



# Metrics for V&V of Cyber defenses

Martin S. Feather, Joel M. Wilf, Joseph Priest

© 2013 California Institute of Technology.  
Government sponsorship acknowledged.

This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

# Acknowledgements

## JPL's Cyber Defense Research Initiative

- Kymie Tan, *Principal Investigator*
- Robert Vargo, *Initiative Leader*
- Bryan Johnson
- Frank Kuykendall
- DJ Byrne
- Chris Dorros
- Ed Silber
- David Foor

# Motivation for cyber defense

## ASSUMPTION:

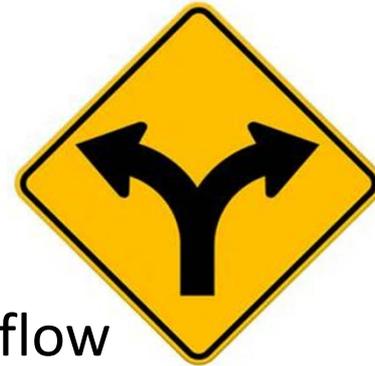
*you already agree that  
cyber threats are a **serious risk***

LIKELIHOOD	5 – Near certain	Green	Yellow	Red	Red	Red
	4 – Highly likely	Green	Yellow	Yellow	Red	Red
	3 – Likely	Green	Yellow	Yellow	Yellow	Red
	2 – Low Likelihood	Green	Green	Green	Yellow	Yellow
	1 – Not Likely	Green	Green	Green	Green	Yellow
		1	2	3	4	5
		CONSEQUENCE				Loss of Mission

*Likelihood hard to estimate but there are known to have been cyber penetrations of space assets*

# Problem

- Context: Contemplating introducing a cyber defense into a flight project environment (development or operations)
- Question: *should it be deployed?*
- Approach to answering:
  - Adaptation of a traditional V&V workflow
  - Collection & presentation of appropriate metrics
  - Help inform deployment decision



# Context for this work

JPL's Cyber Defense Research Laboratory

GOAL: “To develop, evaluate and validate cyber defensive architectures and mitigations for JPL missions in a controlled environment and in the presence of attacks”

FEATURE: a sandboxed computing environment in which security tests and experiments can be run without risk of damage to production systems

# Cyber defense concerns

- Costs



- Benefits



- Risks



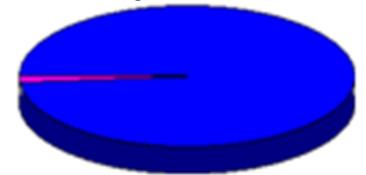
Take all these into account  
when gauging its acceptability – trade-offs involved

# Cyber defense concerns - Costs

- Budgetary
  - Purchases and license fees
  - Labor costs
    - Installing and maintaining the defense
    - Operating the defense (e.g., helpdesk, sysadmin)
    - Trainer and trainee costs of mastering the defense
- Computational
  - CPU, memory, filespace, bandwidth  
(acceptability will depend on unused capacity)
- User Inconvenience
  - Extra user steps
  - Decreased usability / curtailed capabilities
  - Interruptions/interference (e.g., from false positives)



Used space: 1.91 GB  
Freespace: 320 KB



# Cyber defense concerns - Benefits



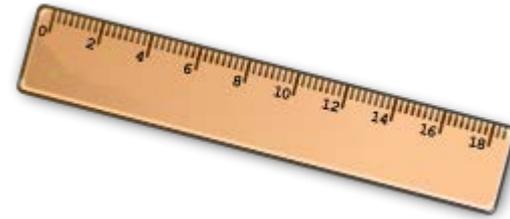
- Nature of defense
  - Prevention – inhibits steps of cyber attack(s)
  - Detection (and the kind of response it leads to)
  - Recovery – assists in recovering after a cyberattack
  - ❖ Logging for forensics later
- Additional security (if any)
  - While designed for one kind of attack, helps against others
- Efficacy
  - Sensitivity & specificity
    - Don't miss attacks (“false negatives”)
    - Don't generate false alarms (“false positives”)
  - Responsiveness (limits the time/extent of attack)
- Additional benefits (if any)
  - E.g., cleanup leading to less downtime, faster normal processing

# Cyber defense concerns – Risks

- Vulnerabilities
  - New or increased “attack surface”
  - Impede or undermine other defenses
- Critical interference
  - Under some circumstances (e.g., off-nominal):  
minor inconvenience escalates to major impediment



# Assessment



Field candidate defense in operational environment and measure its costs, benefits and risks?

**NO!!!!!!!!!!!!!!!**



# Assessment

Field candidate defense in “sandboxed” test environment and measure its costs, benefits and risks?

YES!

- Safe – isolated from institutional network so malware cannot escape
- Non-disruptive to ongoing operations
- Repeatable experimentation



# Fidelity of test environment



“Test like you fly, fly like you test”

- Many “confounders” of test fidelity
  - Fewer computational resources (CPUs, routers, ...)
  - Fewer users and applications; lack of true usage profiles
  - Short-lived duration of tests
  - Subset of full computational milieu
    - Networks
    - Firewalls
    - Other security controls
  - Virtualization perhaps not reflective of operational environment

# Analogy with space testing

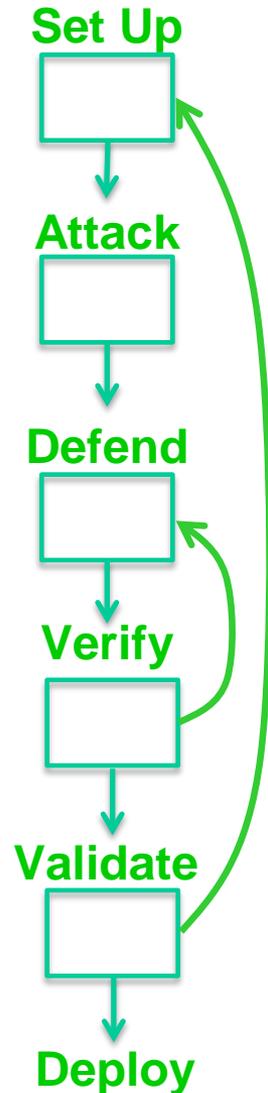
*“The lunar environment cannot be sufficiently emulated on Earth, therefore system verification testing will rely to some extent on extension by analysis and ultimate testing in the field (lunar operations).”*

[P. Craven, N. Ramachandran, J. Vaughn, T. Schneider & M. Nehls. “Test Before You Fly – High Fidelity Planetary Environment Simulation”, Global Space Exploration Conference (GLEXP), 2012.]

- Experiment in test environment to take measures
- Analyze & extrapolate to operational environment
- If confident, deploy to operational environment
  - Maybe test there
  - Probationary period
  - Subsequent monitoring

# V&V workflow

- **Set Up**: configure test environment
- **Attack**: take measurements as cyber-attack is conducted in test environment
- **Defend**: develop & deploy defense in test environment, take measurements during no attack, and during attack
- **Verify**: with real users, extrapolate measurements to infer effects in operational environment; assess acceptability
- **Validate**: Carefully (and reversibly!) field in operational environment
- **Deploy**: commit defense to use



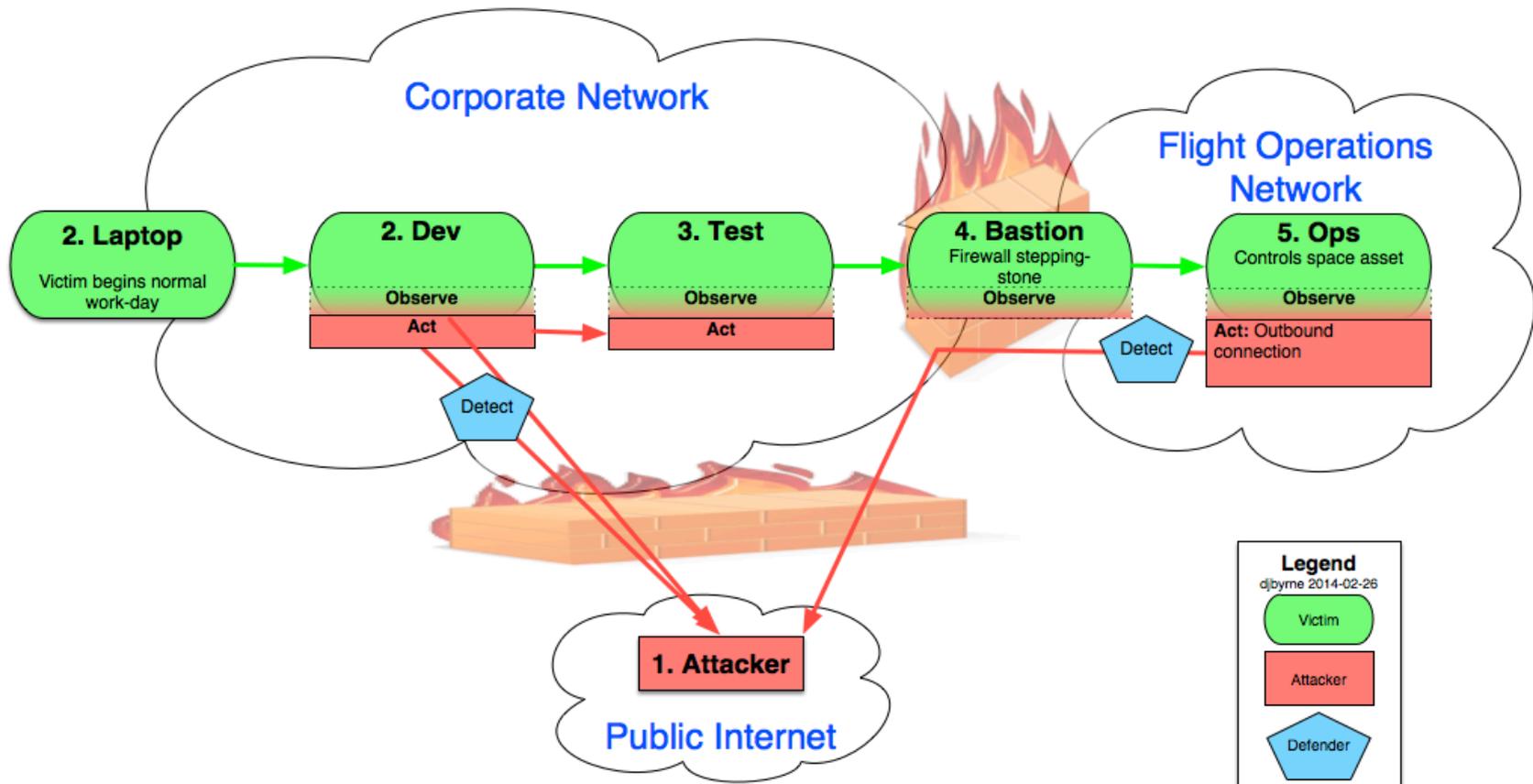
A RUNNING **EXAMPLE** MAY HELP...



# “Reconnaissance attack”



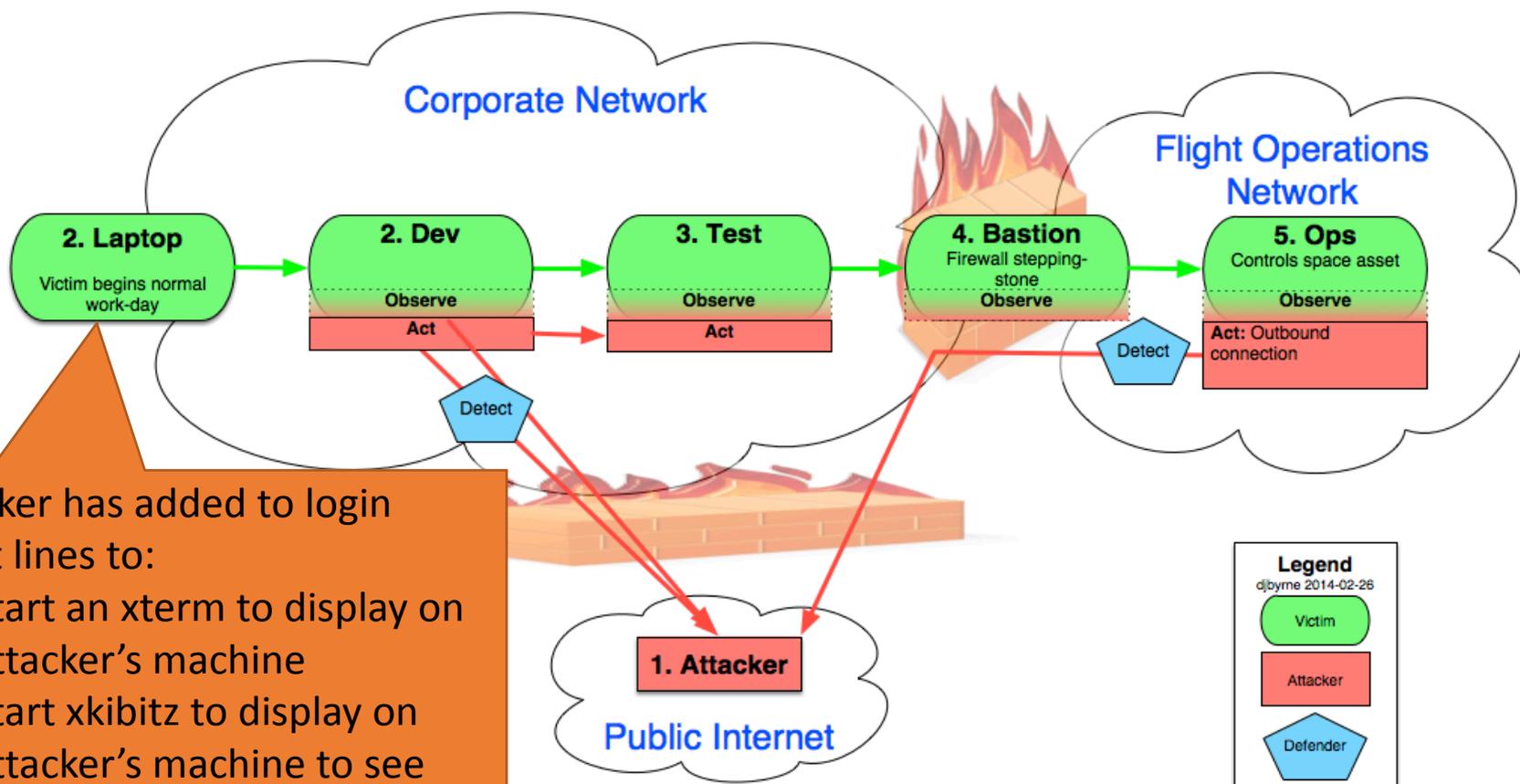
D.J. Byrne, D. Morgan, K. Tan, B. Johnson and C. Dorros, “*Cyber Defense of Space-Based Assets: Verifying and Validating Defensive Designs and Implementations*”, Conference on Systems Engineering Research (CSER 2014) *Procedia Computer Science*, 28 (2014), 522-530



# “Reconnaissance attack”



**Initial breach:** attacker has had brief access to victim’s home directory (multiple plausible ways this could occur)



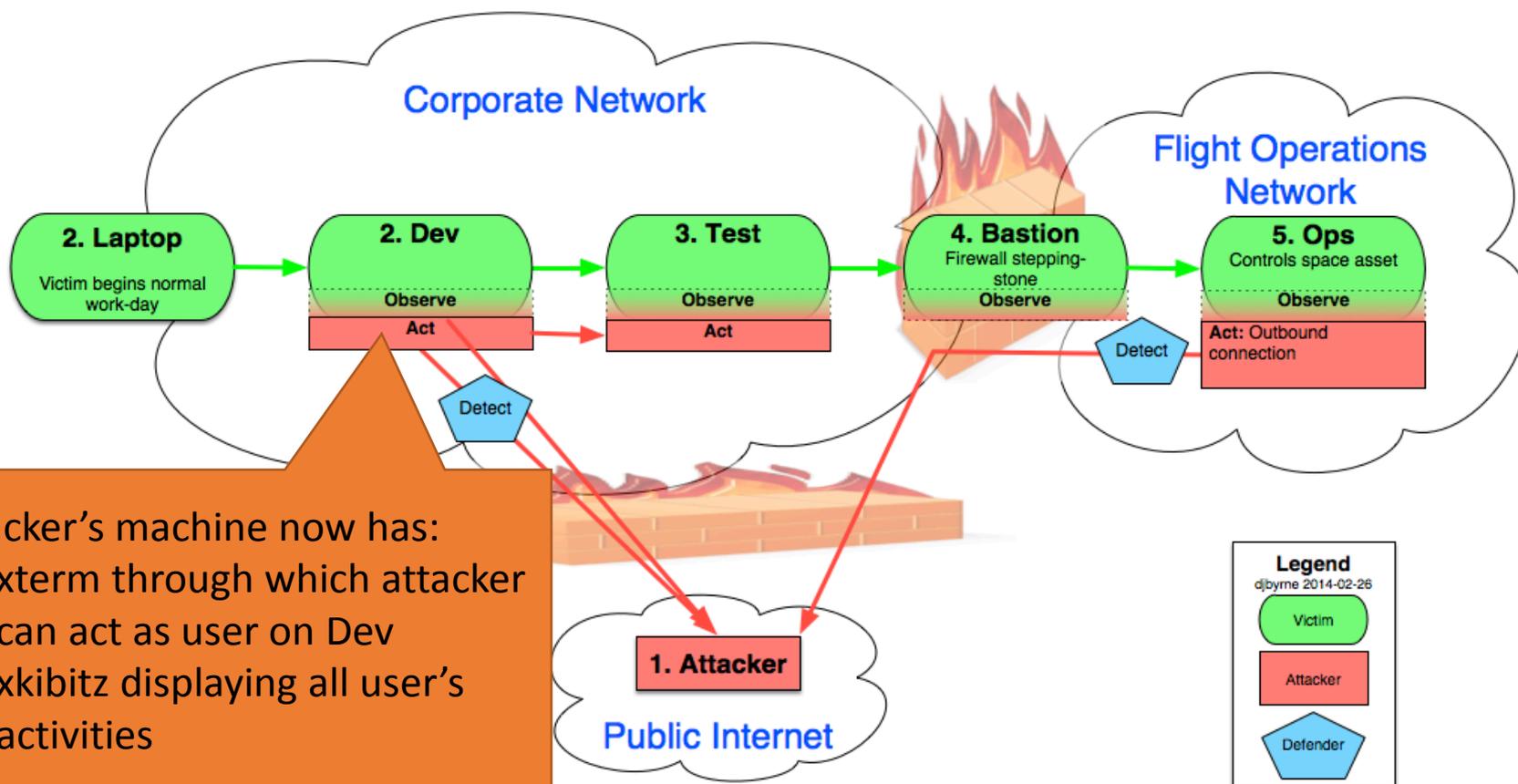
Attacker has added to login script lines to:

- Start an xterm to display on attacker’s machine
- Start xkibitz to display on attacker’s machine to see everything victim does

# “Reconnaissance attack”



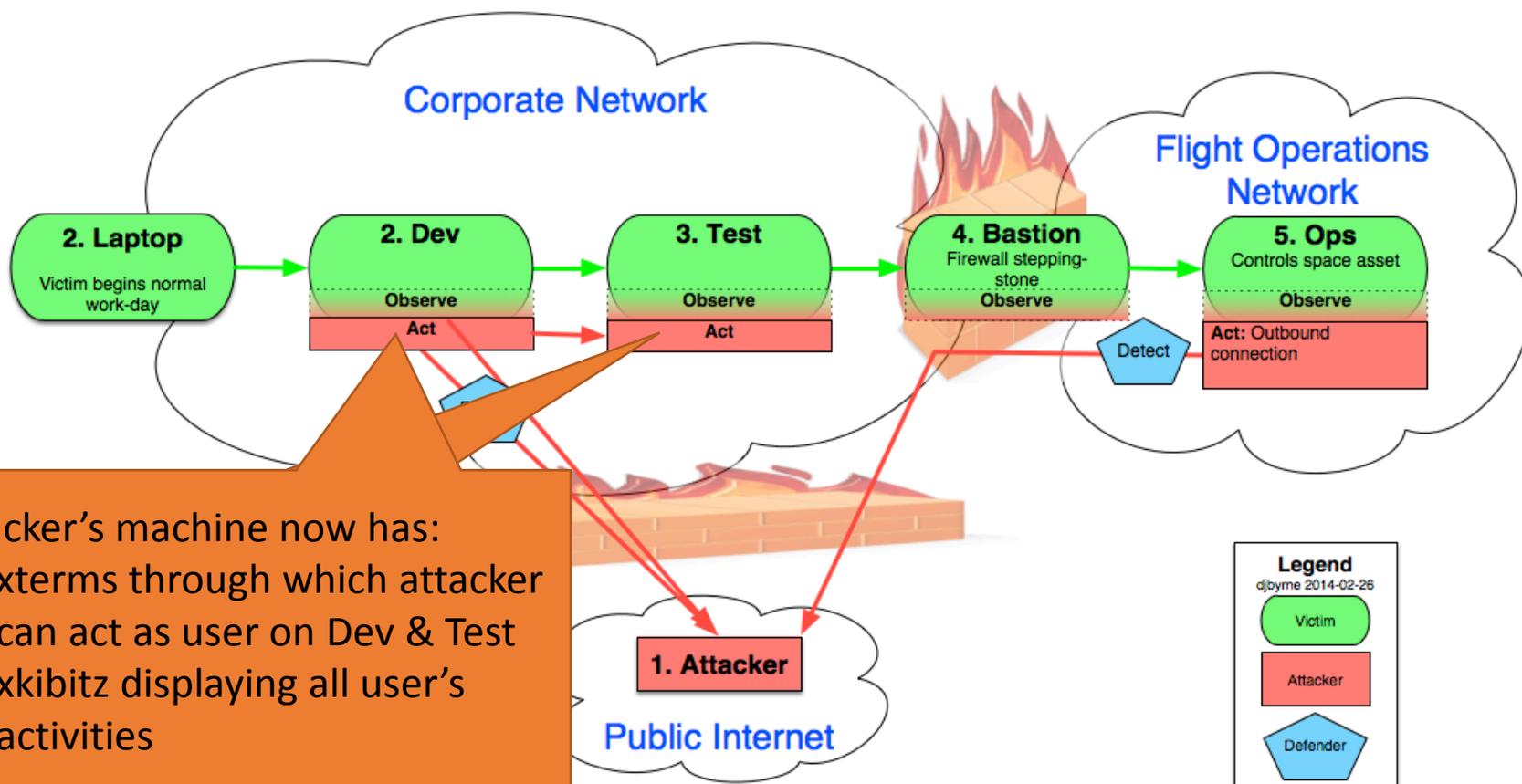
Victim logs in to Dev using multi-factor authentication



# “Reconnaissance attack”



Victim logs in from Dev to Test using “Single Sign On” ticket



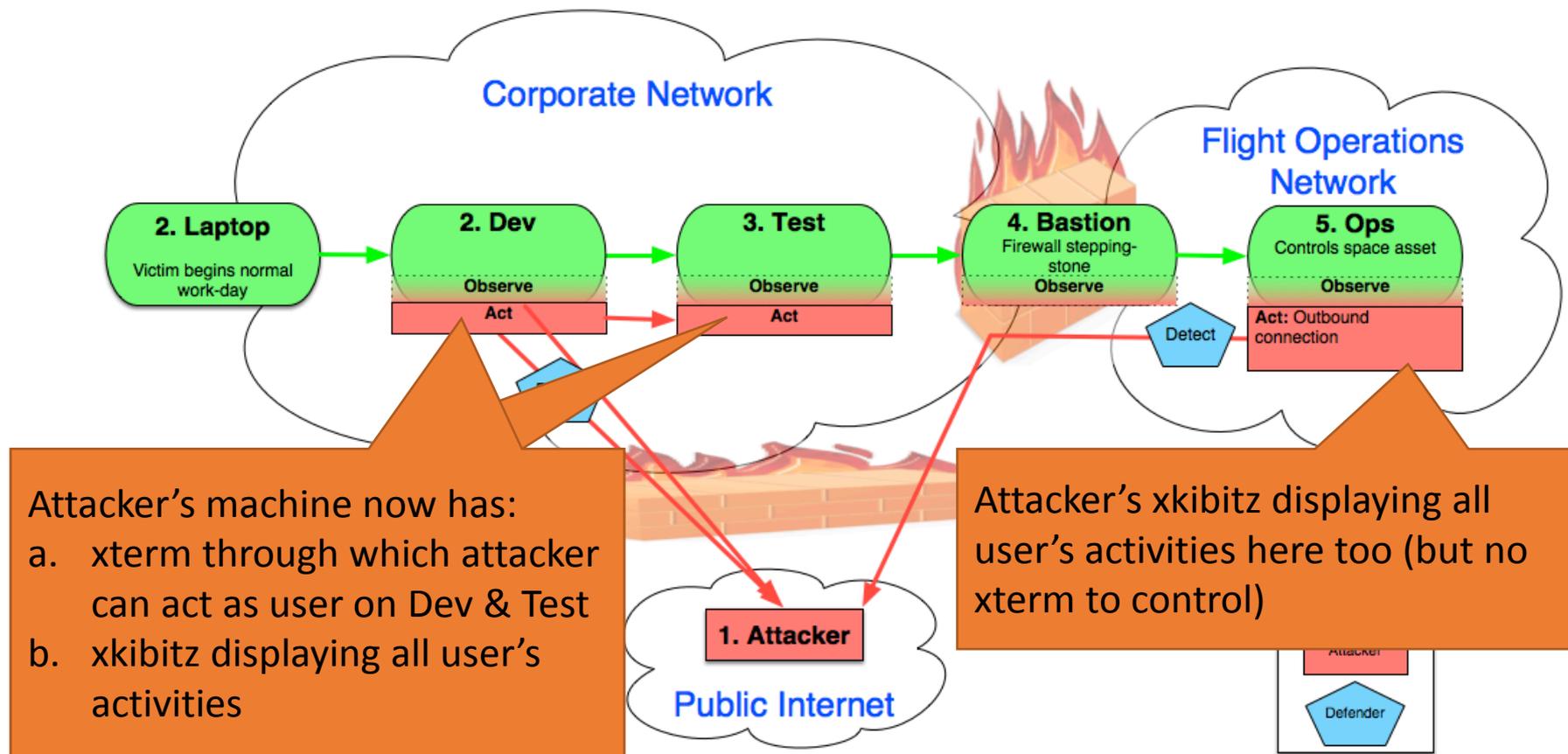
- Attacker's machine now has:
- a. xterms through which attacker can act as user on Dev & Test
  - b. xkibitz displaying all user's activities

Note: xterms persist after victim has logged off!

# “Reconnaissance attack”



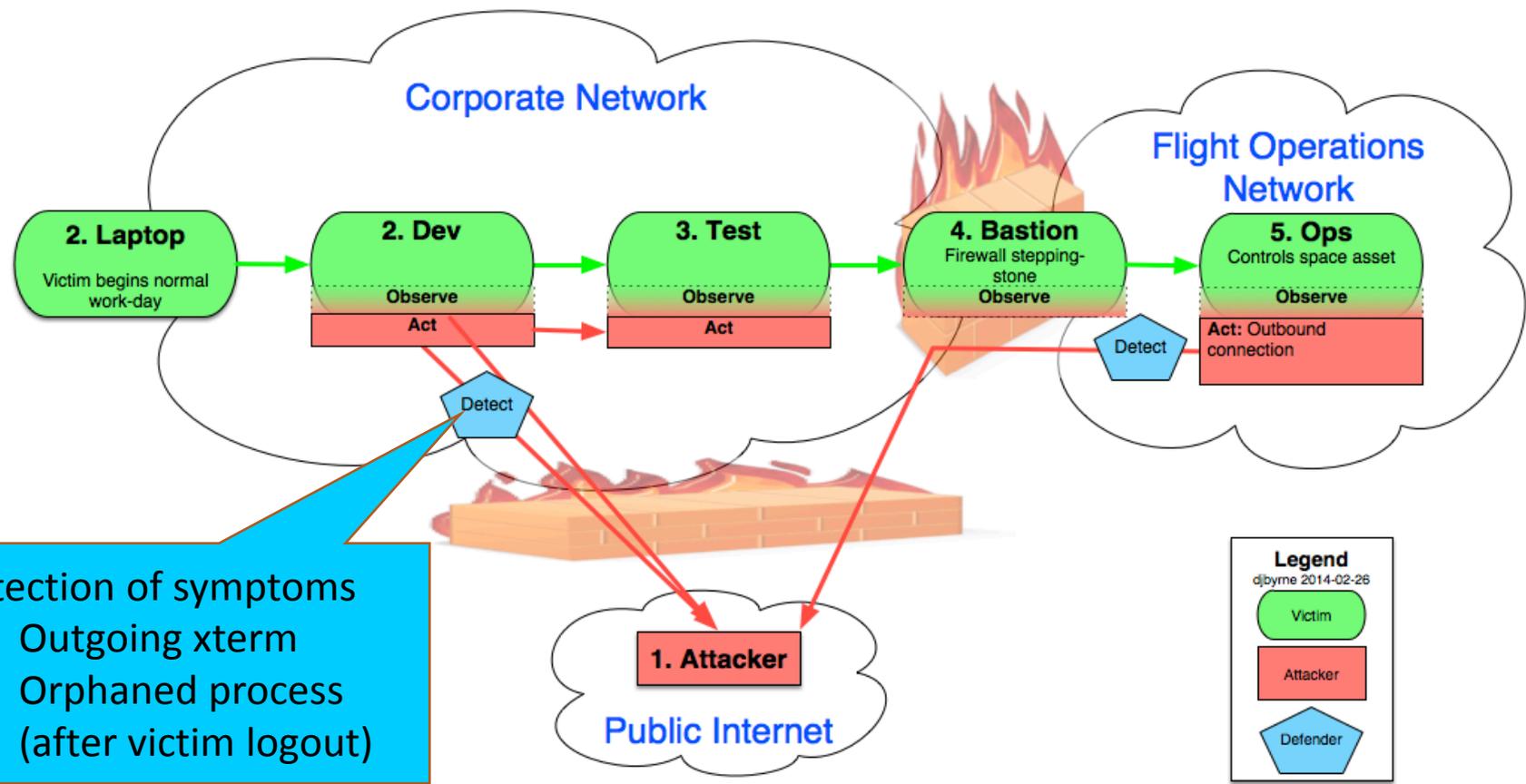
Victim logs in through Bastion to Ops (requiring multi-factor authentication again)



# “Reconnaissance attack”



Victim logs out, goes home for the day



Detection of symptoms

- i. Outgoing xterm
- ii. Orphaned process (after victim logout)

# V&V workflow – Set Up



- Identify system and scenario(s) to be defended  
Spacecraft commanding – confidentiality & integrity
- Select or design cyber attack to be defended against  
“Reconnaissance attack”
- Determine (test?) that the cyber attack would be a threat in the *operational* environment  
Possible to test; observed in the wild; plausible
- Configure test environment to model operational environment as required  
High fidelity like environment in CDRL (Lab) (CPUs, Network, authentication services, ...)  
WE SIMPLIFIED FURTHER  
Virtualized CDRL setup  
(absent irrelevant services...)



# V&V workflow – Attack



- Determine that the attack succeeds
  - In *test* environment
  - Without the defense present

Yes, when victim logs in, xterm & xkibitz open on attacker's machine ✓

- Measure attack effects – breaches of:

• Confidentiality – view victim activities ✓

• Integrity – perform user-allowed actions, persists even after victim logs out ✓

• Availability – ignored (but also plausible)



# V&V workflow – Attack



```
Machine View Devices Help
[mfeather@ ~]$ ls -l *.txt
-rw-r--r-- 1 mfeather jpl 150 Aug 28 12:54 command-dictionary.txt
-rw-r--r-- 1 root root 6286866 Jul 20 19:33 iftoplog_20140720.txt
-rw-r--r-- 1 mfeather jpl 1840 Jun 6 22:39 log0runbads.txt
-rw-r--r-- 1 mfeather jpl 14070 Jun 8 08:59 log120runexperiments.txt
-rw-r--r-- 1 mfeather jpl 8875 Jun 7 08:17 log60runexperiments.txt
-rw-r--r-- 1 mfeather jpl 15305 Jun 14 15:24 logdebugs_20140614a.txt
-rw-r--r-- 1 mfeather jpl 63438 Jun 15 19:55 logdebugs_20140615a.txt
-rw-r--r-- 1 mfeather jpl 161020 Jul 6 19:08 logifconfig.txt
-rw-r--r-- 1 root root 6914088 Jul 23 14:18 logiftop.txt
-rw-r--r-- 1 mfeather jpl 600 Jun 7 00:19 logrunbads.txt
-rw-r--r-- 1 mfeather jpl 25404 Jun 23 12:55 logrunmanyxterms_20140623.txt
-rw-r--r-- 1 mfeather jpl 19073 Jun 25 11:48 logrunmanyxterms_20140625.txt
-rw-r--r-- 1 mfeather jpl 19044 Aug 14 00:51 logrunmanyxterms_20140814.txt
-rw-r--r-- 1 mfeather jpl 207829 Jun 23 12:46 logtop_20140623.txt
-rw-r--r-- 1 mfeather jpl 177600 Jun 25 11:41 logtop_20140625.txt
-rw-r--r-- 1 root root 229081 Jul 20 19:14 logtop_20140720.txt
-rw-r--r-- 1 mfeather jpl 4578 Jun 30 10:58 logtop_tiny_20140630.txt
-rw-r--r-- 1 root root 344902 Jul 23 13:32 logtop.txt
-rw-r--r-- 1 mfeather jpl 41 Jul 6 15:35 my_cron_jobs.txt
-rw-r--r-- 1 root root 28 Jul 22 10:13 traflog.txt
[mfeather@ ~]$ _
```

**Victim's window**

```
[mfeather@ ~]$ ls -l *.txt
-rw-r--r-- 1 mfeather jpl 150 Aug 28 12:54 command-dictionary.txt
-rw-r--r-- 1 root root 6286866 Jul 20 19:33 iftoplog_20140720.txt
-rw-r--r-- 1 mfeather jpl 1840 Jun 6 22:39 log0runbads.txt
-rw-r--r-- 1 mfeather jpl 19073 Jun 25 11:40 logrunmanyxterms_20140625.txt
-rw-r--r-- 1 mfeather jpl 19044 Aug 14 00:51 logrunmanyxterms_20140814.txt
-rw-r--r-- 1 mfeather jpl 207829 Jun 23 12:46 logtop_20140623.txt
-rw-r--r-- 1 mfeather jpl 177600 Jun 25 11:41 logtop_20140625.txt
-rw-r--r-- 1 root root 229081 Jul 20 19:14 logtop_20140720.txt
-rw-r--r-- 1 mfeather jpl 4578 Jun 30 10:58 logtop_tiny_20140630.txt
-rw-r--r-- 1 root root 344902 Jul 23 13:32 logtop.txt
-rw-r--r-- 1 mfeather jpl 41 Jul 6 15:35 my_cron_jobs.txt
-rw-r--r-- 1 root root 28 Jul 22 10:13 traflog.txt
[mfeather@ ~]$
```

**Attacker's xkibitz window  
see all victim's activities**

```
[mfeather@ ~]$ ls command*
command-dictionary.txt
[mfeather@ ~]$ cat command-dictionary.txt
(this is completely fictitious, not a real command dictionary)
Go into safe mode CHD01-SH
Turn on heater CHD01-HTR-ON
Turn off heater CHD01-HTR-OFF
[mfeather@ ~]$
```

**Attacker's xterm window  
act as user**

**Screenshot of laptop running reconnaissance attack in virtual test environment**

# V&V workflow – Defend

- Develop defense, deploy in *test* environment

Commercial network monitoring + query for detecting remote xterm + *automated* response to kill rogue process on victim's machine

- Take measurements during *no* attack

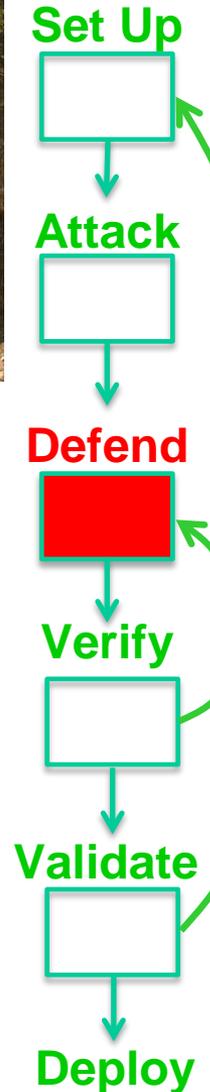
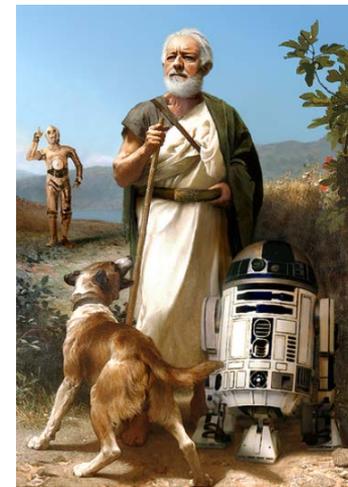
- Understand the computational etc. costs of the defense, its interference on normal operation, etc.

CPU, memory, network; license & monitoring host \$

- Take measurements during attack

- Efficacy of the defense at preventing / detecting & responding to / recovering from the attack

durations of attacker's xterm & xkibitz windows



# V&V workflow – Defend



Automated response

```
[mfeather@ ~]$ ls -l *.txt
-rw-r--r-- 1 mfeather jpl 150 Aug 28 12:54 command-dictionary.txt
-rw-r--r-- 1 root root 6286866 Jul 20 19:33 iftoplog_20140720.txt
-rw-r--r-- 1 mfeather jpl 1840 Jun 6 22:39 log0runbads.txt
-rw-r--r-- 1 mfeather jpl 14070 Jun 8 08:59 log120runexperiments.txt
-rw-r--r-- 1 mfeather jpl 8875 Jun 7 08:17 log60runexperiments.txt
-rw-r--r-- 1 mfeather jpl 15305 Jun 14 15:24 logdebugs_20140614a.txt
-rw-r--r-- 1 mfeather jpl 63438 Jun 15 19:55 logdebugs_20140615a.txt
-rw-r--r-- 1 mfeather jpl 161020 Jul 6 19:08 logifconfig.txt
-rw-r--r-- 1 root root 6914088 Jul 23 14:18 logiftop.txt
-rw-r--r-- 1 mfeather jpl 600 Jun 7 00:19 logrunbads.txt
-rw-r--r-- 1 mfeather jpl 25404 Jun 23 12:55 logrunmanyxterms_20140623.txt
-rw-r--r-- 1 mfeather jpl 19073 Jun 25 11:40 logrunmanyxterms_20140625.txt
-rw-r--r-- 1 mfeather jpl 19044 Aug 14 00:51 logrunmanyxterms_20140814.txt
-rw-r--r-- 1 mfeather jpl 207829 Jun 23 12:46 logtop_20140623.txt
-rw-r--r-- 1 mfeather jpl 177600 Jun 25 11:41 logtop_20140625.txt
-rw-r--r-- 1 root root 229081 Jul 20 19:14 logtop_20140720.txt
-rw-r--r-- 1 mfeather jpl 4578 Jun 30 10:58 logtop_tiny_20140630.txt
-rw-r--r-- 1 root root 344902 Jul 23 13:32 logtop.txt
-rw-r--r-- 1 mfeather jpl 41 Jul 6 15:35 mj_cron_jobs.txt
-rw-r--r-- 1 root root 28 Jul 22 10:13 traflog.txt
[mfeather@ ~]$
```

```
[mfeather@ ~]$ ls -l *.txt
-rw-r--r-- 1 mfeather jpl 150 Aug 28 12:54 command-dictionary.txt
-rw-r--r-- 1 root root 6286866 Jul 20 19:33 iftoplog_20140720.txt
-rw-r--r-- 1 mfeather jpl 1840 Jun 6 22:39 log0runbads.txt
-rw-r--r-- 1 mfeather jpl 14070 Jun 8 08:59 log120runexperiments.txt
-rw-r--r-- 1 mfeather jpl 8875 Jun 7 08:17 log60runexperiments.txt
-rw-r--r-- 1 mfeather jpl 15305 Jun 14 15:24 logdebugs_20140614a.txt
-rw-r--r-- 1 mfeather jpl 63438 Jun 15 19:55 logdebugs_20140615a.txt
-rw-r--r-- 1 mfeather jpl 161020 Jul 6 19:08 logifconfig.txt
-rw-r--r-- 1 root root 6914088 Jul 23 14:18 logiftop.txt
-rw-r--r-- 1 mfeather jpl 600 Jun 7 00:19 logrunbads.txt
-rw-r--r-- 1 mfeather jpl 25404 Jun 23 12:55 logrunmanyxterms_20140623.txt
-rw-r--r-- 1 mfeather jpl 19073 Jun 25 11:40 logrunmanyxterms_20140625.txt
-rw-r--r-- 1 mfeather jpl 19044 Aug 14 00:51 logrunmanyxterms_20140814.txt
-rw-r--r-- 1 mfeather jpl 207829 Jun 23 12:46 logtop_20140623.txt
-rw-r--r-- 1 mfeather jpl 177600 Jun 25 11:41 logtop_20140625.txt
-rw-r--r-- 1 root root 229081 Jul 20 19:14 logtop_20140720.txt
-rw-r--r-- 1 mfeather jpl 4578 Jun 30 10:58 logtop_tiny_20140630.txt
-rw-r--r-- 1 root root 344902 Jul 23 13:32 logtop.txt
-rw-r--r-- 1 mfeather jpl 41 Jul 6 15:35 mj_cron_jobs.txt
-rw-r--r-- 1 root root 28 Jul 22 10:13 traflog.txt
[mfeather@ ~]$
```



```
[mfeather@ ~]$ ls command*
command-dictionary.txt
[mfeather@mlvsts]$ cat command-dictionary.txt
(this is completely fictitious, not a real command dictionary)
Go into safe mode CHD01-SM
Turn on heater CHD01-HTR-ON
Turn off heater CHD01-HTR-OFF
[mfeather@ ~]$
```

```
[mfeather@ ~]$ ls command*
command-dictionary.txt
[mfeather@mlvsts]$ cat command-dictionary.txt
(this is completely fictitious, not a real command dictionary)
Go into safe mode CHD01-SM
Turn on heater CHD01-HTR-ON
Turn off heater CHD01-HTR-OFF
[mfeather@ ~]$
```

# V&V workflow – Verify



- Verify:

- Cyber experts converse *with real users*
- Extrapolate measurements from *test* environment to infer effects in *operational* environment  
Note: beware of confounders to test fidelity

Are extrapolated results acceptable?



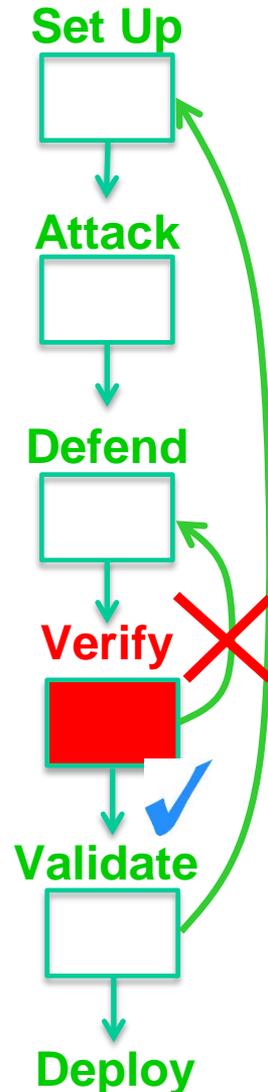
YES: advance to **Validate**

(to determine acceptability in *operational* environment)



NO: return to **Defend**

(to address identified improvement needs)



# V&V workflow – Verify



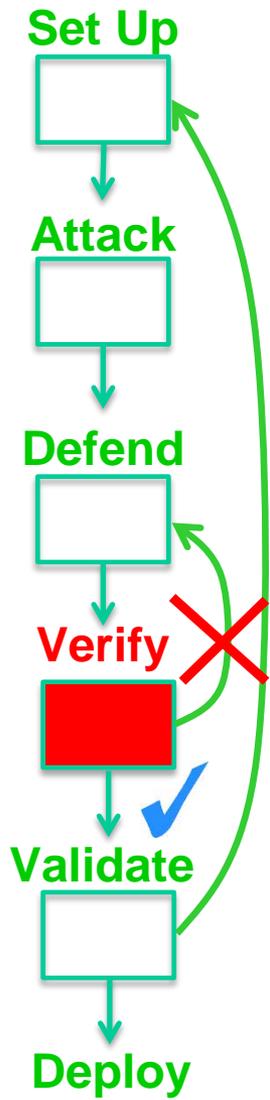
- Verify:
  - Cyber experts converse *with real users*

2014-07-23 12:41:09	0	2014-07-23 12:40:57	0.76	0.005
2014-07-23 12:41:14	0	2014-07-23 12:40:59	0.76	0.055
2014-07-23 12:41:19	0	2014-07-23 12:41:01	0.70	0.01
2014-07-23 12:41:24	0	2014-07-23 12:41:03	0.70	0.01
2014-07-23 12:41:29	0	2014-07-23 12:41:05	0.70	0.049
2014-07-23 12:41:34	1.25	2014-07-23 12:41:07	0.80	0.039
2014-07-23 12:41:39	1.3	2014-07-23 12:41:09	0.80	0.059
2014-07-23 12:41:44	0.58	2014-07-23 12:41:11	0.74	0.015
2014-07-23 12:41:49	0.48	2014-07-23 12:41:13	0.74	0.025
2014-07-23 12:41:54	0	2014-07-23 12:41:15	0.74	0.055



recon_log_events-140				
2014-07-23 12:40:08	2546	00:00	0	
2014-07-23 12:40:21	2601	00:00	0	
2014-07-23 12:40:26	2546	00:19	19	
2014-07-23 12:40:32	2686	00:00	0	
2014-07-23 12:40:45	2746	00:00	0	
2014-07-23 12:40:48	2601	00:28	28	
2014-07-23 12:40:				
2014-07-23 12:40:				
2014-07-23 12:41:				
2014-07-23 12:41:				

Reconnaissance attack's raw measurements captured in log files

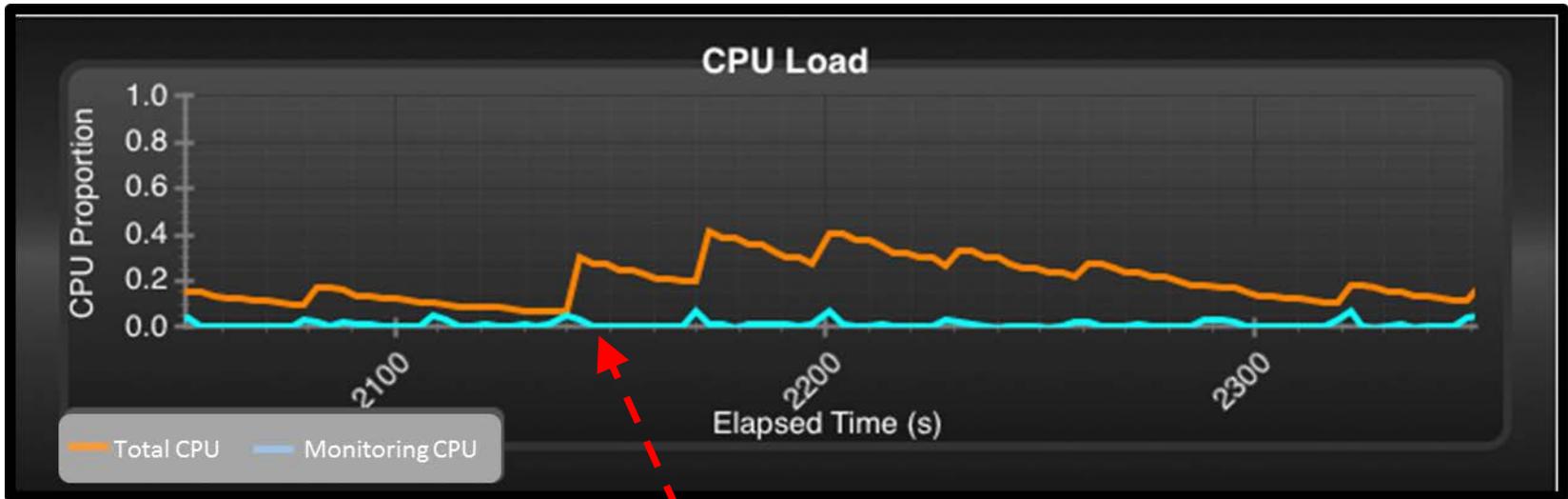


# Information Visualization

2014-07-23 12:41:09	0	2014-07-23 12:40:57	0.76	0.00
2014-07-23 12:41:14	0	2014-07-23 12:40:59	0.76	0.055
2014-07-23 12:41:19	0	2014-07-23 12:41:01	0.70	0.01
2014-07-23 12:41:24	0	2014-07-23 12:41:03	0.70	0.01
2014-07-23 12:41:29	0	2014-07-23 12:41:05	0.70	0.049
2014-07-23 12:41:34	1.25	2014-07-23 12:41:07	0.80	0.039
2014-07-23 12:41:39	1.3	2014-07-23 12:41:09	0.80	0.059
2014-07-23 12:41:44	0.58	2014-07-23 12:41:11	0.74	0.015
2014-07-23 12:41:49	0.46	2014-07-23 12:41:13	0.74	0.025
2014-07-23 12:41:54	0	2014-07-23 12:41:16	0.74	0.046
2014-07-23 12:41:59	0	2014-07-23 12:41:18	0.74	0.046
2014-07-23 12:42:04	0	2014-07-23 12:40:08	2546	00:00 0
2014-07-23 12:42:09	0	2014-07-23 12:40:21	2546	00:00 0
2014-07-23 12:42:14	0	2014-07-23 12:40:26	2546	00:19 19
2014-07-23 12:42:19	0	2014-07-23 12:40:32	2686	00:00 0
2014-07-23 12:42:24	0	2014-07-23 12:40:45	2746	00:00 0
2014-07-23 12:42:29	0	2014-07-23 12:40:48	2601	00:28 0
2014-07-23 12:42:34	0	2014-07-23 12:40:52	2686	00:22 22
2014-07-23 12:42:39	0	2014-07-23 12:40:59	2851	00:00 0
2014-07-23 12:42:44	0	2014-07-23 12:41:12	2872	00:00 0
2014-07-23 12:42:49	0	2014-07-23 12:41:16	2842	00:23 23

**Total load**  
on CPU 

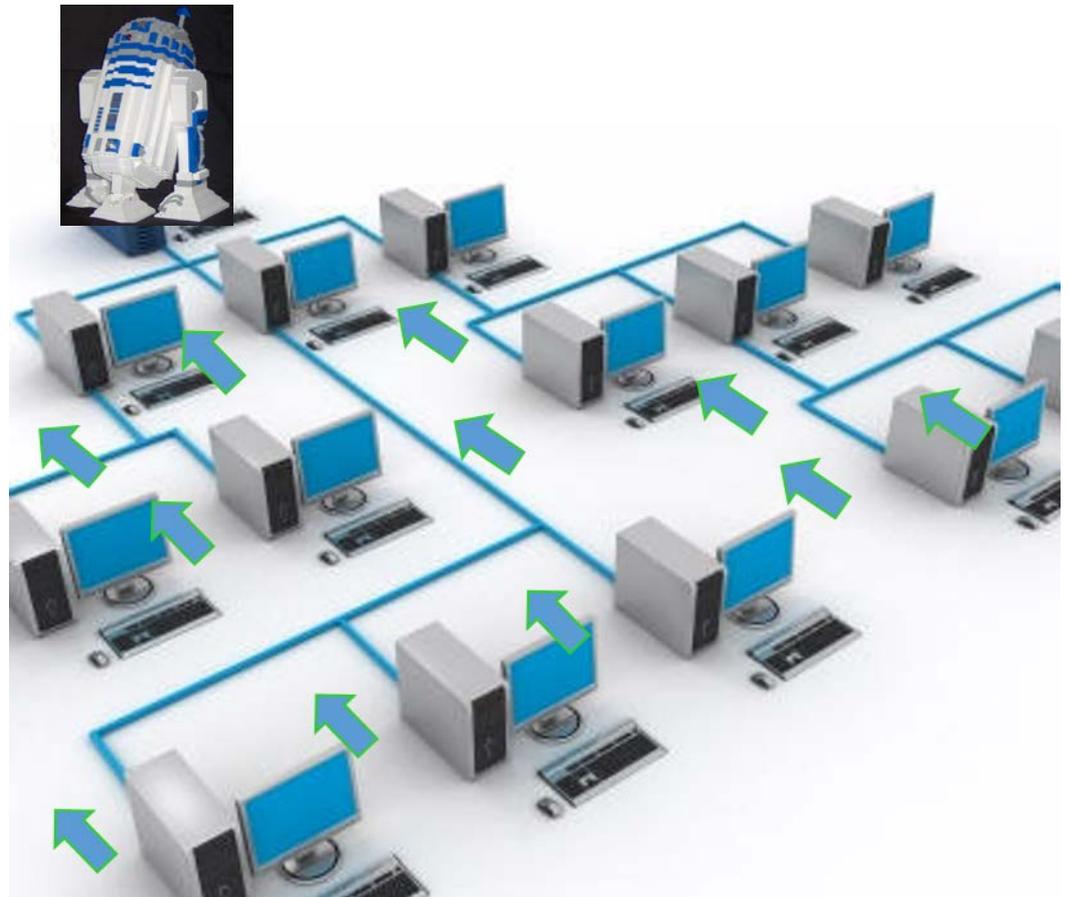
**Monitoring's**  
load on CPU 



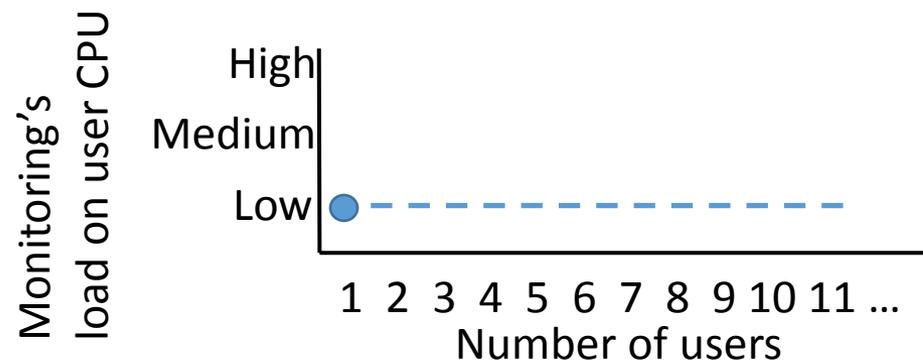
Monitoring's CPU load on user's machine *low* relative to system load & capacity 

# Extrapolation

Monitoring architecture:  
information from users' machines sent to dedicated machine for analysis & detection

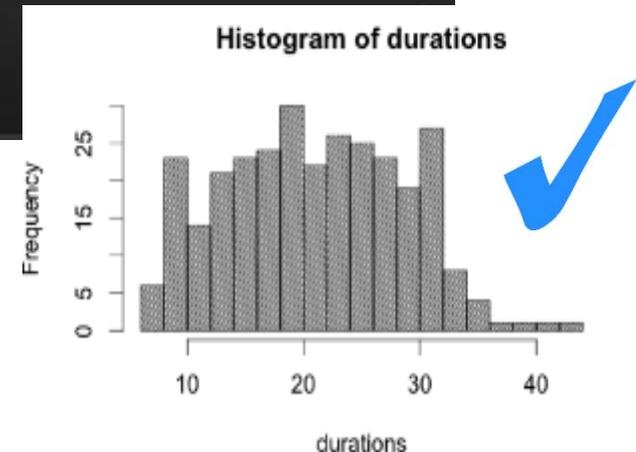
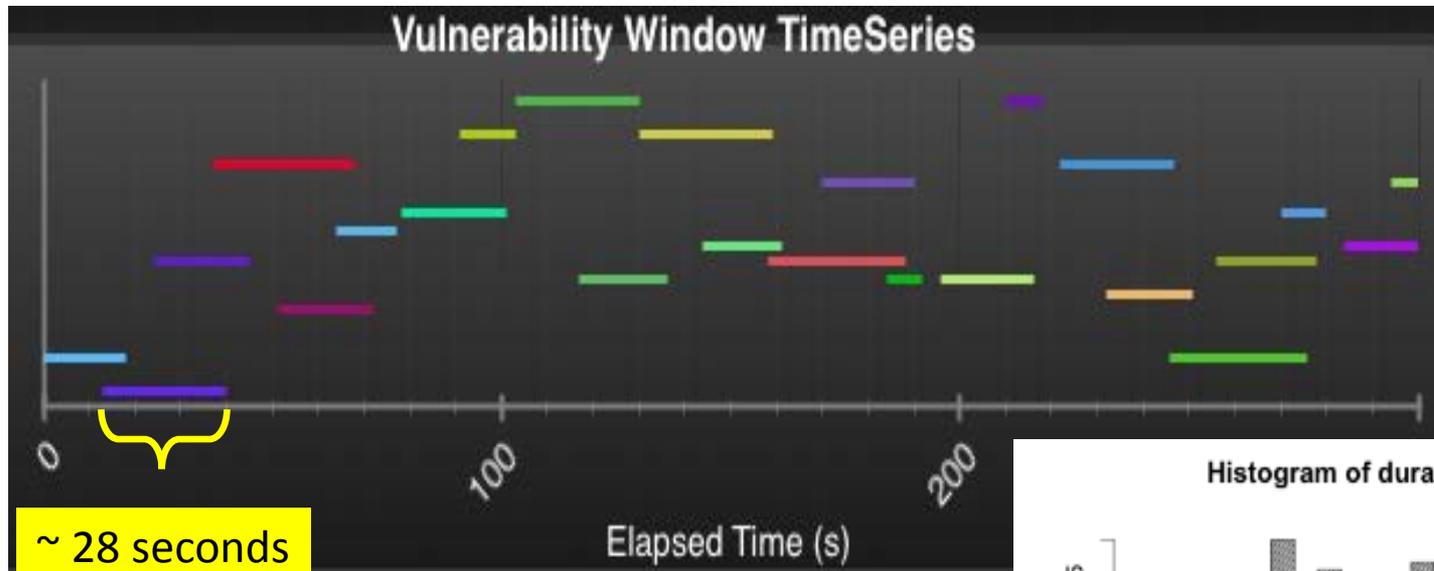


Monitoring's CPU load  
on user's machine  
independent of number  
of user machines –  
remains low



# V&V workflow – Verify benefits

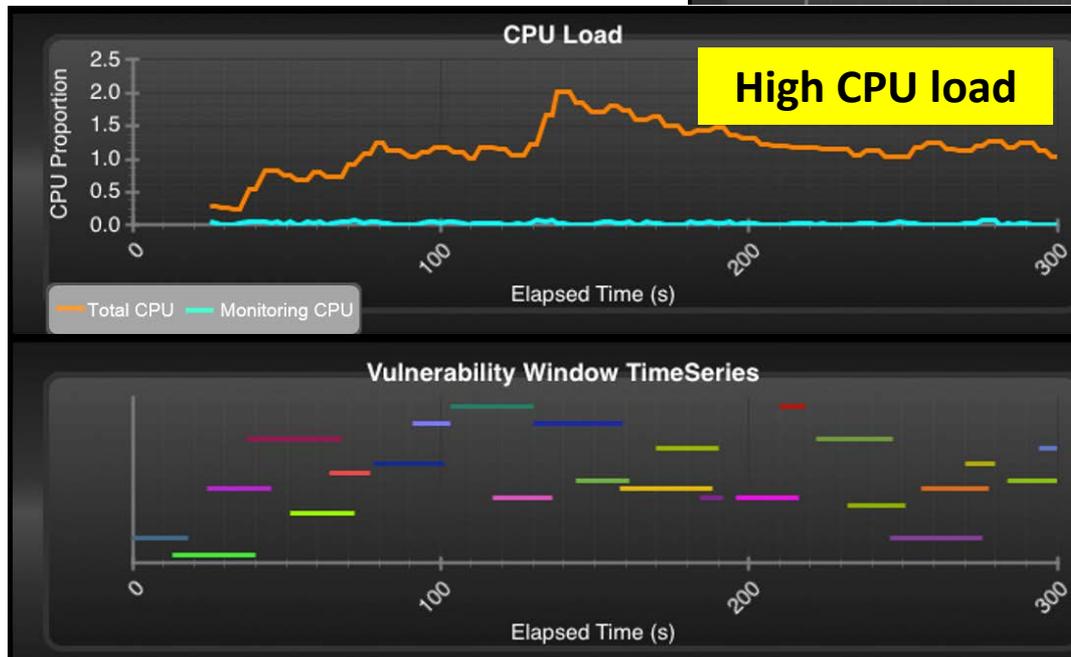
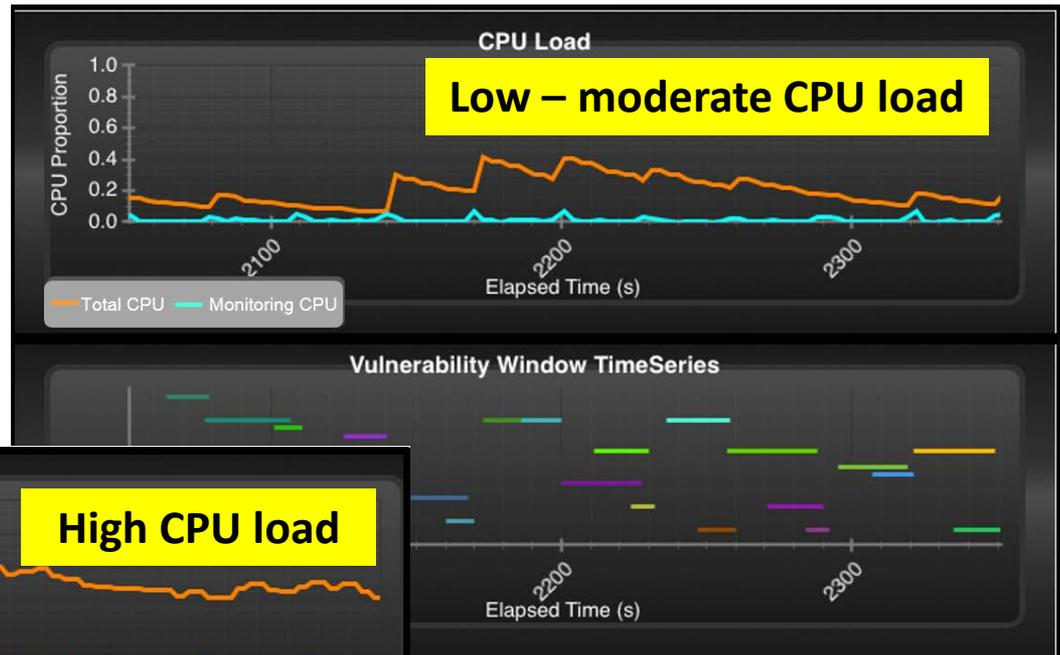
Colored line segment = duration of vulnerability  
(attacker's xterm or xkibitz window open)



Reconnaissance attack repeatedly initiated to speedily gather lots of data

# V&V workflow – Verify benefits

Experiments  
conducted in different  
CPU load conditions

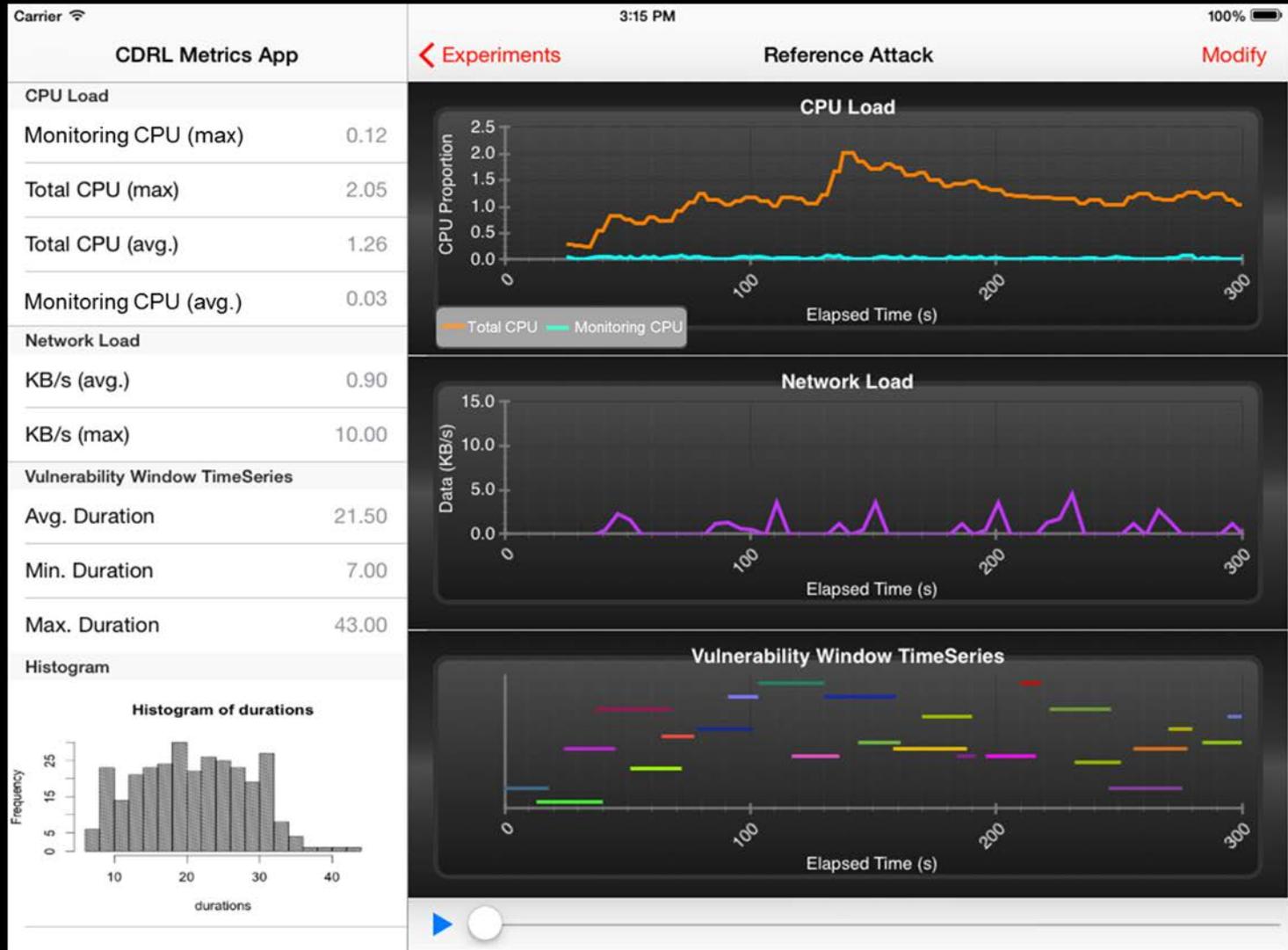


Vulnerability  
durations only slightly  
increased (~1 sec)

# Metrics dashboard



# Mobile metrics dashboard



Intended for iPad display

# V&V workflow – Verify costs

Commercial network monitoring

+

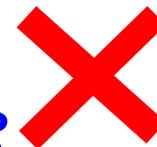
Dedicated machine for its  
analysis & detection

*Justifiable if can amortize  
over other monitoring needs*



Cannot keep open *any*  
remote xterm

*Unacceptable user inconvenience*



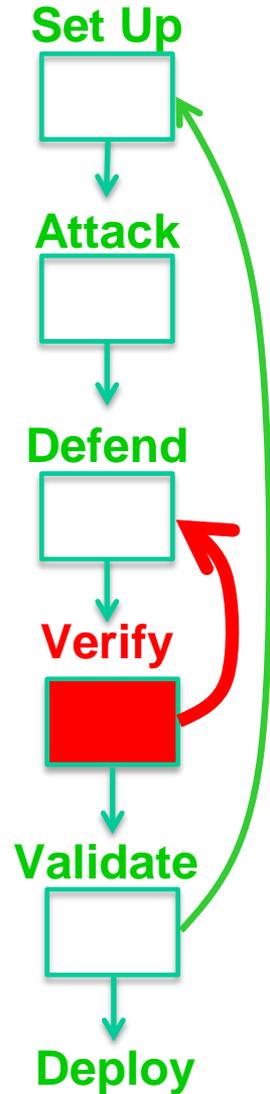
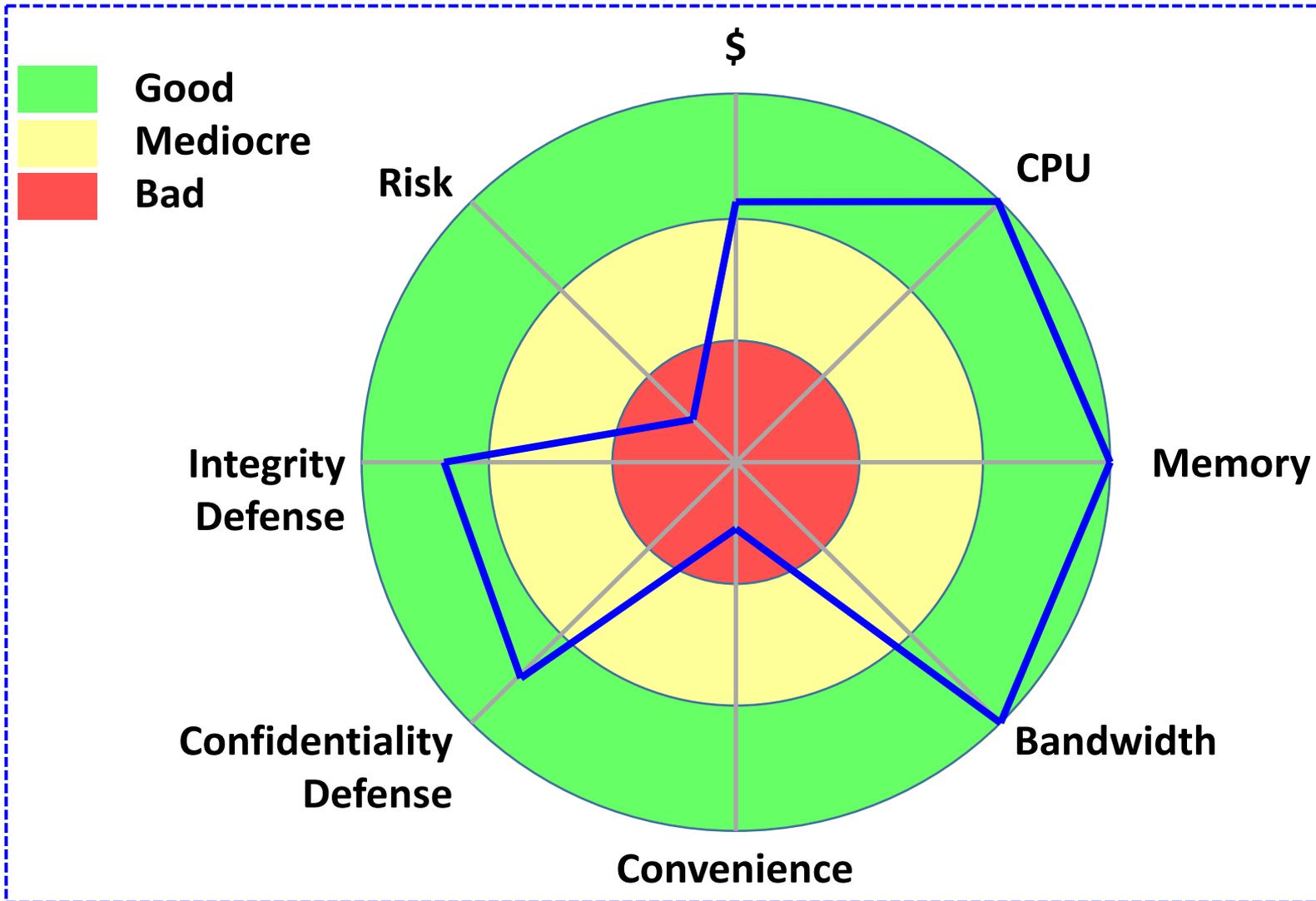
# V&V workflow – Verify risks

Passwordless-ssh as mechanism  
to kill rogue process

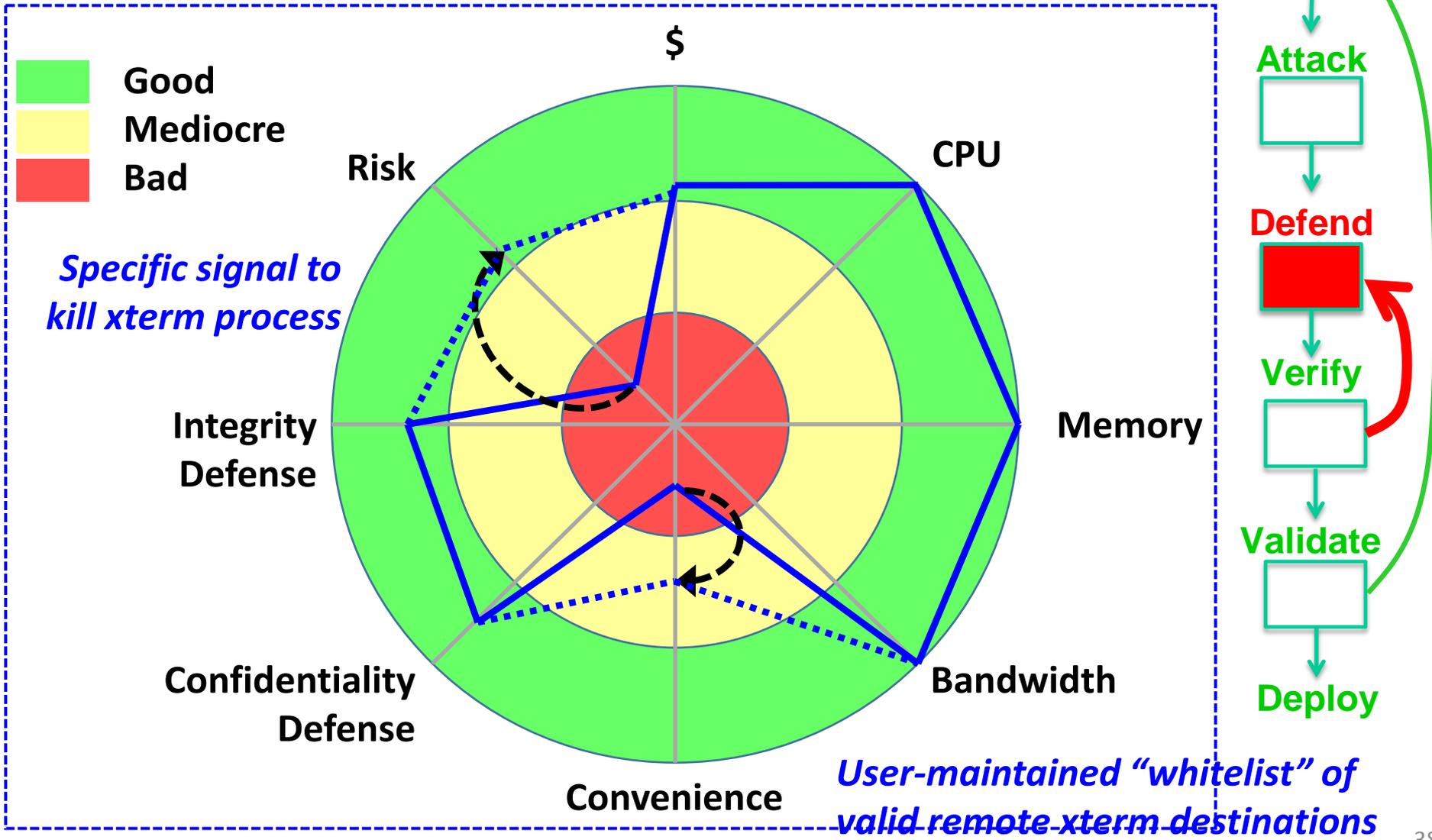


*Violates principle of least privilege*

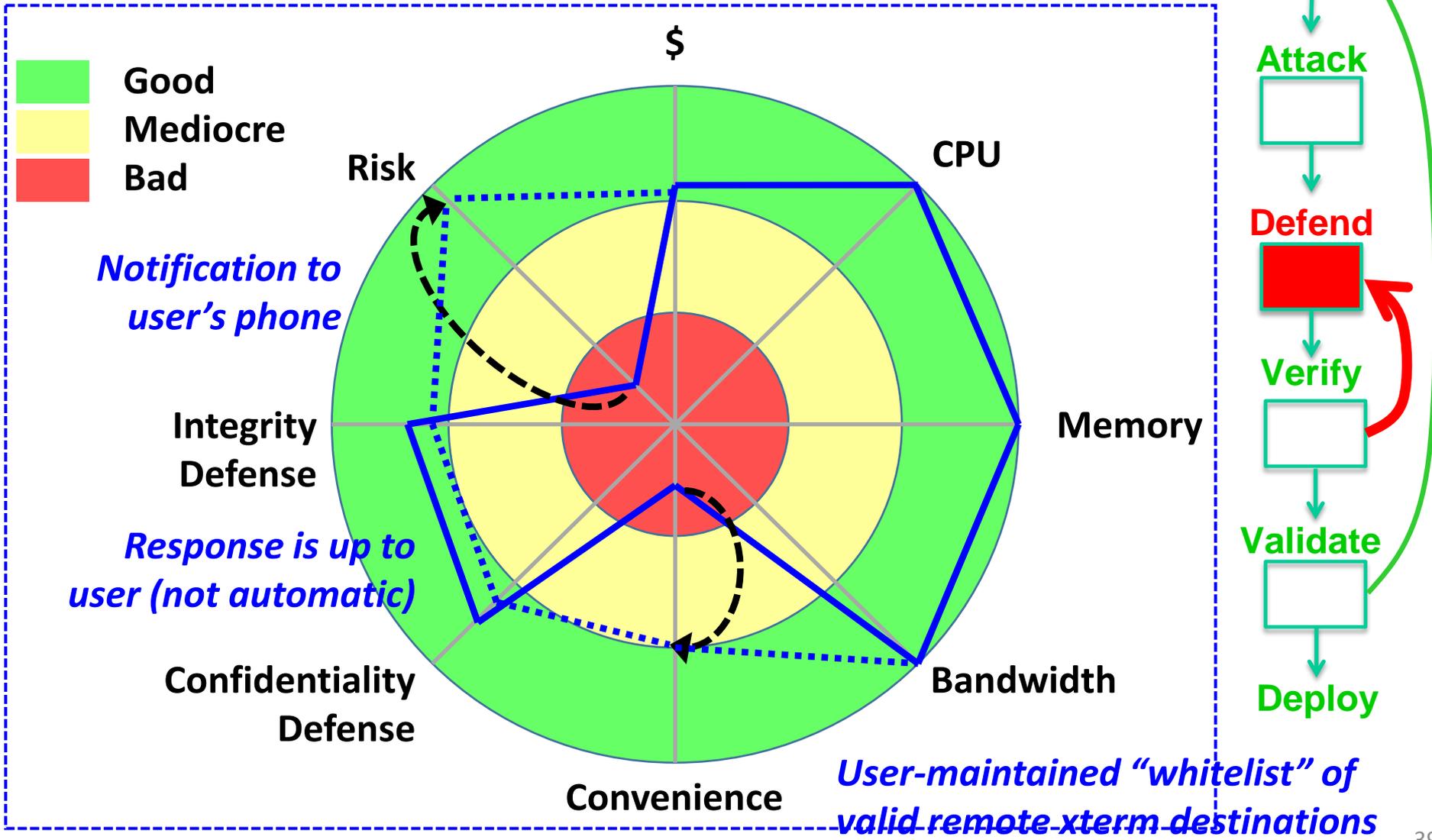
# V&V workflow – Verify status



# V&V workflow – *Redo Defense*



# V&V workflow – *Redo Defense*



# V&V workflow – Validate

CAUTIOUSLY deploy defense in operating environment

- Be willing to tolerate some disruption

IF SAFE TO DO SO, conduct attack

- Be prepared in case defense fails to stop attack

Is experience acceptable?

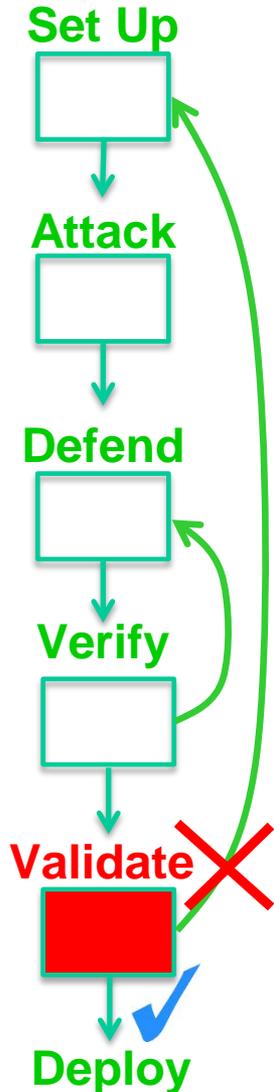
✓ YES: advance to **Deploy**

✗ NO: analyze what was wrong:

- Redesign defense
- Improve extrapolation
- Correct Set Up



*"It is difficult to make predictions, especially about the future"*

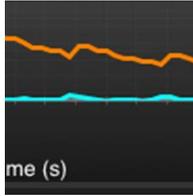
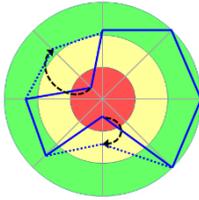


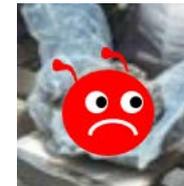
# V&V workflow – Deploy

- Probationary period
  - Continue to maintain backup and fallback capabilities
- Limited extent
  - Subset of user community (learn from their experiences)
  - Subset of network
- Continue monitoring after full deployment
  - Internal and/or external conditions may change



# Recap

- Purpose: inform the deployment decision for a cyber defense
- JPL's Cyber Defense Research Laboratory – sandboxed environment for safely running security experiments
- Cyber defense concerns: costs, benefits, risks   
- Fidelity challenge: cannot “test like you fly, fly like you test”
- V&V workflow: **Set Up** → **Attack** → **Defend** → **Verify** → **Validate** → **Deploy**
- Information visualization to comprehend & communicate 
- Assessment and comparison of defense alternatives 



Set Up



Attack



Defend



Verify



Validate

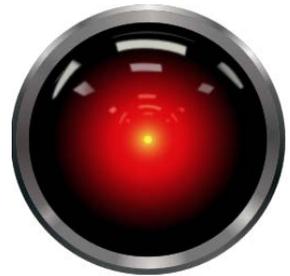


Deploy



# Confounders & Pitfalls

- “Reconnaissance attack” defenses tested in a vastly simplified sandbox (no TFA, etc.)
- Used “as is” a detection query crafted only for demonstration – got some detection “escapes”



# Future Work

- Continue to deploy – well-established operational environments vs. future ones
- Expand range of attacks & defenses
- Library of resource monitors and of artificial load



# Global issues

Test lab environment and procedures:

- Test environment configuration
- Protocols for keeping testing safe
- Handling sensitive data about attacks and defenses

*THANKS* to our colleagues for their ongoing work on these in development of a Cyber Defense Research Laboratory

**i** **Protected View** This file originated from an Internet location and might be unsafe.

Assessment in a specific operational setting of:

- Cyber risk
- Mitigation from cyber defenses

An ongoing concern for us and the cyber community at large