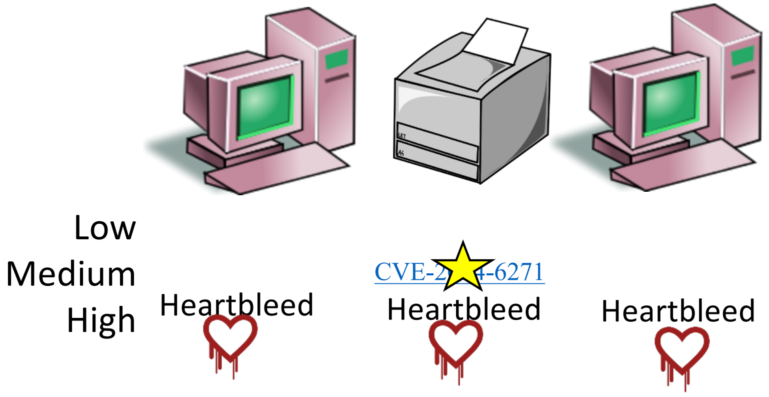
Data-Driven Cyber Vulnerability Maintenance

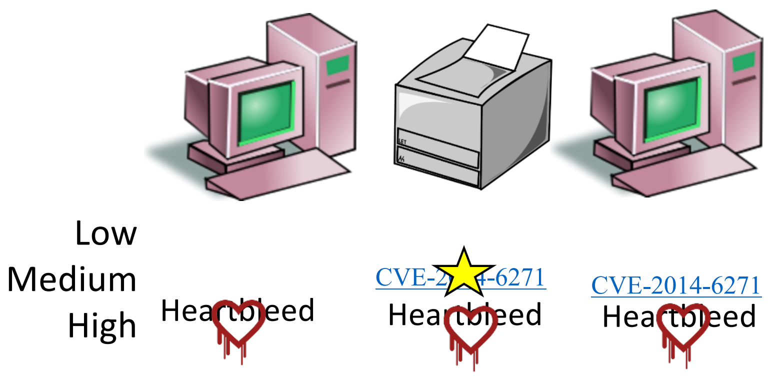
Theodore T. Allen, Ph.D. (Ted) Associate Professor

Integrated Systems Engineering



Description of Use Cases

In our 2014 data set over 91% of intrusions exploit known vulnerabilities. 90% is often quoted.



Personnel and Tests

Fixes, Insurance, Losses

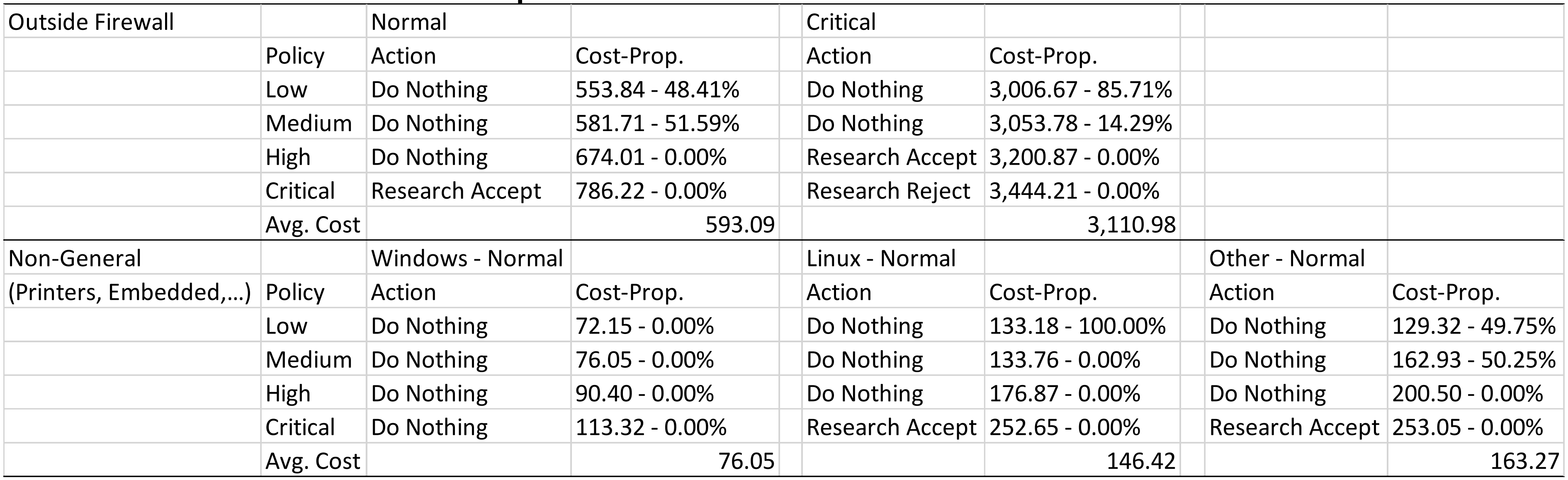
Min: Expected[Repair Cost + Intrusion Cost]

Common Vulnerability Scoring System (CVSS) Score is a number 0-10.

- Host differ by outside of the firewall, non-general, inside unmanaged, managed, and critical servers
- 30,000 host scan data for 22 months and incident data also, expected discounted sum of costs

Description of Use Cases: Firewalls & Not- General

- Firewall: Do not accept risk on critical vulnerabilities even for 1 month

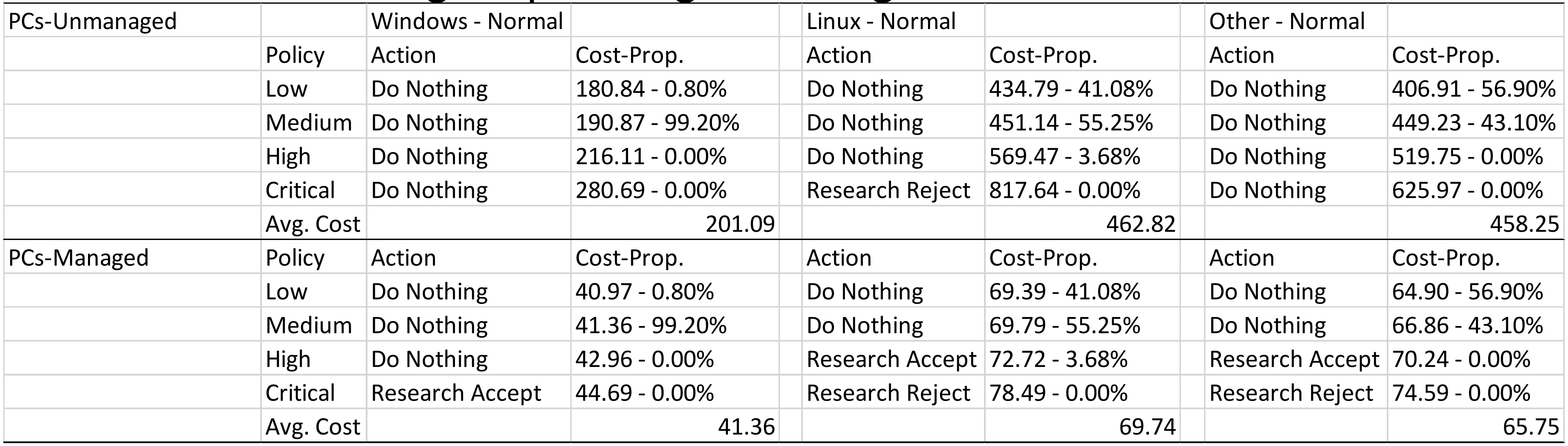


Outside Firewall		Normal		Critical				
	Policy	Action	Cost-Prop.	Action	Cost-Prop.			
	Low	Do Nothing	553.84 - 48.41%	Do Nothing	3,006.67 - 85.71%			
	Medium	Do Nothing	581.71 - 51.59%	Do Nothing	3,053.78 - 14.29%			
	High	Do Nothing	674.01 - 0.00%	Research Accept	3,200.87 - 0.00%			
	Critical	Research Accept	786.22 - 0.00%	Research Reject	3,444.21 - 0.00%			
	Avg. Cost		593.09		3,110.98			
Non-General		Windows - Normal		Linux - Normal			Other - Normal	
(Printers, Embedded,…)	Policy	Action	Cost-Prop.	Action	Cost-Prop.		Action	Cost-Prop.
	Low	Do Nothing	72.15 - 0.00%	Do Nothing	133.18 - 100.00%		Do Nothing	129.32 - 49.75%
	Medium	Do Nothing	76.05 - 0.00%	Do Nothing	133.76 - 0.00%		Do Nothing	162.93 - 50.25%
	High	Do Nothing	90.40 - 0.00%	Do Nothing	176.87 - 0.00%		Do Nothing	200.50 - 0.00%
	Critical	Do Nothing	113.32 - 0.00%	Research Accept	252.65 - 0.00%		Research Accept	253.05 - 0.00%
	Avg. Cost		76.05		146.42			163.27

- Research accept – try to patch but do nothing if no patch is available.
- Research reject – try to patch and remediate if no patch is available.

Description of Use Cases: PCs

- Consider backing off patching unmanaged hosts without critical data



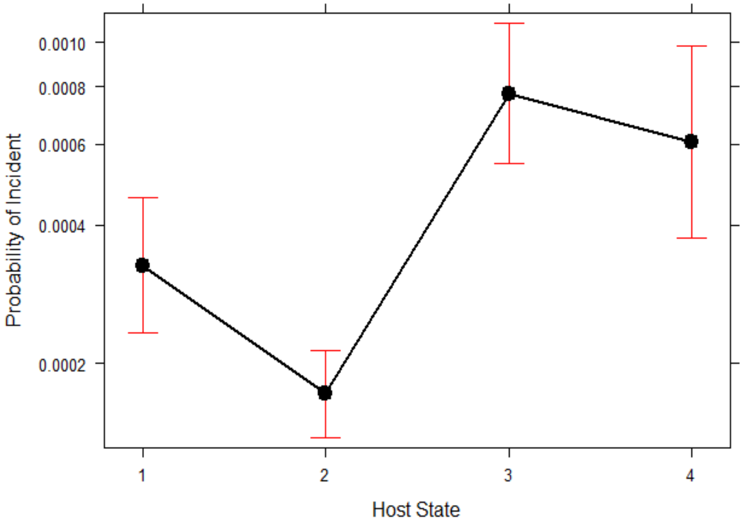
PCs-Unmanaged		Windows - Normal			Linux - Normal			Other - Normal	
	Policy	Action	Cost-Prop.		Action	Cost-Prop.		Action	Cost-Prop.
	Low	Do Nothing	180.84 - 0.80%		Do Nothing	434.79 - 41.08%		Do Nothing	406.91 - 56.90%
	Medium	Do Nothing	190.87 - 99.20%		Do Nothing	451.14 - 55.25%		Do Nothing	449.23 - 43.10%
	High	Do Nothing	216.11 - 0.00%		Do Nothing	569.47 - 3.68%		Do Nothing	519.75 - 0.00%
	Critical	Do Nothing	280.69 - 0.00%		Research Reject	817.64 - 0.00%		Do Nothing	625.97 - 0.00%
	Avg. Cost		201.09			462.82			458.25
PCs-Managed	Policy	Action	Cost-Prop.		Action	Cost-Prop.		Action	Cost-Prop.
	Low	Do Nothing	40.97 - 0.80%		Do Nothing	69.39 - 41.08%		Do Nothing	64.90 - 56.90%
	Medium	Do Nothing	41.36 - 99.20%		Do Nothing	69.79 - 55.25%		Do Nothing	66.86 - 43.10%
	High	Do Nothing	42.96 - 0.00%		Research Accept	72.72 - 3.68%		Research Accept	70.24 - 0.00%
	Critical	Research Accept	44.69 - 0.00%		Research Reject	78.49 - 0.00%		Research Reject	74.59 - 0.00%
	Avg. Cost		41.36			69.74			65.75

- Manually patch or remediate Linux critical vulns. if no patch is available
- $160, $400, $400 as lifetime maintenance savings per host managed.

Description of Cases: Critical Servers

- Critical servers → expensive incidents making big maintenance costs

Critical Servers	Policy	Action	Cost-Prop.
	Low	Do Nothing	2,582.70 - 100.00%
	Medium	Research Accept	2,742.93 - 0.00%
	High	Research Accept	3,023.48 - 0.00%
	Critical	Research Reject	3,267.99 - 0.00%
	Avg. Cost		2,810.30

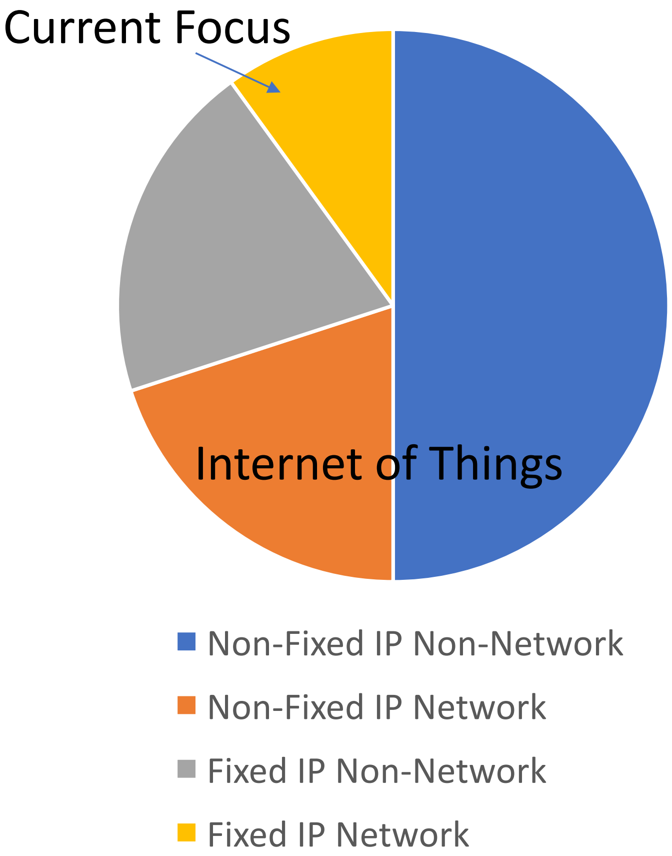


- Patching medium vulnerabilities is advised.
- Remediating critical vulnerabilities with no patches is advised.

Non-Fixed IP (Phones, laptops,…) and Policy

- Create a list of cell phones and laptops
- Use smart sampling to select hosts for vulnerability scanning
- Scan hosts and inspect for incidents
- Develop optimal scanning and maintenance policy

- Future: Closed loop control with scans and patching actions or tickets



Current Focus

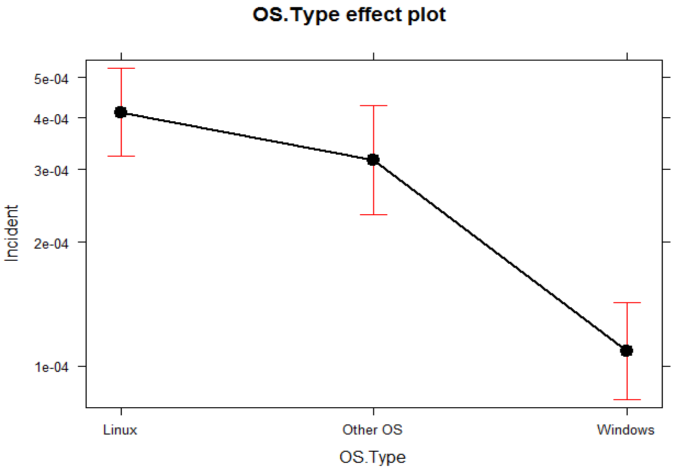
Internet of Things

Pilots deployed to date and level of support

Description	Date Started	Date Results	Commitment
Firewalls,…,Non-General	April 2017	October 2017	≤ 65 buildings
PCs: Unmanaged…	April 2017	October 2017	≤ 65 buildings
Critical Servers	April 2017	October 2017	≤ 65 buildings
Sampling non-fixed IPs	April 2017	October 2017	1 department
Automatic control	Not yet	Not yet	1 department

- General lack of willingness to ignore high and critical vulnerabilities.
- Willingness to patch selected mediums.
- Willingness to remediate or manually patch selected vulnerabilities with no patches

Operational technical requirements: OS, integration with current software, etc.



Vulnerability Policy

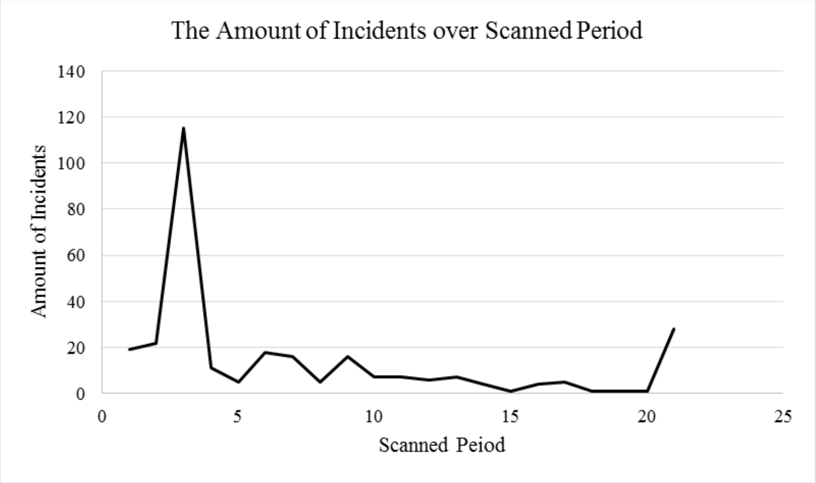
- Firewall,…,PC,…critical server policy…likely immediately relevant
- Ideally: Local vulnerability scan and incident data → Tailored policy
- Want: Aggregate data to measure success

Non-Fixed IP Sampling

- Need: List and staff willingness to bring in phones & laptops for scans

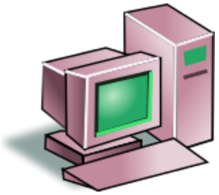
Closed Loop Control

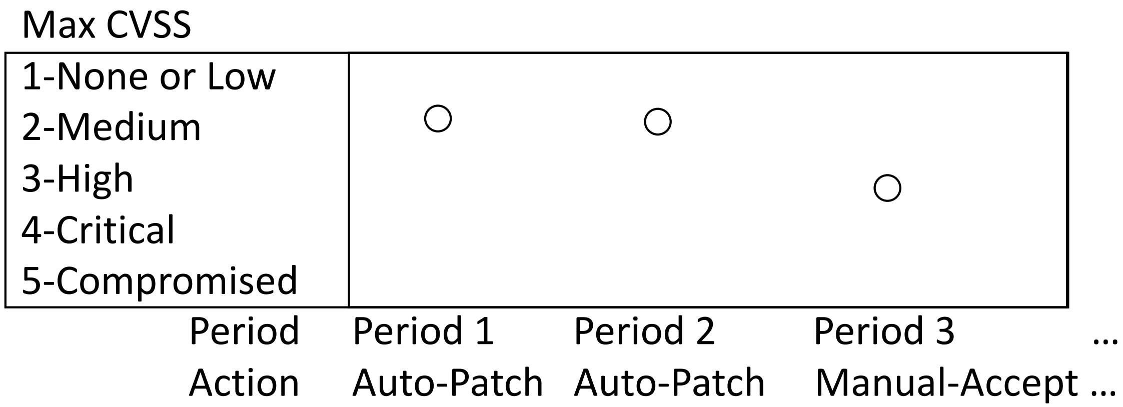
- Want: Management software API for closed loop control



Questions?

Host Evolution





Max CVSS

1-None or Low
2-Medium
3-High
4-Critical
5-Compromised

Period	Period 1	Period 2	Period 3	…
Action	Auto-Patch	Auto-Patch	Manual-Accept	…

Act=(1,0)		Low -1	Med-M2	High-3	Critical-4	Attack-5
Auto-Patch	Low-1	48504	402	11	5	15
Only	Med-2	317	49030	244	132	96
	High-3	1	25	214	1	9
	Critical-4	0	9	1	67	4
	Attack-5	15	62	4	5	11

Data Driven Markov Decision Processes (DDMDP)

$$Y_t|Y_{t-1}, a_{t-1}, \mathbf{p}_{(k)}^{a_{t-1}}, (k) \sim Multinomial[Row_{Y_{t-1}}(\mathbf{p}_{(k)}^{a_{t-1}})]$$

Additional expectation as compared with MDP

$$\max_{\mathbf{x}_1,\ldots,\mathbf{x}_{H-1}} \sum_{k=1}^{q} P(k) E_{Y_1,Y_2,\ldots,Y_H}[\sum_{t=1}^{H-1} \gamma^{t-1} r^{a_t|\mathbf{x}_t}_{Y_t|\mathbf{p}_{(k)}^{a_t}, Y_{t+1}|\mathbf{p}_{(k)}^{a_{t-1}}, \theta_{t-1}, (k)} + \gamma^{H-1} r^0_{Y_H}].$$

- Delage and Mannor (2010) OR problem is “intractable” and proposed approximate methods (hierarchical model).