Selecting and Scheduling Cybersecurity Mitigations with Resource Constraints

Ashley Peper, Jim Luedtke, Laura A. Albert, Department of Industrial and Systems Engineering, University of Wisconsin - Madison

Problem Setting

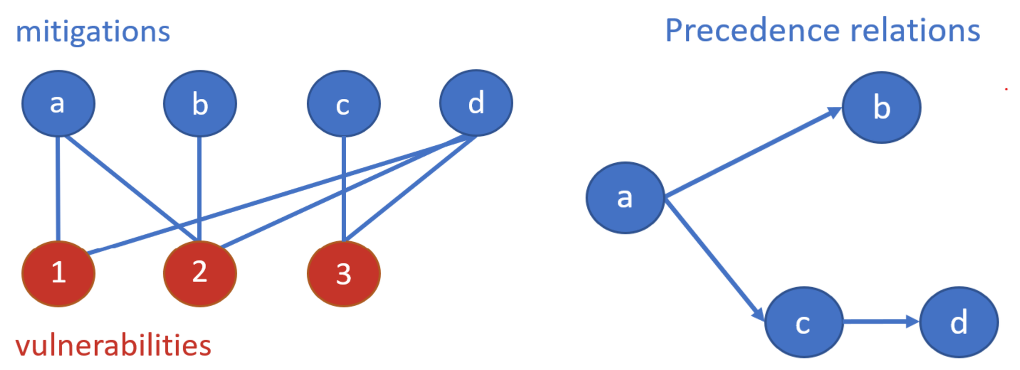
IT managers regularly face the challenging problem of deploying mitigations to improve cybersecurity.

Mitigation selection challenges:

- Appropriately allocating resources over time to achieve security quickly and efficiently.
- Addressing precedence relations when implementing multiple mitigations.
- Prioritizing important vulnerabilities without sacrificing time-efficient overall coverage.

Problem

What is the best way to schedule the implementation of mitigations subject to resource, budget, and precedence constraints, to achieve maximal coverage of vulnerability nodes when covering a node multiple times gives diminishing returns?



Existing Model Limitations

- **Mitigation selection** [2]: Provide ways to choose mitigations under this multiple-coverage notion, but do not consider deployment in resource-constrained settings.
- **Resource Constrained Project Scheduling** [1]: RCPSPs match our problem's scheduling structure, but cannot model the multiple-coverage objective.

IP Model

$\mathcal{T}$	set $\{1, ..., T\}$ of time periods
N	set of nodes
J	set of jobs/mitigations
R	set of resources
P	set of precedence relations
w_{jn}	benefit of completing $j \in J$ on $n \in N$
τ_j	time required to complete $j \in J$
c_{jr}	cost per period of $r \in R$ for $j \in J$
C_j	cost of $j \in J$ for total budget
b_{rt}	budget for $r \in R$ for period $t \in \mathcal{T}$
B	total budget (not time indexed)
f_n	piecewise-linear concave function for objective
α_t	time-weighting coefficient for objective
z_{nt}	amount of coverage for $n \in N$ at time $t \in \mathcal{T}$.
x_{jt}	=1 if job $j \in J$ finishes at time $t \in \mathcal{T}$, binary

$$\max \sum_{t=1}^{T} \sum_{n \in N} \alpha_t f_n(z_{nt})$$

$$\text{s.t. } z_{nt} \le \sum_{j \in J} \sum_{s=1}^{t} w_{jn} x_{js} \qquad \forall t \in \mathcal{T},\ n \in N$$

$$\sum_{t=1}^{T} x_{jt} \le 1 \qquad \forall j \in J$$

$$x_{jt} = 0 \qquad \forall j \in J, t = 1, .., \tau_j - 1$$

$$\sum_{j \in J} \sum_{s=t}^{t+\tau_j-1} c_{jr} x_{js} \le b_{rt} \qquad \forall t \in \mathcal{T},\ r \in R$$

$$\sum_{t=1}^{T} \sum_{j \in J} C_j x_{jt} \le B$$

$$\sum_{s=1}^{t} x_{js} \le \sum_{s=1}^{t-\tau_j} x_{is} \qquad \forall (i,j) \in P, t = 1, ..., T$$

$$x_{jt} \in \{0, 1\} \qquad \forall j \in J,\ t \in \mathcal{T}$$

$$z_{nt} \ge 0 \qquad \forall n \in N, t \in \mathcal{T}$$

Benefit of Integrated Model

What if we don't combine coverage and scheduling?

1. **RCPSP**
   We relax the notion of coverage by removing constraints with z, and using the objective
   $$\max \sum_{j \in J} \sum_{t=1}^{T} a_t h_j x_{jt}$$
   where h_j is some estimation of coverage provided by job j, and a_t is a time-weighting parameter.
2. **Select then Schedule (*STS*)**
   Ignore scheduling, choose jobs for best coverage. Then use an RCPSP to schedule these jobs.

Solving Large Instances

We propose a rolling horizon heuristic using an interval model derived from [1].

Interval Model

- Group time periods into a set of time intervals
- Provides a relaxation of our full model
- Schedules jobs into intervals, which we can use to schedule into time periods (*Int-fast*)

Rolling Horizon Heuristic (*Int-roll*)

1. Use interval model to find a solution.
2. Fix some jobs at beginning of horizon.
3. Repeat, fixing more jobs later into the horizon at each iteration.

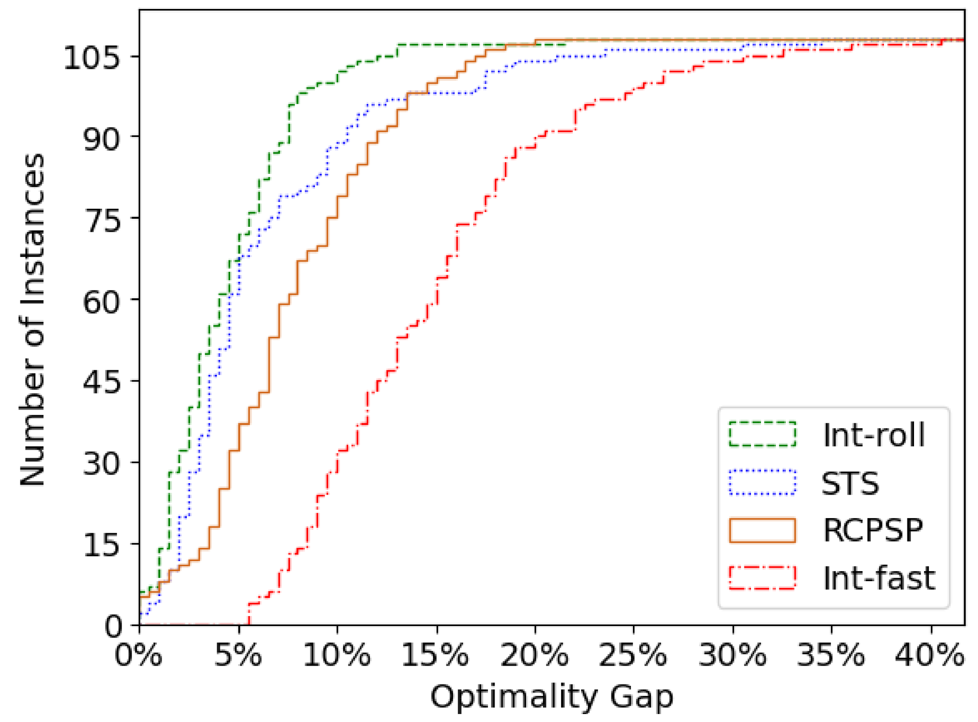
Contact Info & Acknowledgements

Ashley Peper: apeper2@wisc.edu

This work was in part funded by the National Science Foundation Award 2000986.

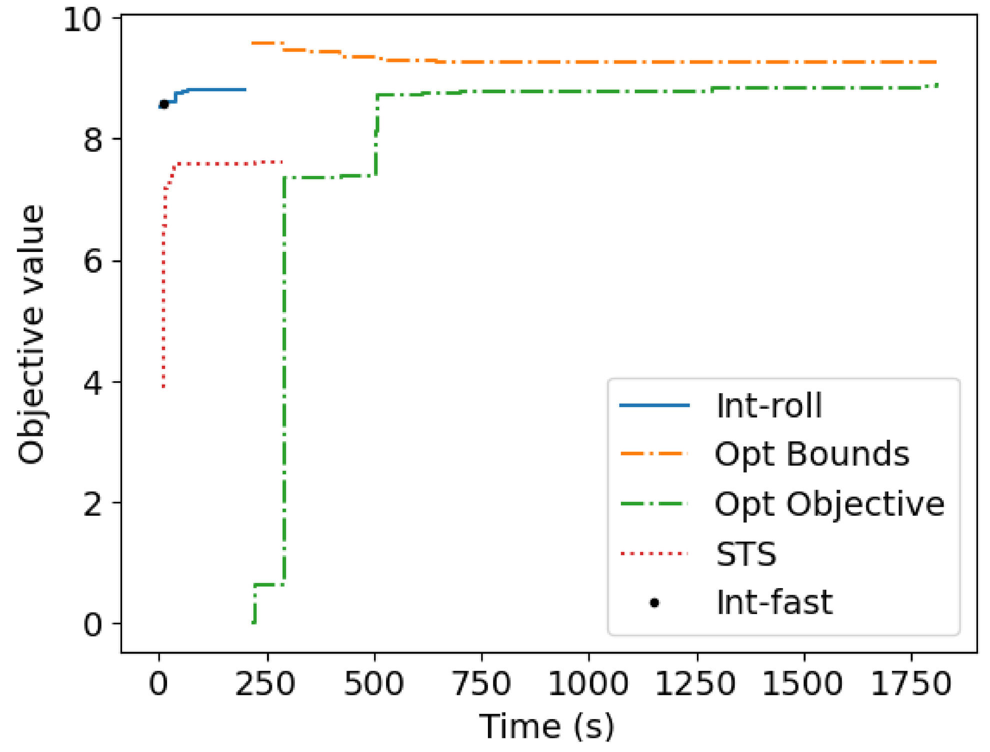
Computational Comparisons

- *RCPSP* and *STS* average 7% optimality gaps, showing benefit to an integrated model.



Heuristic Performance

- *Int-roll* finds good solutions faster than other methods given a time limit.



References

[1] Rodrigo A Carrasco, Diego Fuentes, and Eduardo Moreno. *Approximation algorithm for resource- constrained project scheduling problems with net present value objective.* arXiv preprint arXiv:2209.02029, 2022.

[2] Kaiyue Zheng, Laura A Albert, James R Luedtke, and Eli Towle. *A budgeted maximum multiple coverage model for cybersecurity planning and management.* IISE Transactions, 51(12):1303–1317, 2019.