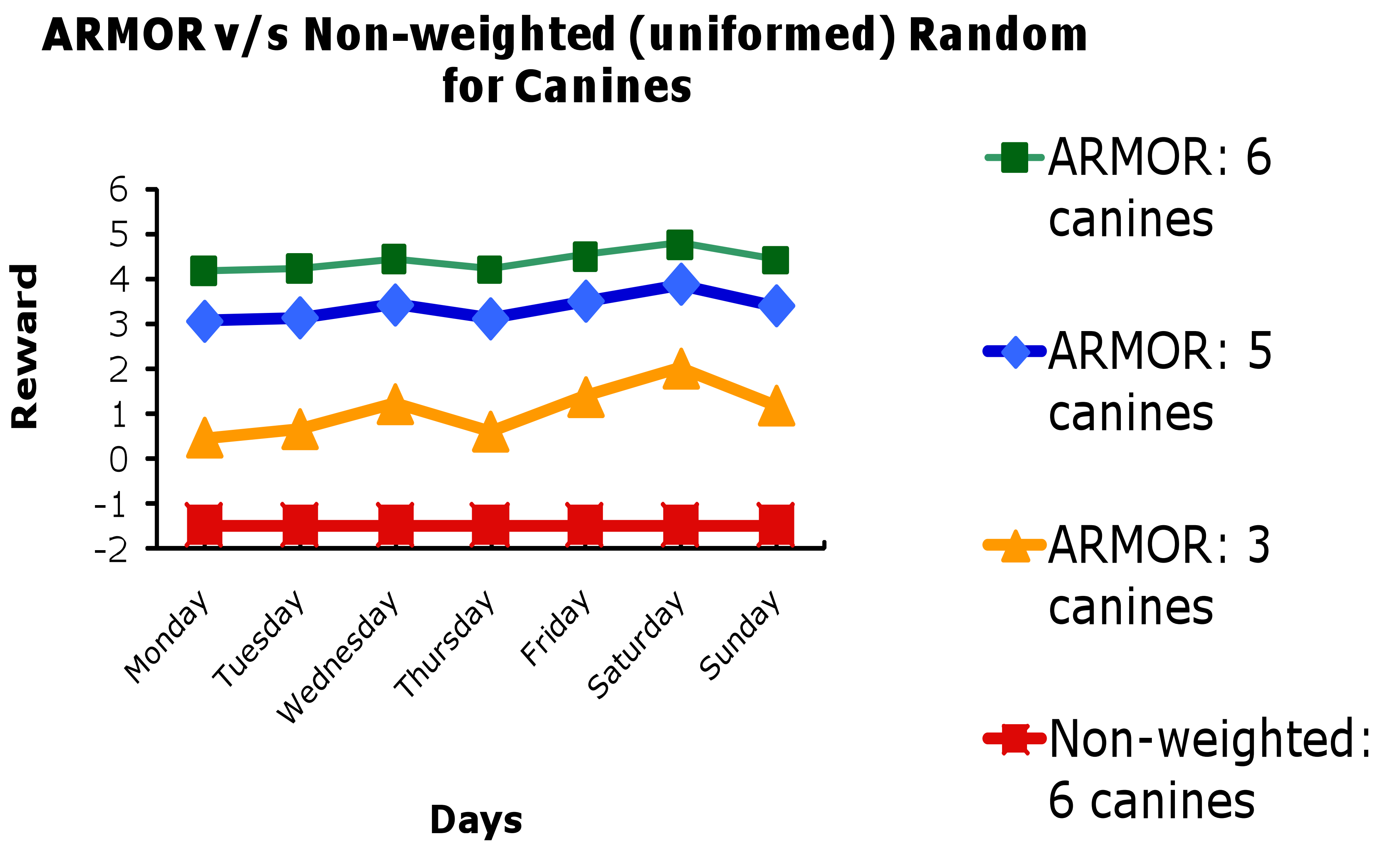
Reviewer questions	**Operational perspective**

So how can we evaluate?...

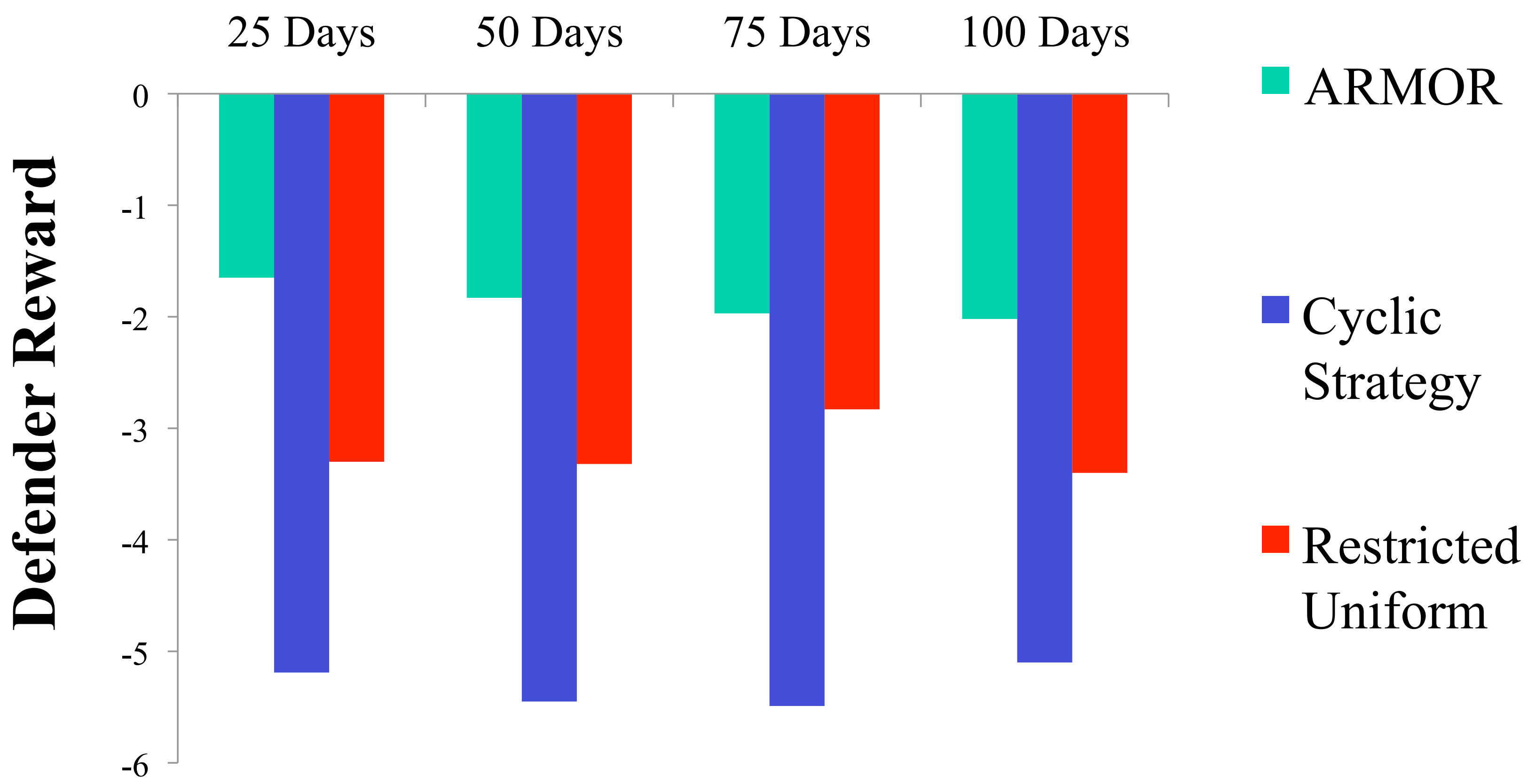
No 100% security; are we better off than previous approaches?

- *Models and simulations*
- *Human adversaries in the lab*
- *Expert evaluation*
- *Supportive indicators from the field*

Models & Simulations I



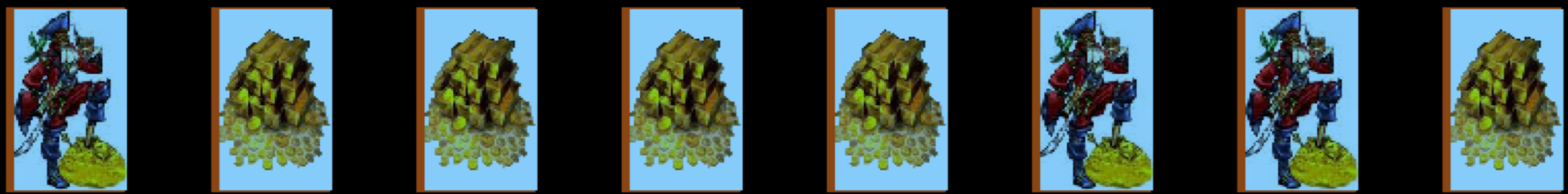
Models & Simulations II



Models and Simulations III

Human Adversaries In the Lab

	1	2	3	4	5	6	7	8



Your Rewards:

8	5	3	10	1	3	9	4

Your Penalties:

−3	−2	−3	−2	−3	−3	−2	−3

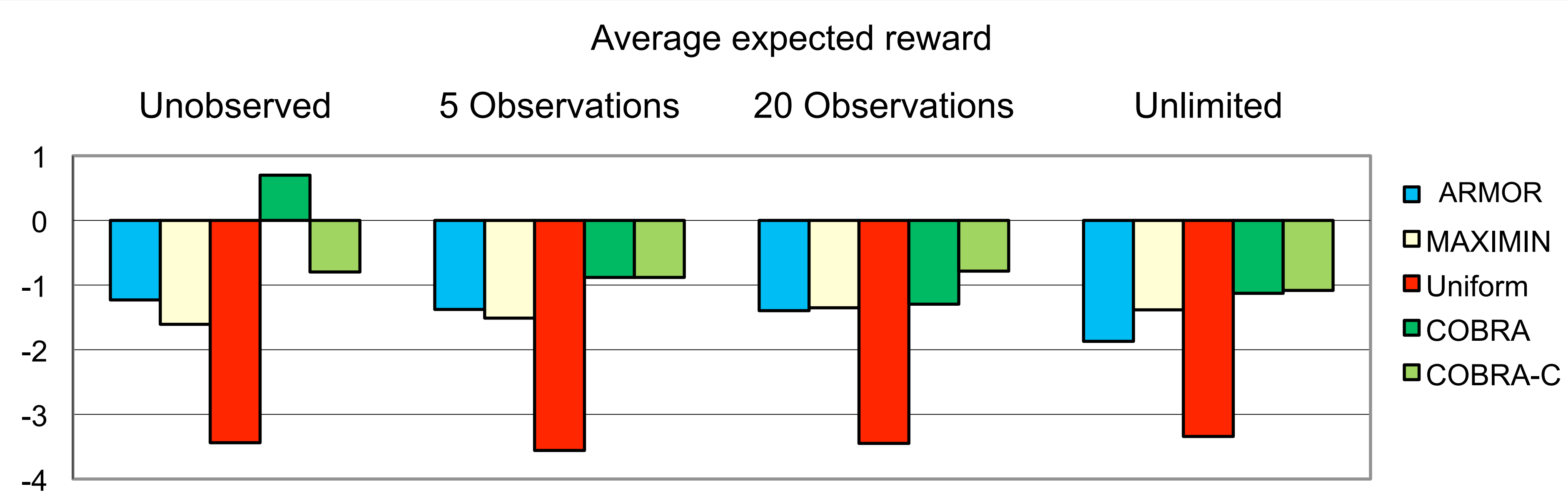
Pirate's Rewards:

4	3	1	5	1	2	5	2

Pirate's Penalties:

−8	−10	−1	−8	−1	−3	−11	−5

Human Adversaries in the Lab



- **ARMOR:** Outperforms uninformed random, not Maximin
- **COBRA:** Anchoring bias, "epsilon-optimal"

$$\max_{x,q} \sum_{i \in X} \sum_{l \in L} \sum_{j \in Q} p^l R^l_{ij} x_i q^l_j$$

$$s.t. \quad x' = (1-\alpha)x + \alpha(1/|X|)$$

$$\varepsilon(1 - q^l_j) \le (a^l - \sum_{i \in X} C^l_{ij} x'_i) \le \varepsilon + (1 - q^l_j)M$$

Expert Evaluation I

April 2008

February 2009

LAX Spokesperson, CNN.com, July 14, 2010: "*Randomization and unpredictability is a key factor in keeping the terrorists unbalanced….It is so effective that airports across the United States are adopting this method.*"

Expert Evaluation II

- Federal Air Marshals Service (May 2010):

We…**have continued to expand the number of flights scheduled using IRIS**….we are **satisfied with IRIS and confident in using this scheduling approach.**

James B. Curren

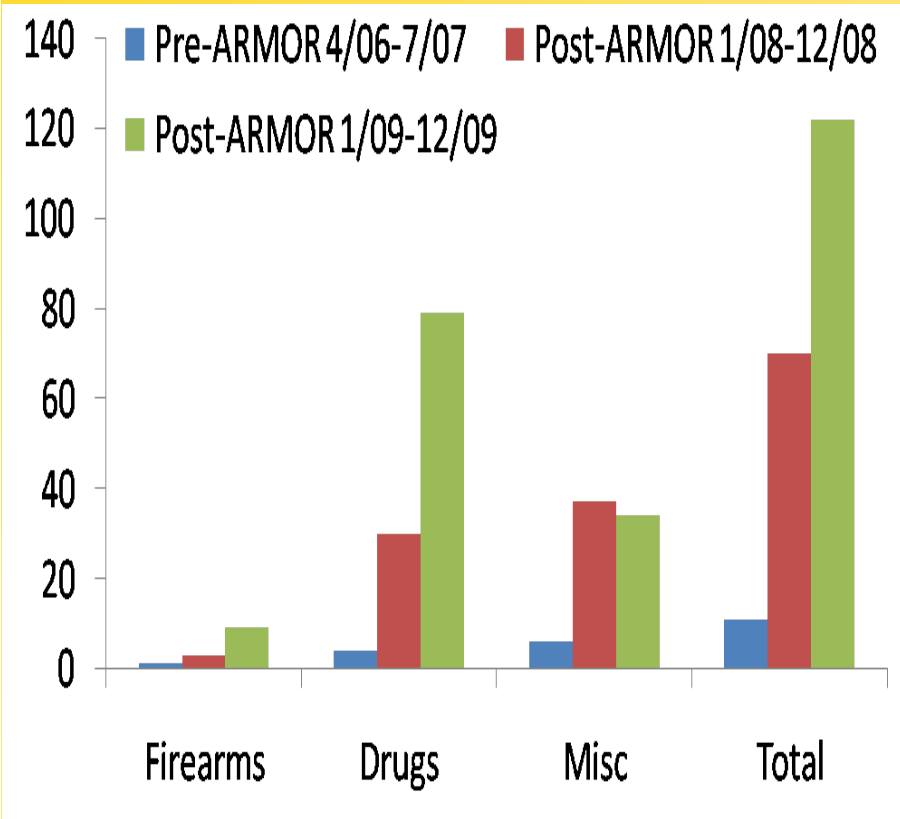
Special Assistant, Office of Flight Operations,

Federal Air Marshals Service

Supporting Indicators from the Field

They are using our systems for a number of years!

Arrest record (Not a scientific test!):

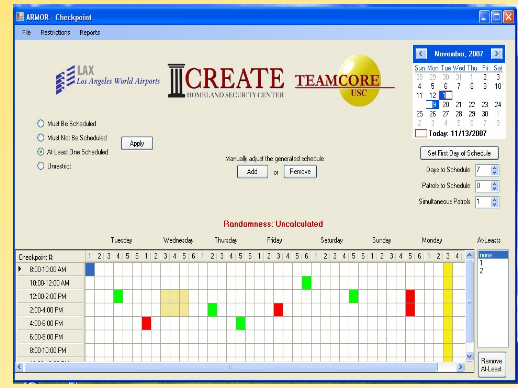


January 2009

- January 3rd *Loaded 9/mm pistol*
- January 9th *16-handguns, 4-rifles,1-assault rifle; 1000 rounds of ammo*
- January 10th *Two unloaded shotguns*
- January 12th *Loaded 22/cal rifle*
- January 17th *Loaded 9/mm pistol*
- January 22nd *Unloaded 9/mm pistol*

Takeaways

- Deployed game-theoretic solutions
  - *Operational, day-to-day decision-making*
  - *Scaling to national problems*
  - *Research advances allow new applications*
  - *Transition is challenging, but rewarding*
- Many open research problems
  - *Scaling up algorithms*
  - *Game modeling and elicitation*
  - *Explaining game solutions*
  - *Robustness to uncertainty*



Thank you!

http://teamcore.usc.edu

Chris Kiekintveld: *cdkiekintveld@utep.edu*
Janusz Marecki: *marecki@us.ibm.com*

- Milind Tambe
- Chris Kiekintveld
- Manish Jain
- James Pita
- Praveen Paruchuri
- Janusz Marecki
- Jonathan Pearce
- Fernando Ordonez
- Sarit Kraus
- Vince Conitzer
- David Kempe
- Jason Tsai