CERIAS

The Center for Education and Research in Information Assurance and Security

Development of Malware Analysis Techniques (Work in Progress)

Jaideep Juneja
Professor Marcus Thompson
Purdue University

Research Question:

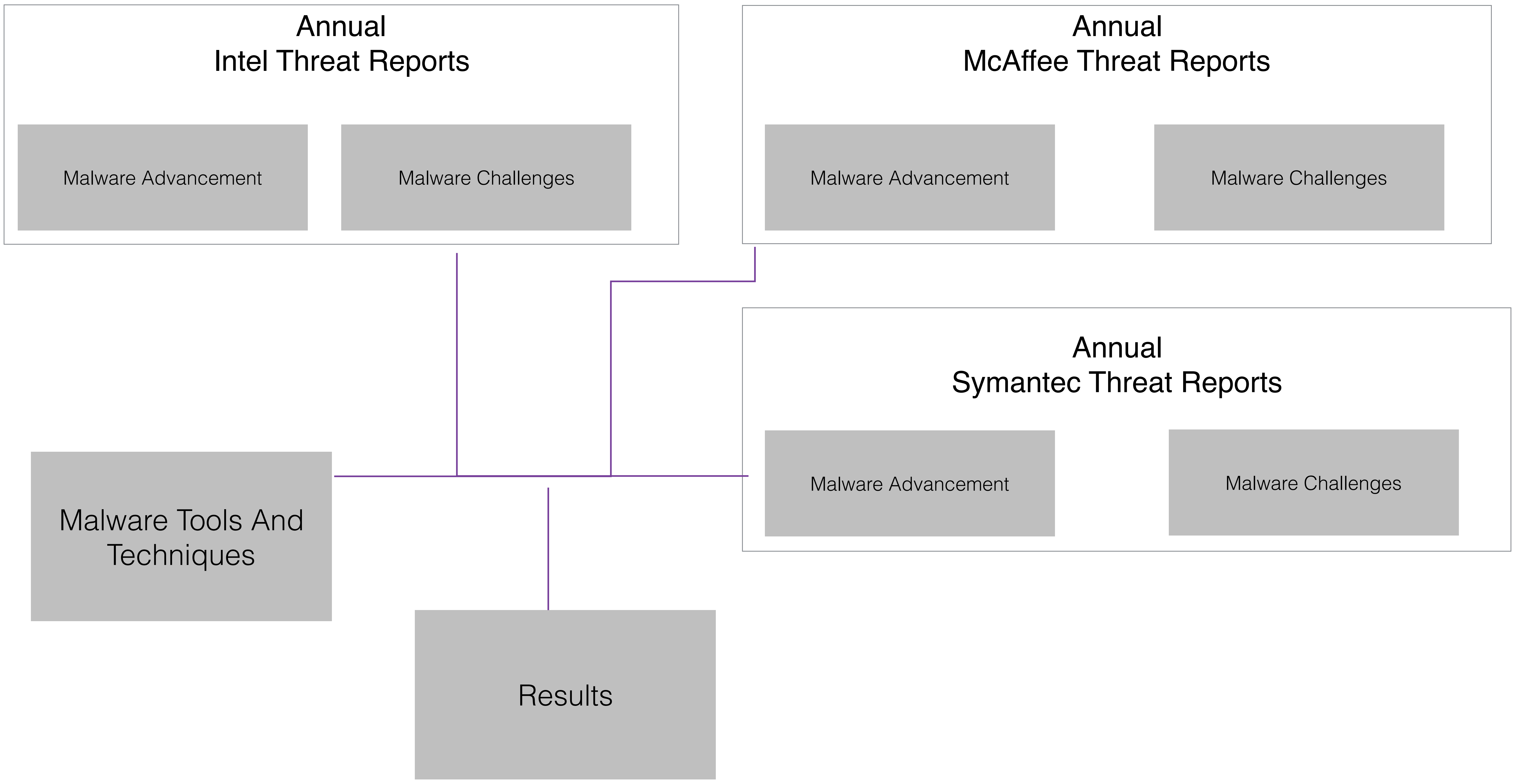
The sudden increase in new and unique malware, begs the question, are malware techniques keeping up with newer forms of malware. The hypothesis is that malware techniques are able to keep up with malware.

Direction:

The way to answer the research question is to look at the past and understand how malware has grown over the years. Further we must look at how malware analysis techniques are affected by new and improved malware. Lastly threat reports and malware challenges must be observed and tied together to get clear results

Methodology:

1) Obtain and analyze yearly threat reports
2) Find out the most common malware over the years
3) Understand the malware challenges and goals for the years 2008 to 2017
4) Observe the changes in challenges for the chosen period of time
5) Use the data to understand the time period taken to solve the challenges
6) Infer data from observations and answer the research question



Annual
Intel Threat Reports

Malware Advancement

Malware Challenges

Annual
McAffee Threat Reports

Malware Advancement

Malware Challenges

Annual
Symantec Threat Reports

Malware Advancement

Malware Challenges

Malware Tools And Techniques

Results