

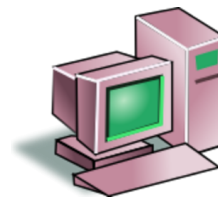
# Data-Driven Cyber Vulnerability Maintenance



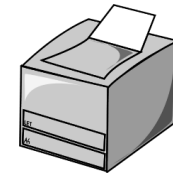
Theodore T. Allen, Ph.D.  
(Ted) Associate Professor  
(Cathy Xia, Gagan Agrawal,  
Rajiv Ramnath, Enhao Liu,  
Tianyu Jaing)

Integrated Systems  
Engineering

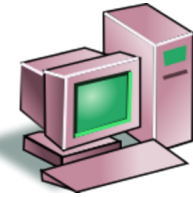
Low  
Medium  
High



Heartbleed  

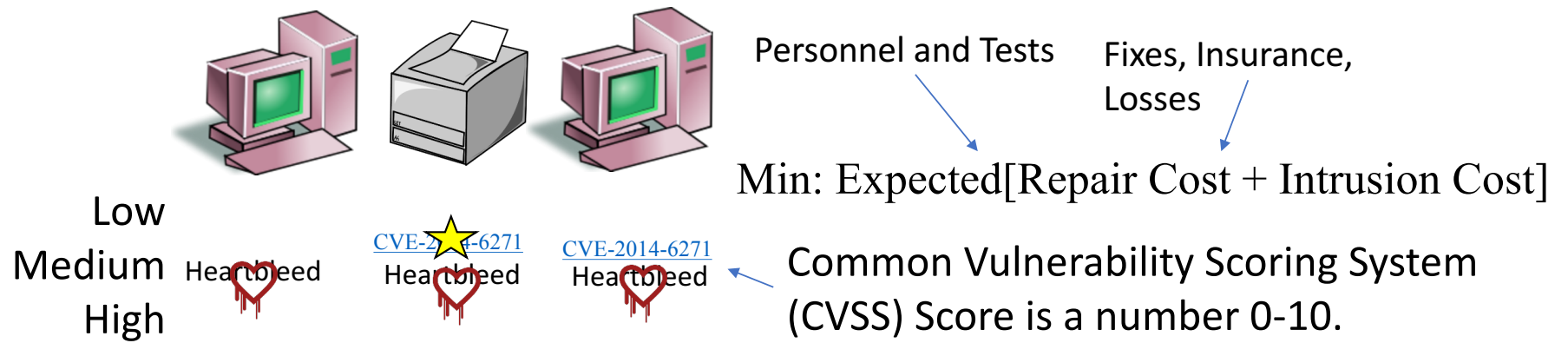
[CVE-2014-016271](#)  
Heartbleed  

Heartbleed  


# Description of Use Cases: Data Set

In our 2014 data set over 91% of warnings/"incidents" were on hosts with medium or higher vulnerabilities. It is often 90+% of incidents exploit known vulnerabilities.

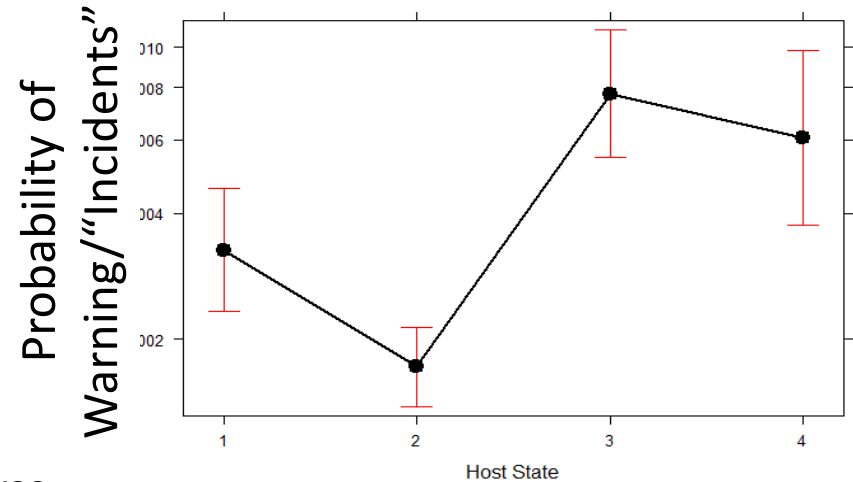


- Host differ by outside of the firewall, non-general, inside administrator privilege, restricted privilege, and critical servers
- 30,000+ host nessus scan data for 22 months and warning/"incident" data also, expected discounted sum of costs

# Description of Cases: Analysis

## Assumptions

- Host state is the level of the worst vulnerability.
- \$150 on average vulnerability investigation/patching
- \$2,000 for warning on non-critical server
- \$10,000 for warning on critical server
- Conservative: Some incidents not included, just IDS warnings (usually data going out, black-listed IPs, IP data,...260)
- Estimated life costs are underestimates.
- If you have <10 hosts in your unit with the same OS and vulns, the local operator likely has administrator privilege.
- Ordinary Markov Decision Process and...



## Max CVSS

1-None or Low				
2-Medium	○	○		
3-High			○	
4-Critical				
5-Compromised				
	Period 1	Period 2	Period 3	...
	Auto-Patch	Auto-Patch	Manual-Accept ...	

## Description of Use Cases: Firewalls

Outside Firewall	Policy	Normal Action	Cost (\$) - Proportion	Critical Action	Cost (\$) - Proportion
	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 Compen	3,444.21 - 0.00%
	Avg. Cost		593.09		3,110.98

- Research accept – try to patch but do nothing if no patch is available.
- Research compensate – try to patch and remediate if no patch is available.
- Ask 1: For critical firewalls, do not risk accept critical vulnerabilities (already common)

# Non- General

- Ask 1: Consider granting long term acceptance for non-general devices not associated with critical data (1 warning/“incident ” over 22 months).

Non-General		Windows - Normal	
(Printers, Embedded,...)	Policy	Action	Cost (\$)-Proportion
	Low	Do Nothing	72.15 - 0.00%
	Medium	Do Nothing	76.05 - 0.00%
	High	Do Nothing	90.40 - 0.00%
	Critical	Do Nothing	113.32 - 0.00%
	Avg. Cost		76.05

Linux - Normal		Other - Normal	
Action	Cost (\$)-Proportion	Action	Cost (\$)-Proportion
Do Nothing	133.18 - 100.00%	Do Nothing	129.32 - 49.75%
Do Nothing	133.76 - 0.00%	Do Nothing	162.93 - 50.25%
Do Nothing	176.87 - 0.00%	Do Nothing	200.50 - 0.00%
Research Accept	252.65 - 0.00%	Research Accept	253.05 - 0.00%
	146.42		163.27

# Description of Use Cases: PCs

PCs-		Windows - Normal		Linux - Normal		Other - Normal	
Administrator	Policy	Action	Cost (\$) - Proportion	Action	Cost (\$) - Proportion	Action	Cost (\$) - Proportion
Privilege	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 Compen	817.64 - 0.00%	Do Nothing	625.97 - 0.00%
	Avg. Cost		201.09		462.82		458.25
PCs-No Privilege	Policy	Action	Cost (\$) - Proportion	Action	Cost (\$) - Proportion	Action	Cost (\$) - Proportion
	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 Compen	78.49 - 0.00%	Research Comper	74.59 - 0.00%
	Avg. Cost		41.36		69.74		65.75

- Consider backing off administrator privilege hosts without critical data
- Ask 1: Reduced administrator privilege granting \$160, \$400, and \$400 are est. lifetime maintenance costs for unique hosts over non-unique.
- Ask 2: Manually patch or remediate Linux critical vulns. if no patch...

## Description of Cases: Critical Servers

- Critical servers → expensive incidents making big maintenance costs

Critical Servers	Policy	Action	Cost (\$) - Proportion
	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 Compensa	3,267.99 - 0.00%
	Avg. Cost		2,810.30

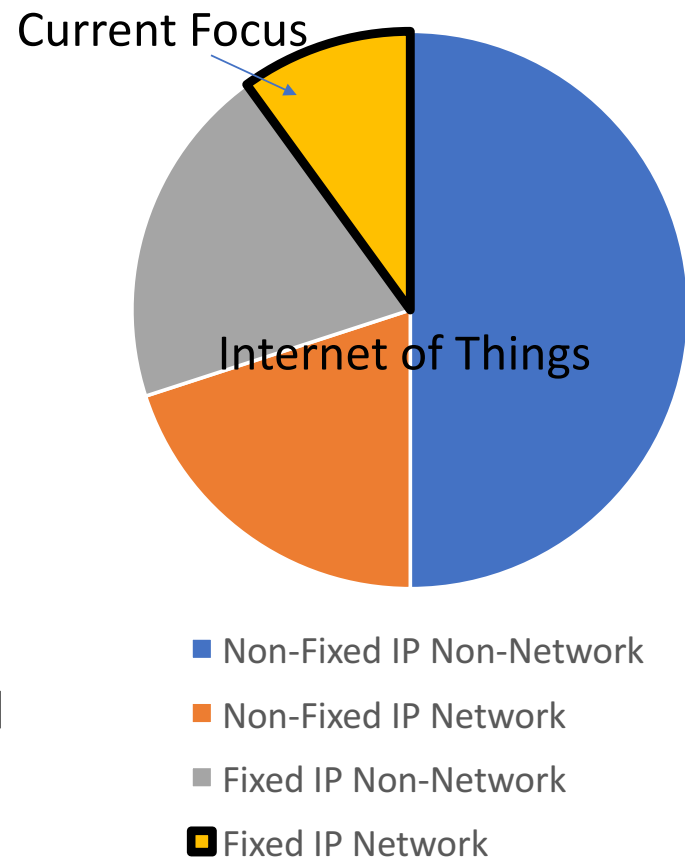
- Big Ask: Patching medium vulnerabilities is advised.
- Ask: Remediating critical vulnerabilities with no patches is advised.

# 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

Ask: Collaboration and expertise related to non-Fixed IP address vulnerability sampling, incident clarifications, and control

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





## Pilots deployed to date and level of support

Description	Summary	Date Started	Date Results	Commitment
Firewalls,...,Non-General	Ask 1: Tighten crits. comps. Ask 2: Loosen non-generals.	April 2017	October 2017	≤ 65 buildings
PCs: Admin. Priv....	Ask 1: Grant fewer privileges. Ask 2: Non-windows crits.	April 2017	October 2017	≤ 65 buildings
Critical Servers	Big Ask: Res. accept meds.	April 2017	October 2017	≤ 65 buildings
Sampling non-fixed IPs	Welcome collaboration.	Not yet	Not yet	1 department
Automatic control	Welcome collaboration.	Not yet	Not yet	1 department

- General lack of willingness to ignore high and critical vulnerabilities.
- Willingness to remediate critical vulnerabilities faster.
- Some willingness to patch selected mediums.
- If you interested in changing practices, please contact [allen.515@osu.edu](mailto:allen.515@osu.edu).

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

### Vulnerability Policy

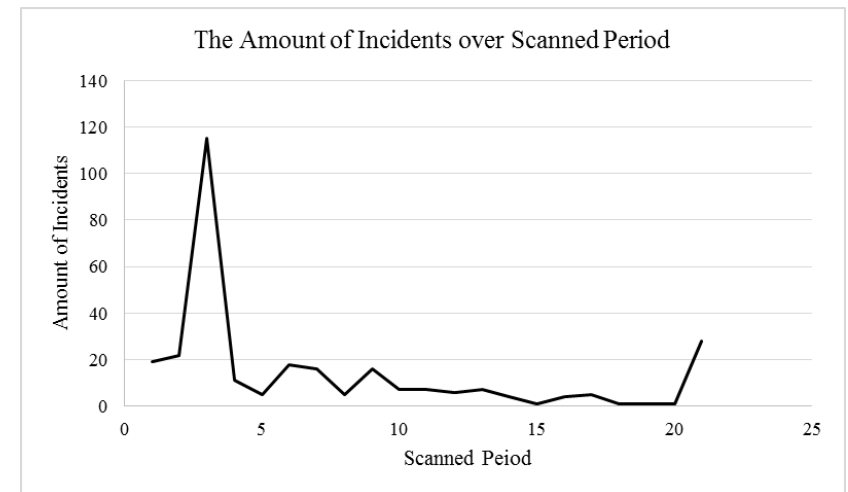
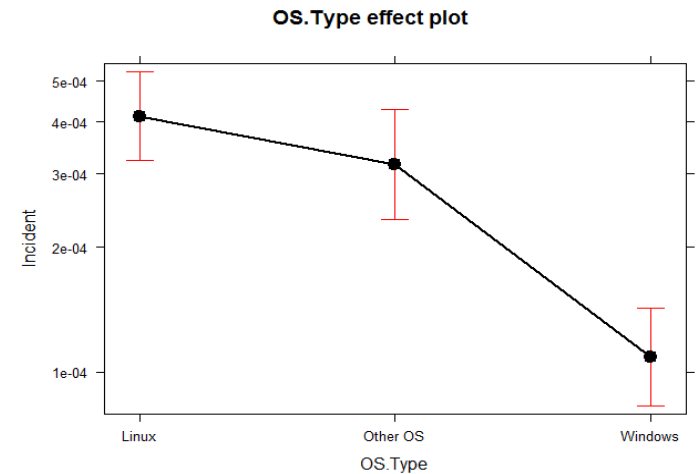
- Firewall,...,PC,...critical server policy...likely immediately relevant
- Ideally: Local vulnerability scan and incident data → Tailored policy
- Want: Aggregate data to measure success

### 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?

## Data Driven Markov Decision Processes (DDMDP)

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

Additional expectation as compared with MDP

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

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