ALDR: A New Metric for Measuring Effective Layering of Defenses

Nathaniel Boggs, Salvatore J. Stolfo
Columbia University

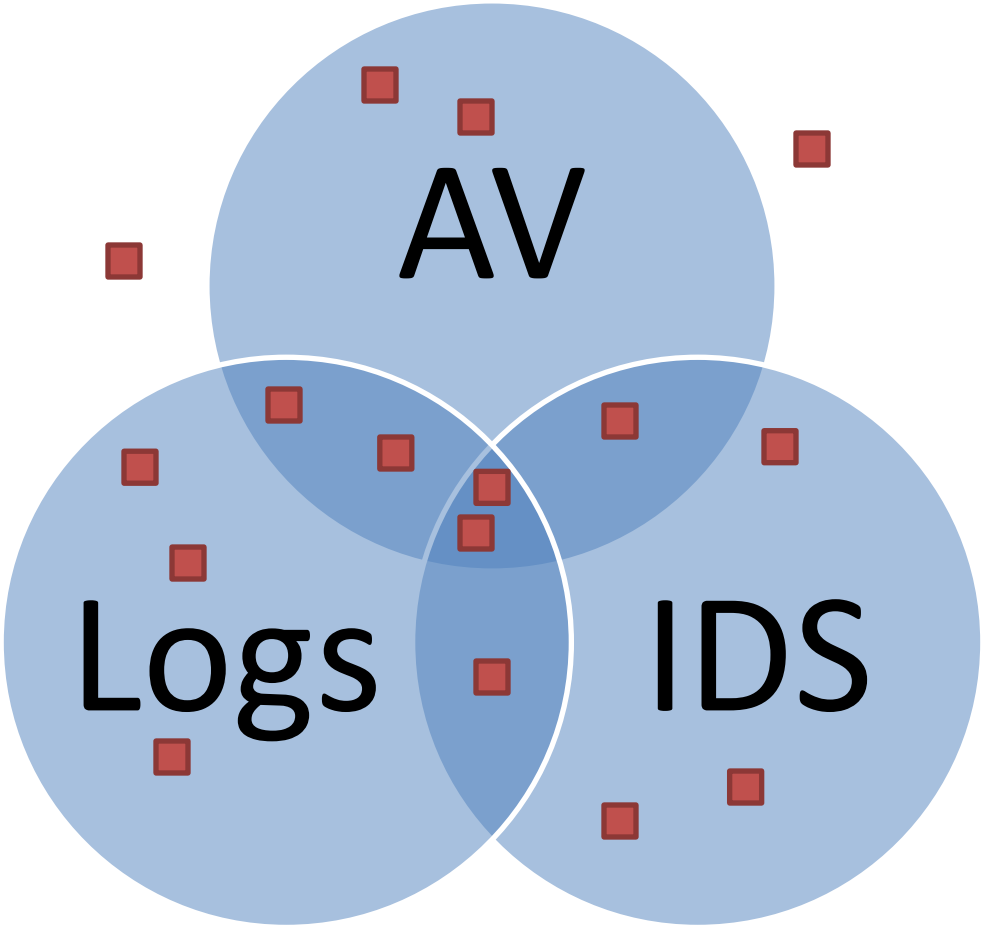
Motivation

- Buy security product X?
- Am I secure?

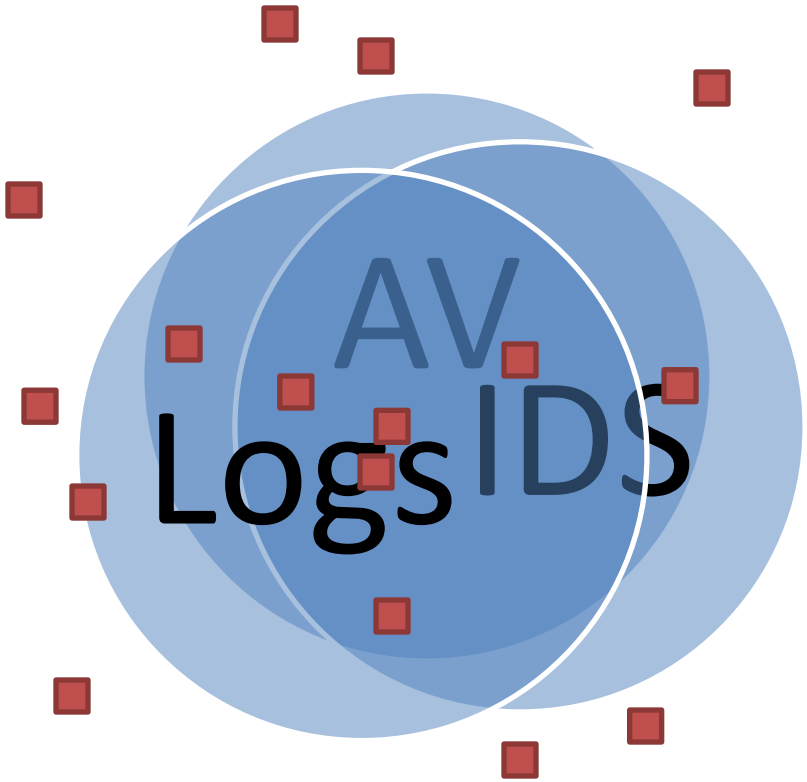
Current Answers

- Compliance checklist
- “Best Practices”
- Evaluate class of products
- Penetration testing
- Defense in Depth
- Can we do better?

Defense in Depth



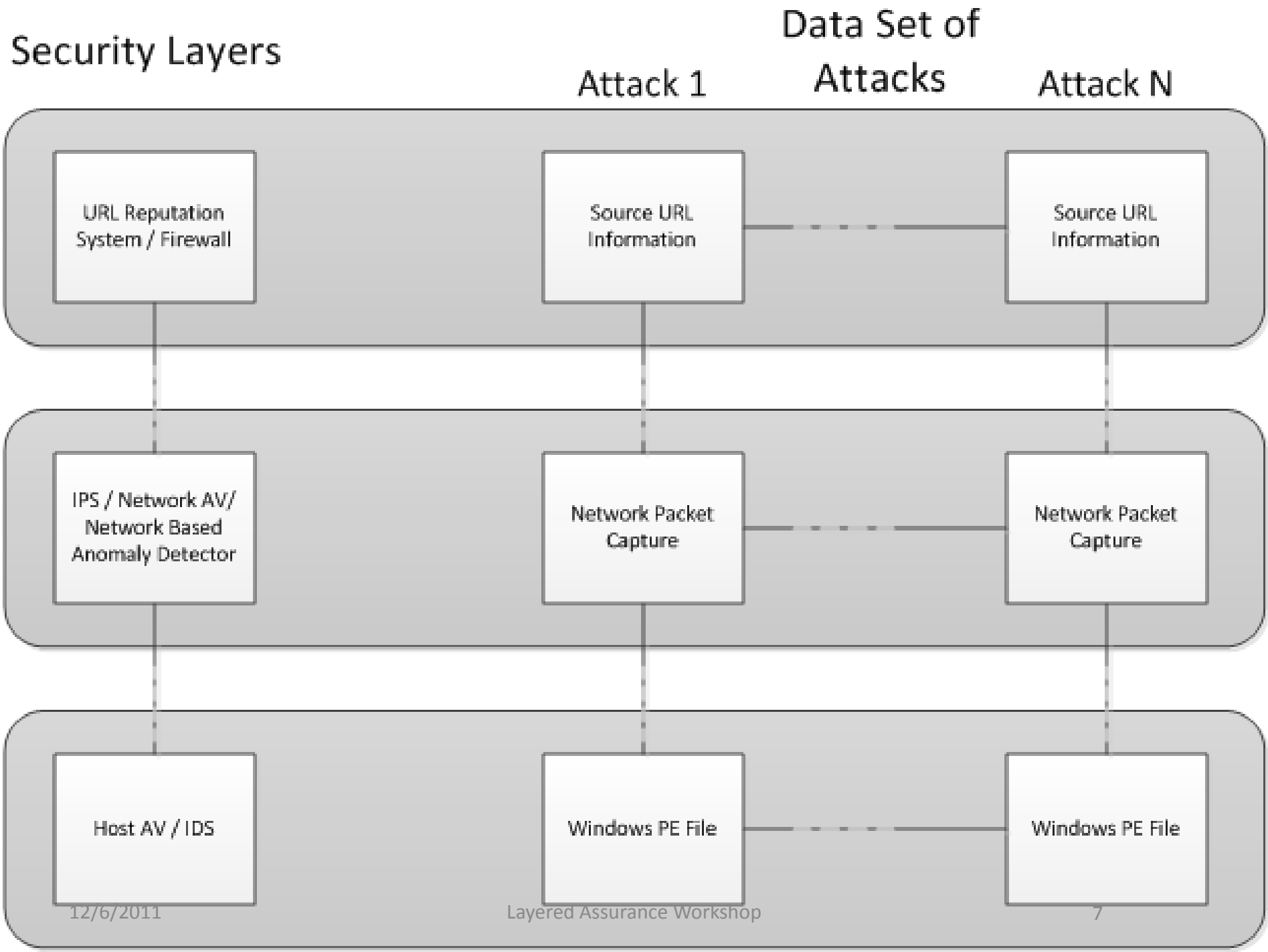
Defense in Depth



Compare Different Layers

- Compare apples to oranges
- Measure detection of ‘Attacks’
- ‘Attacks’
  - Source domain
  - Network traffic
  - Executable
  - And many more…

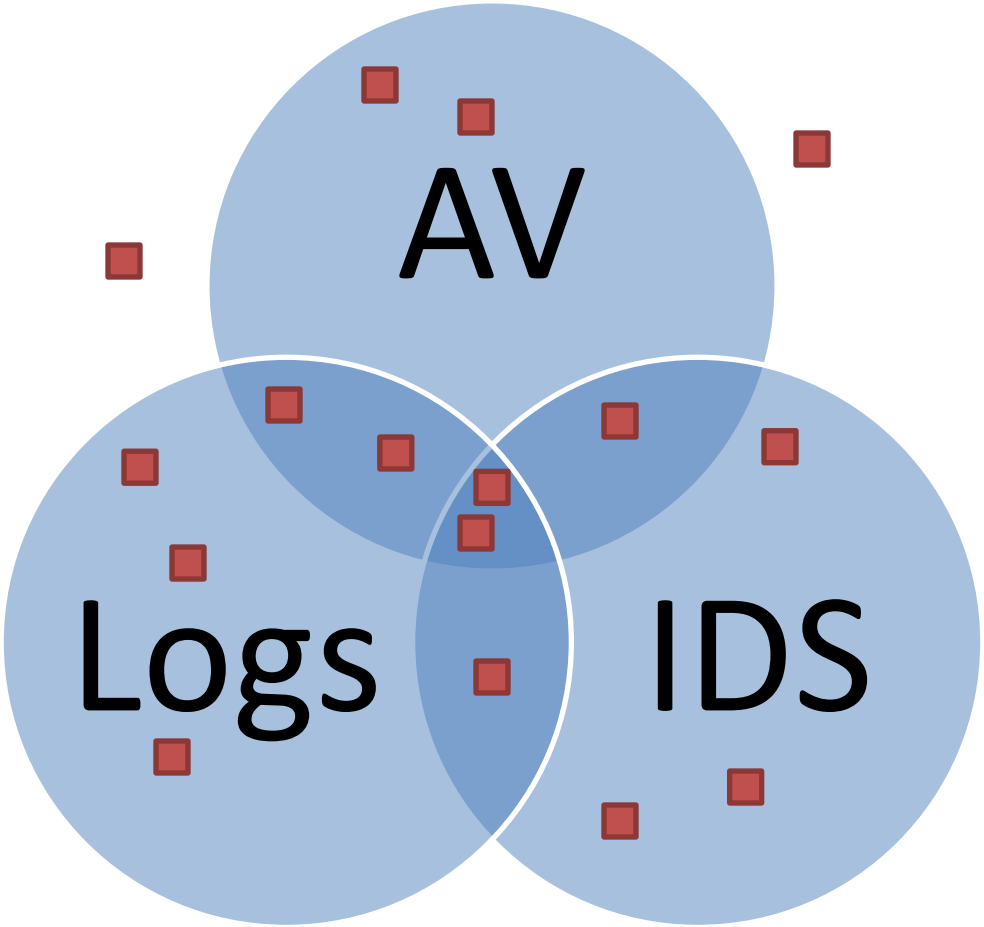
CS@CU


Security Layers
Data Set of Attacks
Attack 1
Attack N
URL Reputation System / Firewall
Source URL Information
Source URL Information
IPS / Network AV/ Network Based Anomaly Detector
Network Packet Capture
Network Packet Capture
Host AV / IDS
Windows PE File
Windows PE File

All Layer Detection Rate (ALDR)

- Test each security project
- # attacks detected / total attacks
- Total attacks detected by a set of products

ALDR: 0.875 (14/16)



ALDR – Key Attributes

- Products tested individually
- Expandable framework
  - Measure education benefit
  - Social engineering attacks
  - Any ‘attack’ representable
- Evaluate products in context

Additional Metrics

- False Positives
- Redundancy
  - Good redundancy vs bad
  - Classify detection method

What Should I Buy?

- Calculate increase in TP, FP, redundancy
- Organization specific
- Testing not organization specific!
- Measure/Predict relative security change

Am I secure?

- Given a set of products
- Specific attack dataset
- Measure how many attacks evade
- Find product(s) to fix
- Increase relative security

Challenges – Data Sets

- How to link ‘attacks’
- Define ‘attacks’
- Future attacks differ?

Challenges

- Not all attacks equal
- Past predicts future?
- Create a future data set?

Future Work - Experiments

- Require data sets
  - Linked attacks
  - Ground truth
- Drive-by downloads?
- Historical data?

Conclusion

- New metrics needed
- Security products are not isolated
- Many challenges, no show stoppers
- Measure relative security

CS@CU

Questions?