Program Manager: Kevin Thompson
OAC Office of Advanced Cyberinfrastructure (OAC)
CSE Direct For Computer & Information Science & Engineering
Theodore Allen allen.515@osu.edu (Principal Investigator)
Rajiv Ramnath (Co-Principal Investigator)
Laura Albert (Co-Principal Investigator)

2019 SaTC PI Meeting October 2019

EAGER: A Framework For Economical Cyber Security Inspection and Assurance

Key Personnel: Helen Patton, Robert Pardee, Christopher Hartley
Graduate Students: Enhao Liu (Ph.D. Candidate, ISE)
Mehdi Mashayekhi (Ph.D. Candidate, ISE)

Innovative Vulnerability Scanning & Patching Framework

POMDP-Directed Inspection

TABLE 2 Counts of transitions from a major university for Linux hosts under four actions (a) Auto-patching, (b) Research-Accept, (c) Research-compensate and (d) Remediation

(a) Auto-patching

From\to	Low	Medium	High	Critical
Low	16075	1404	35	15
Medium	412	127519	756	59
High	0	412	127519	815
Critical	0	0	412	128334

(b) Research-Accept

From\to	Low	Medium	High	Critical
Low	1073	4	0	0
Medium	463	610	4	0
High	34	429	610	4
Critical	8	53	18	799

(c) Research-compensate

From\to	Low	Medium	High	Critical
Low	1077	0	0	0
Medium	1077	0	0	0
High	34	1043	4	0
Critical	8	53	817	0

(d) Remediation

From\to	Low	Medium	High	Critical
Low	100	100	0	0
Medium	100	100	0	0
High	100	100	0	0
Critical	100	100	0	0

TABLE 3 Estimated transition probabilities from a major university for Linux hosts under four actions (a) Auto-patching, (b) Research-Accept, (c) Research-compensate and (d) Remediation

(a) Auto-patching

From\to	Low	Medium	High	Critical
Low	0.9171	0.0801	0.0020	0.0009
Medium	0.0032	0.9905	0.0059	0.0005
High	0.0000	0.0032	0.9905	0.0063
Critical	0.0000	0.0000	0.0032	0.9968

(b) Research-Accept

From\to	Low	Medium	High	Critical
Low	0.9963	0.0037	0.0000	0.0000
Medium	0.4299	0.5664	0.0037	0.0000
High	0.0316	0.3983	0.5664	0.0037
Critical	0.0091	0.0604	0.0205	0.9100

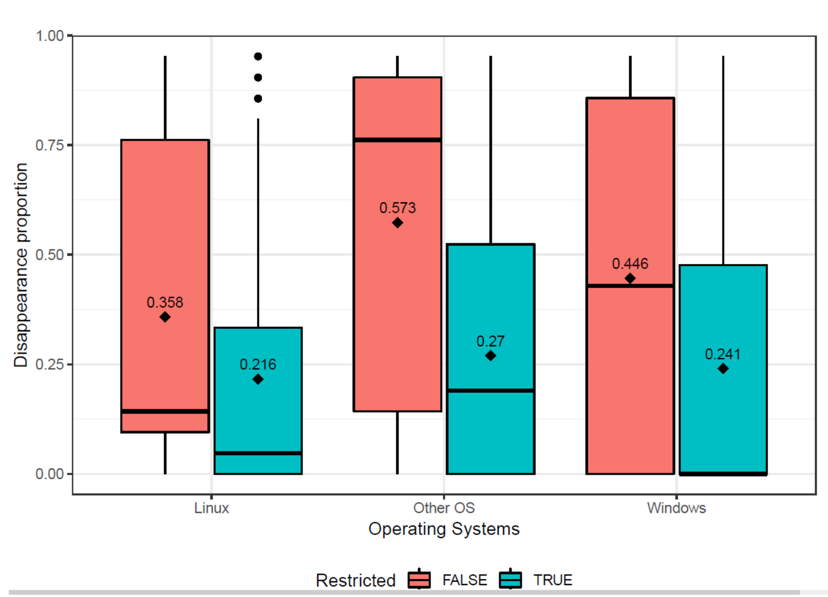
(c) Research-compensate

From\to	Low	Medium	High	Critical
Low	1.0000	0.0000	0.0000	0.0000
Medium	1.0000	0.0000	0.0000	0.0000
High	0.0315	0.9648	0.0037	0.0000
Critical	0.0091	0.0604	0.9305	0.0000

(d) Remediation

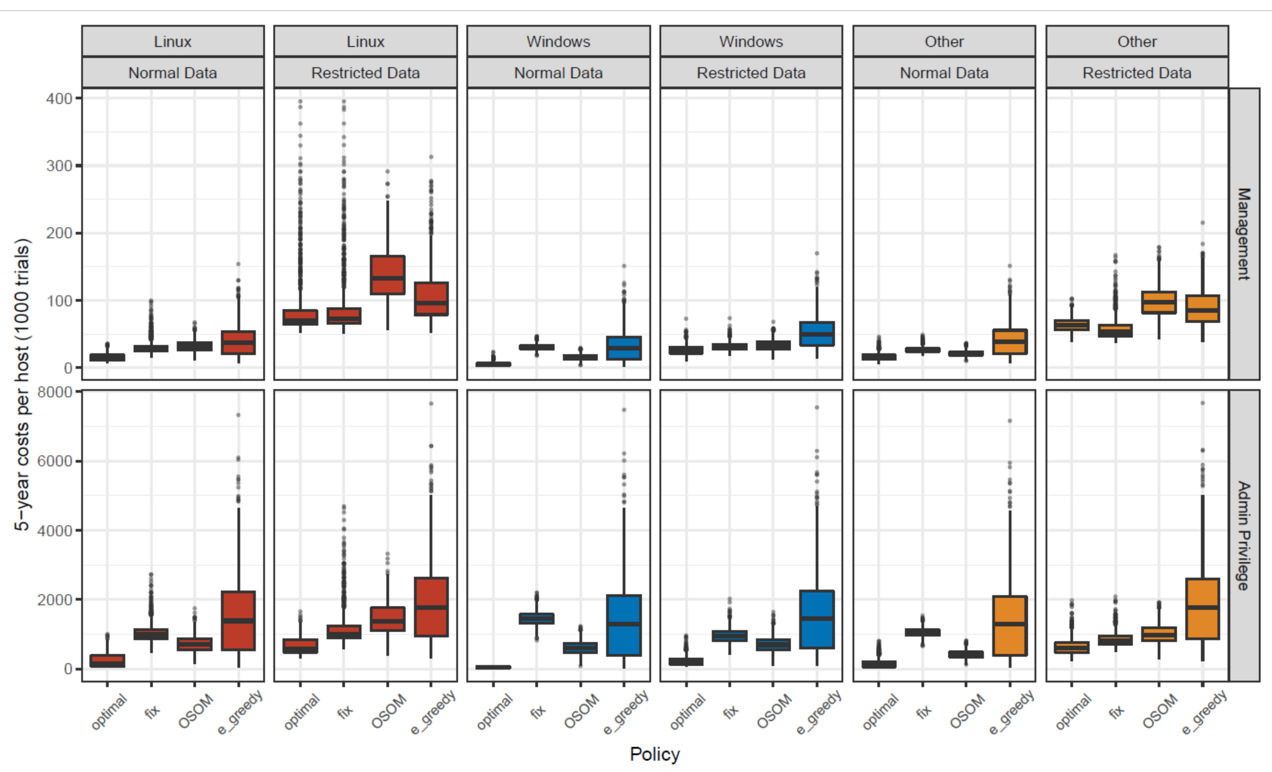
From\to	Low	Medium	High	Critical
Low	0.5000	0.5000	0.0000	0.0000
Medium	0.5000	0.5000	0.0000	0.0000
High	0.5000	0.5000	0.0000	0.0000
Critical	0.5000	0.5000	0.0000	0.0000

Old attempts at complete inspections mostly failed because hosts were turned off



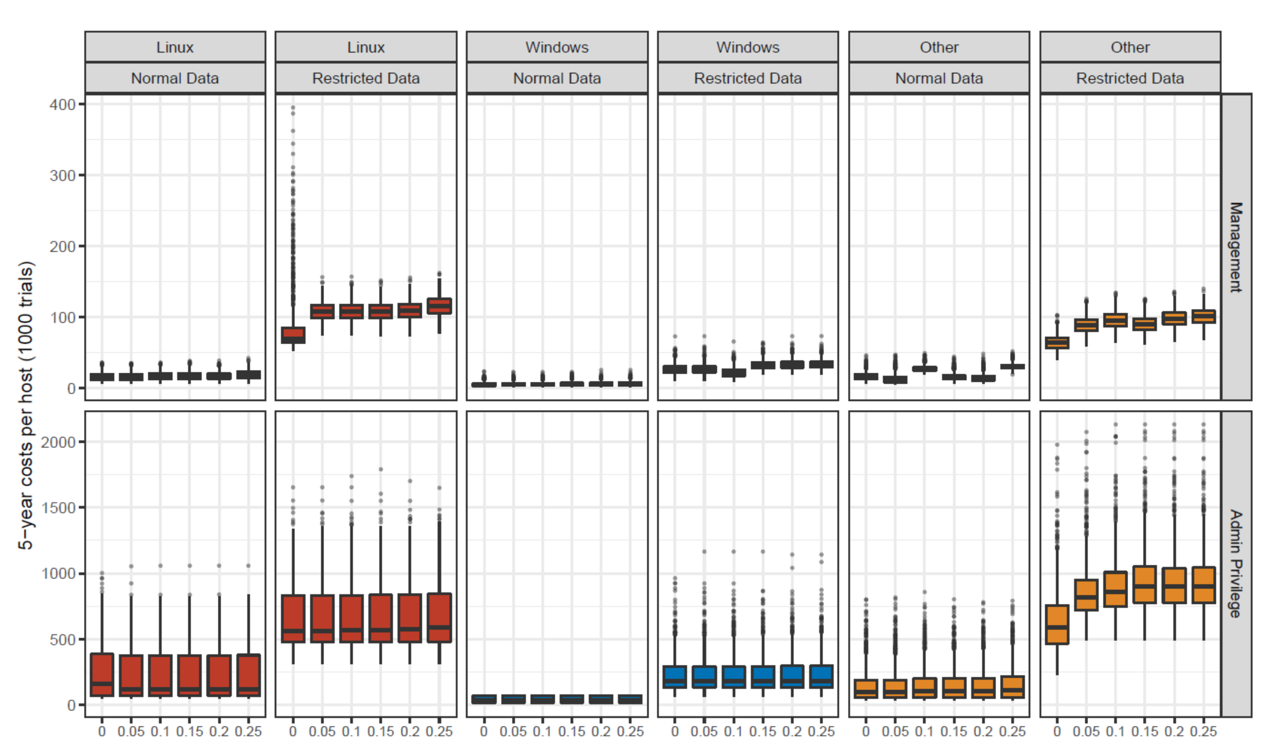
Simulation Permits Alternatives To Be Compared

Out-Of-Sight-Is-Out-Of-Mind Is Expensive

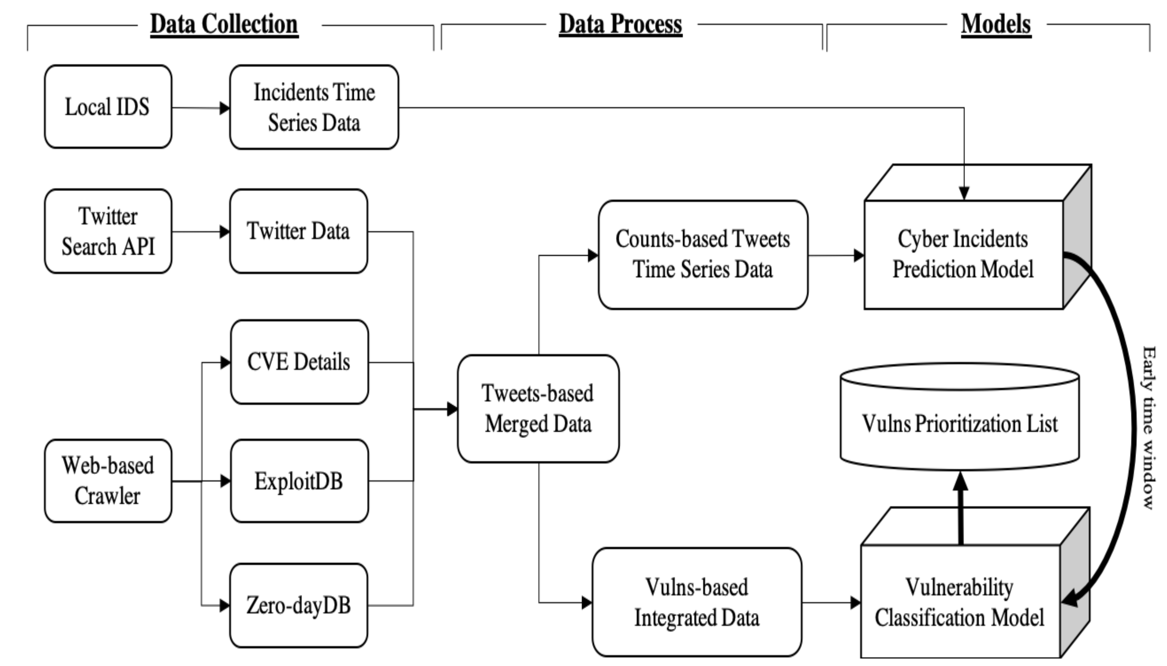


Agent-Based or Optimal Inspection And Control Can Save Millions

A Simple Policy is Almost Optimal

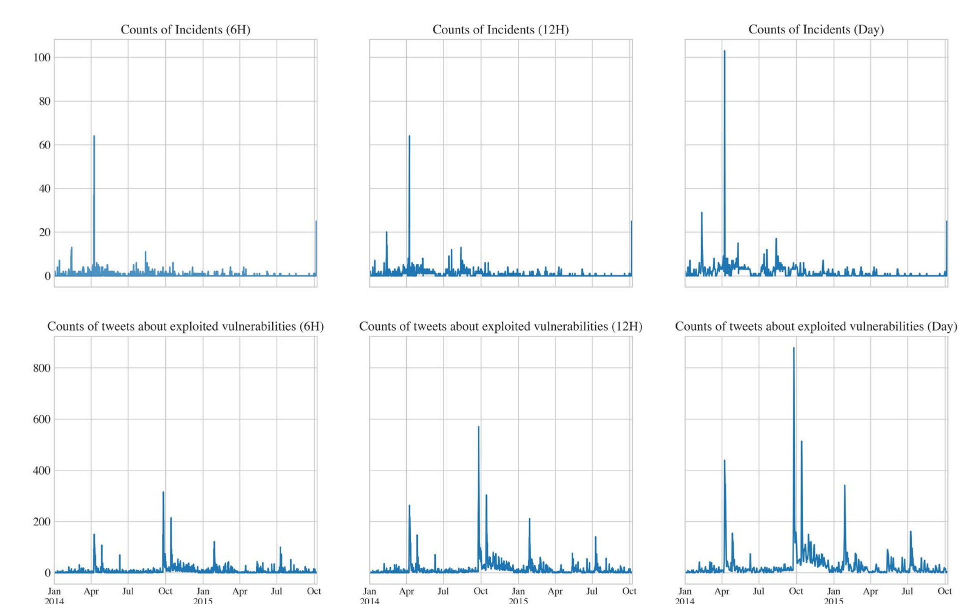


Twitter-Enabled Super-Critical Vulnerability Early Warnings

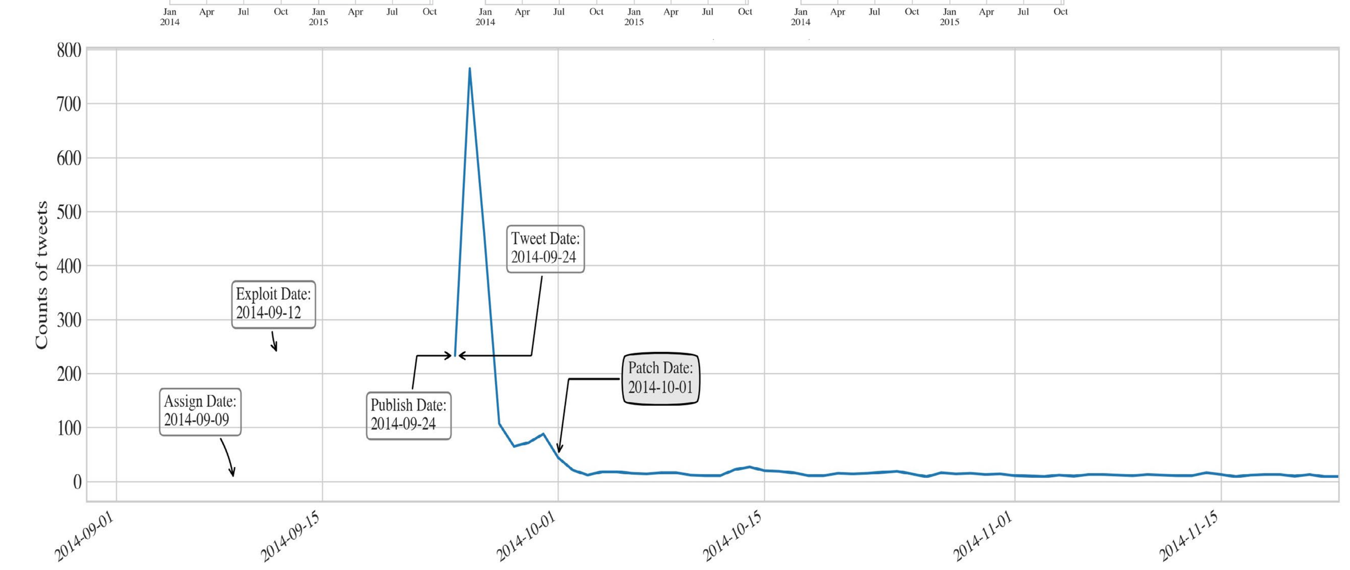


Tweets About Vulnerabilities Correspond

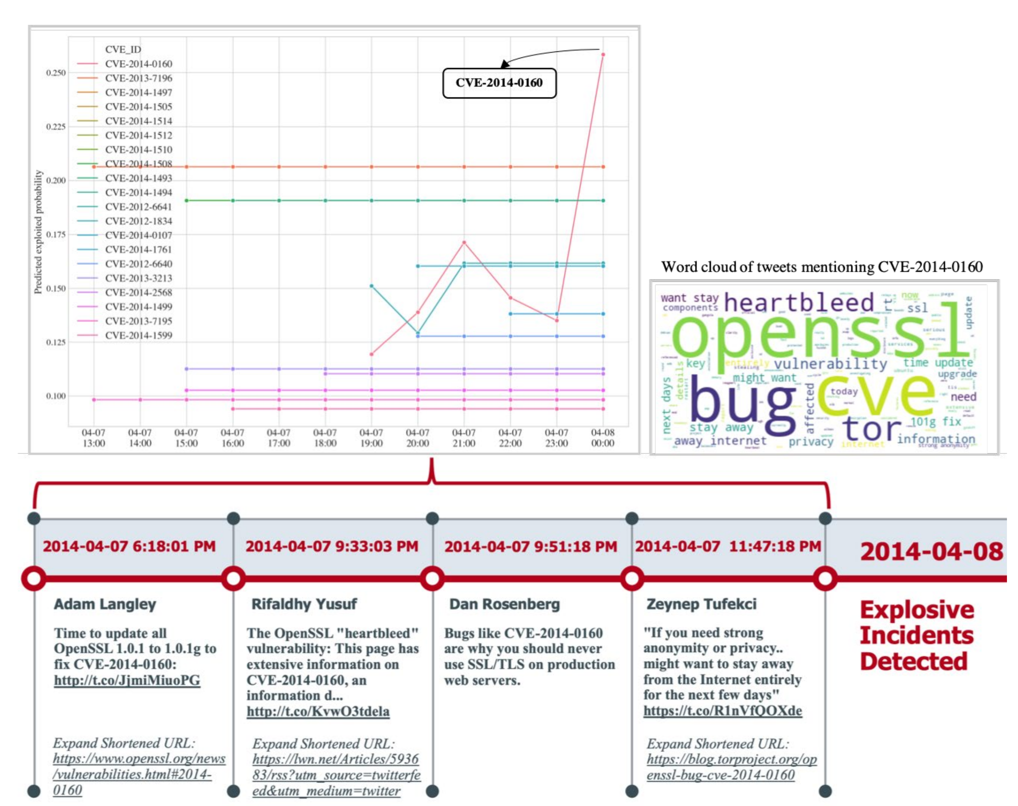
Closely with Compromised Hosts Locally



The Lives of Vulnerabilities Can Be Scrapped Automatically From Multiple Sources



The Probability that An Exploit Exists Is a Good Proxy for Future Celebrity Vulnerabilities



Software Implementations Python and R

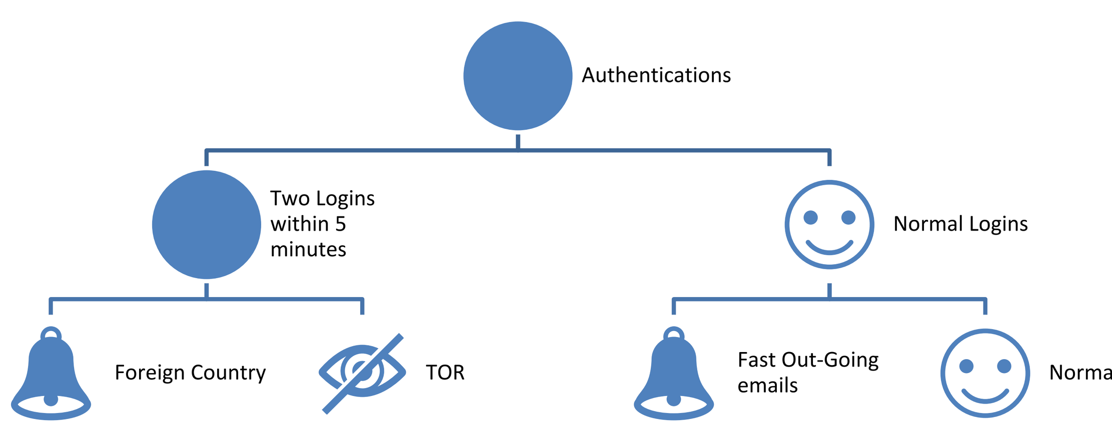
Optimal Trees & Inspection Framework

Optimal Trees with Incomplete Data

$$
\begin{aligned}
\min \quad & \frac{1}{\hat{L}} \sum_{t \in \mathcal{T}_L} L_t + \alpha \sum_{t \in \mathcal{T}_B} d_t \\
\text{s.t.} \quad & L_t \geq N_t - N_{kt} - n(1 - c_{kt}), \quad k = 1, \ldots, K, \quad \forall t \in \mathcal{T}_L, \\
& L_t \leq N_t - N_{kt} + n c_{kt}, \quad k = 1, \ldots, K, \quad \forall t \in \mathcal{T}_L, \\
& L_t \geq 0, \quad \forall t \in \mathcal{T}_L, \\
& N_{kt} = \frac{1}{2} \sum_{i=1}^{n} (1 + Y_{ik}) z_{it}, \quad k = 1, \ldots, K, \quad \forall t \in \mathcal{T}_L, \\
& N_t = \sum_{i=1}^{n} z_{it}, \quad \forall t \in \mathcal{T}_L, \\
& \sum_{k=1}^{K} c_{kt} = l_t, \quad \forall t \in \mathcal{T}_L, \\
& \boldsymbol{a}_m^{\mathsf{T}} \boldsymbol{x}_i \geq b_t - (1 - z_{it}), \quad i = 1, \ldots, n, \quad \forall t \in \mathcal{T}_B, \quad \forall m \in A_R(t), \\
& \boldsymbol{a}_m^{\mathsf{T}} (\boldsymbol{x}_i + \boldsymbol{\epsilon}) \leq b_t + (1 + \epsilon_{\max})(1 - z_{it}), \quad i = 1, \ldots, n, \ \forall t \in \mathcal{T}_B, \quad \forall m \in A \\
& \sum_{t \in \mathcal{T}_L} z_{it} = 1, \quad i = 1, \ldots, n, \\
& z_{it} \leq l_t, \quad \forall t \in \mathcal{T}_L, \\
& \sum_{i=1}^{n} z_{it} \geq N_{\min} l_t, \quad \forall t \in \mathcal{T}_L,
\end{aligned}
$$

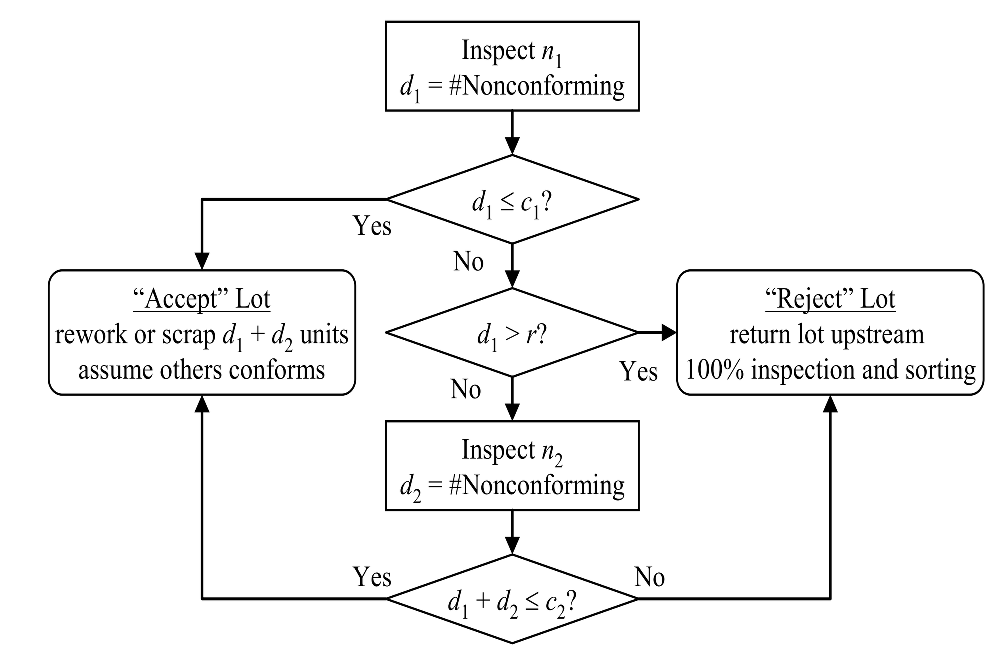
Building on Bertsimas and Dunn (2017)

Statistical Sampling For Marginal Leaves Before Actions



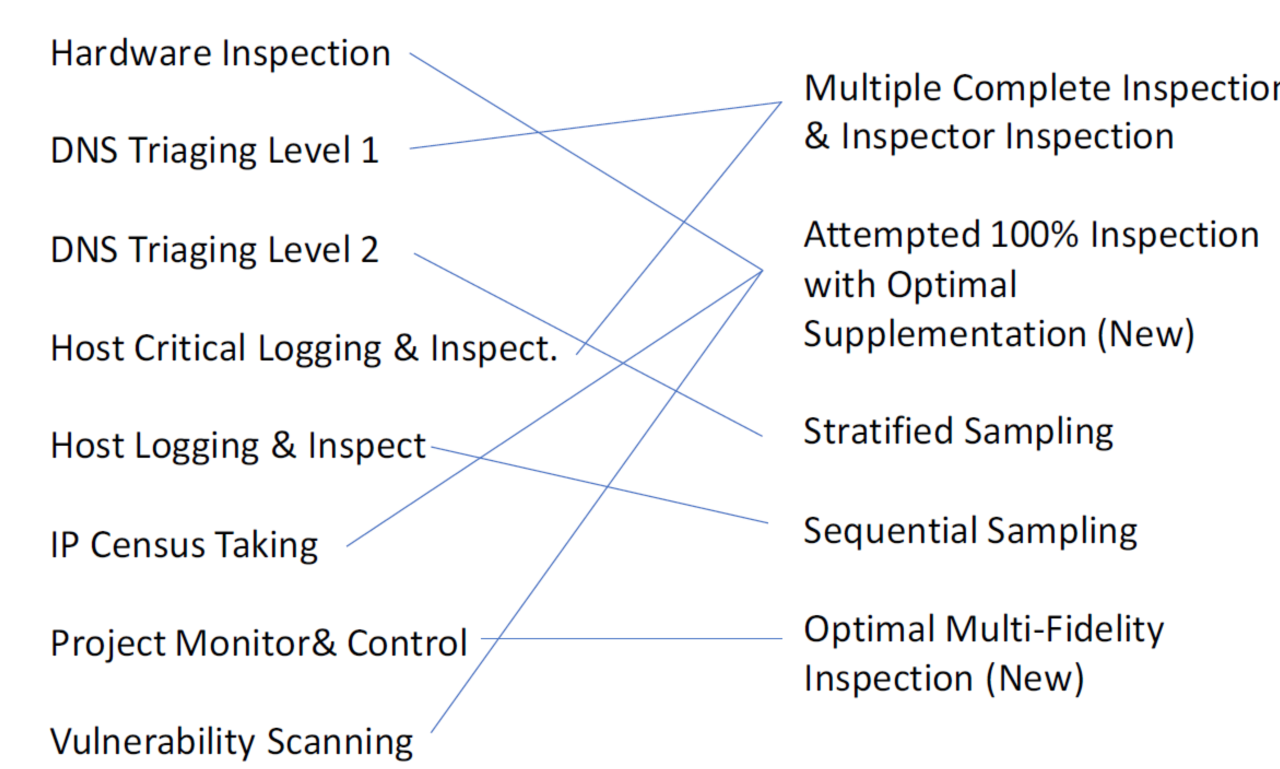
Some Authentication Events Signal that Accounts Should Be Blocked
Others Suggest Further Inspections are Needed

Double Sampling Can Economically Sort Out the Firsts For Marginal Tree Leaves



Hardware Inspections Planned

Triage with Advanced Sampling Incorporated Planned



Liu, E., T. T. Allen, and S. Roychowdhury (in press). Cyber Vulnerability Maintenance Policies That Address the Incomplete Nature of Inspection. *Applied Stochastic Models in Business & Industry*.