

Cluster Security as a Unique Problem with Emergent Properties

Joe Greenseid

National Center for Supercomputing Applications
University of Illinois
jgreen@ncsa.uiuc.edu

LCI International Conference on Linux Clusters:
The HPC Revolution
May 18, 2004



Introduction

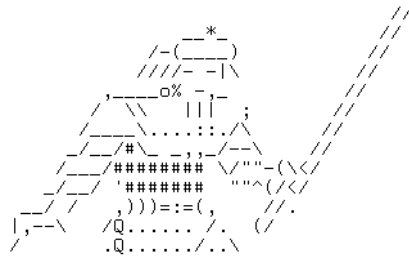
- Commodity cluster systems are increasing in number and in size
- Initial work in clusters focused on usability and management; security has been a secondary concern
- **Fallacy:** “What works for 1 system should work for 100 systems.”
- **Reality:** “A 100-node cluster is different from 100 standalone machines.”



Why are clusters targeted?

1. Attractive targets

- a. High bandwidth
- b. Computational power
- c. Massive storage capacity



2. Prestige

3. Dumb luck (a matter of numbers)

2004-05-18

Cluster Security, Emergent Properties

3



Current Best Security Practices

- **Enclosed vs. Exposed Clusters**
 - Private, non-routable address space
 - Firewalls
- **Authentication (ssh, passwordless authentication, one-time passwords)**
- **Communications**
 - ssh vs. rsh
 - scp vs. ftp
- **Secure/Remote logging**
- **Problem:** Many security solutions are resource hogs

2004-05-18

Cluster Security, Emergent Properties

4



Unique Nature of Clusters

1. Distributed resources to be protected
2. Resource management
3. Heterogeneous management environment
4. Large-scale management requirements
5. Characteristic behavior
6. **Dependent risk**

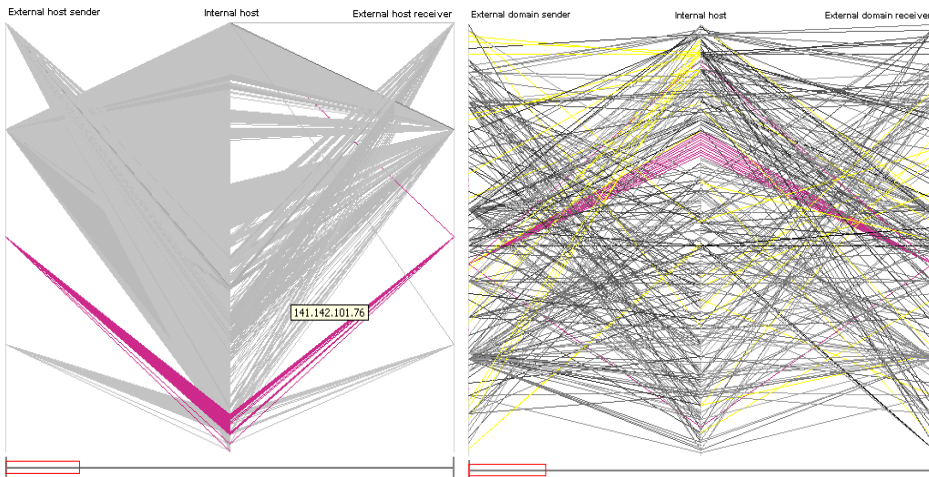
Emergent Property

Definition: a property of a system not found in individual components

Vulnerabilities not present in individual resources appear due to the coupling and interactions of those resources

Successful cluster security management must treat the cluster as a *single unit, and not as a collection of resources*

Why is Cluster Security Unique?



2004-05-18

Cluster Security, Emergent Properties

7



Techniques

- **Key idea: Leverage the unique characteristics of the cluster environment to your advantage**
 1. Process Monitoring
 2. Network Port Scanning
 3. Traffic Analysis
 4. File Integrity Scanning

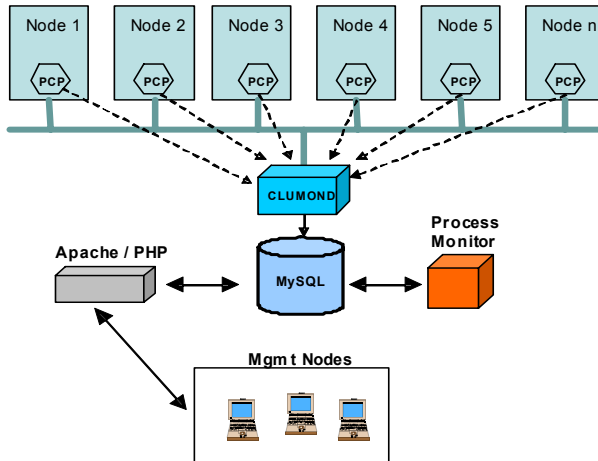
2004-05-18

Cluster Security, Emergent Properties

8



Cluster Security Example



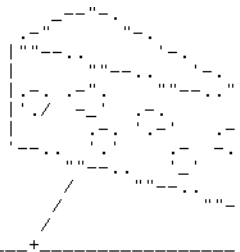
Conclusion

- Standard security practices – a good start, but will only get you half way there
- A cluster is more than the sum of its parts
- *Context is important*
- *Use the unique aspects of the cluster to your advantage*

Thanks goes out to:

- The co-authors of this paper: William Yurcik, Gregory A. Koenig, Xin Meng, and Joe Greenseid
- Joshi Fullop, Clumon developer
- NCSA Security team
- NCA Cluster administrators

Questions?



<<ANGRY HACKER CHEESE WANTS TO SPEAK!!!!!!!

WHAT DA HELL IZ YOU SAYING?!?! I ONLY PENETRATED THE OUTER LAYERS OF YOUR SYSTEMS?!?!
YOU LIKE THIS?!?!?! YOU LIKEE EHTISS?!?!?!
DON'T YOU KNOW MY KUNG FU IS THE BEST?!
MY KUNG FU IS GREEAT!

Thank you!

Joe Greenseid, William Yurcik,
Gregory A. Koenig, Xin Meng

<jgreen, byurcik, koenig, xinmeng
@ncsa.uiuc.edu>