Project Description Form

MSc Information Security

TO BE COMPLETED BY THE PROJECT CANDIDATE

Name

Contact email address:

Provisional Title of Project: Defence in Depth: Is The Perimeter Working?

1. Statement of Objectives

a. I intend to achieve the following objectives

Introduction to the Perimeter

a. Introduce the basic principles of Defence in Depth
b. Introduce the ideology of Deperemiterisation
c. Introduce Malware attack methodologies.

Part 1 (Defence in Depth)

Discuss the current approaches to Defence in Depth incorporating the technological and business perspective and the drivers for this approach.

a. The Business and Information Security drivers of Defence in Depth
b. The requirements for Defence in Depth
c. The Methodology of Defence in Depth
d. Advances in Defence in Depth techniques
e. An analysis with regard to current attack trends within this scope.
f. The future of defence in Depth.

Part 2 (De-paramaterisation)

Discuss the concept of de-parameterisation and why the concept is being discussed with regard to the industry and security drivers for it. Furthermore, if possible, review implementations of de-parameterisation within industry.

a. The concept and thinking behind DP
b. The drivers for DP
c. Evaluate the Jericho Ten Commandments
d. Review Open Group White Papers
e. Investigate current market implementations and solutions of DP
f. Discuss the slow uptake of DP and the reasons for this reluctance.
Part 3 (Attack Trends)

Evaluate the advantages and disadvantages of both defence models. Analyse the attack models to which both approaches are susceptible.

a. Review current attack trends (OWASP Top Ten)
b. Investigate whether Defence in Depth protects adequately, in the context of Part 1, with regard to OWASP.
c. Hypothesize and investigate whether DP meets the security demands of OWASP
d. Evaluate the data and review

Part 4 (The Future)

Propose my thoughts and ideas to this problem.

a. Is Defence in Depth working in the context of this project and the future of this methodology
b. Is DP a viable solution and what is the future in this field
c. Do the two methodologies work in tandem and review this concept
d. Personal judgment and ideas within the realms of Information Security to a workable solution-time permitting.

Conclusion

Provide a conclusion to the stated introduction and summarise the key parts within the project. Outline whether the expected results from the Project mirrored the actual results achieved. Provide predictions within the project scope for the future.

b. Why have you chosen the proposed project?

I chose this project for many several reasons, these being:

a) During several of last semester’s lectures there have been interesting thoughts and ideas on how organizations should defend their assets. I feel this would be an interesting avenue to investigate.

b) There is and has been a lot of discussion in the industry press as to how solving this problem to which there seem to be two separate camps. I feel that by investigating the two ideas would be the basis of a good and interesting project.

2. Methods to be used
The objectives highlighted in the Introduction, Defence in Depth, De-perimeterisation, Attack Trends, The Future and Conclusion to Defence in Depth: Is the Perimeter working will be achieved by:

1) Read resource material on Defence in Depth.
2) Read Standards on Defence in Depth technologies and frameworks
3) Read resource material and Standards on Deperimetrisation. Main resources for this material are the Open Group/Jericho Website.
4) Review the OWASP Top Ten
5) Investigate and review literature on the latest attack models within the context of the objectives.
6) Liase with industry professionals.
7) Issue questionnaires to relevant professionals in relation to the specified objectives.
8) Interview personnel with regard to questionnaires and discuss their ideas and experiences on the subject matter within their scope.
9) Analyse and compile a report on all the information obtained within the earlier objectives
10) Outline and format Objectives (Parts 1 –3)
11) Investigate Objective 4 (The Future).

b. What is your strategy for getting started?

a) The strategy for getting started is to carefully plan the project within the main chapters outlined within the Statement of Objectives. This will formalise the structure of the argument and keep the scope of the project within reasonable and manageable limits.

b) The introduction will provide the reader with an overview of the different concepts being discussed to provide a baseline to which the reader can be inflected and engrossed to further delve into the main topic headers.

c) The main topics of discussion will then be further investigates within the context of the objectives to give the reader a more in depth understanding of the project argument.

d) To achieve this I will perform review the relevant material on a header by header case so as to build up a comprehensive understanding of the content and to aid the reader in understanding the chapter subject.
e) To provide analysis and review of the project and to add weight to the argument I will be liaising with industry, issuing questionnaires aranging interviews and where permitting review current infrastructures in industry. This is dependant upon response from Industry. I aim to achieve this by using prior industry exposure and ISG resources.

Gather resources and information

Books
- Stephen Northcutt and Judy Novak, 2000, Network Intrusion Detection. New Riders
- Dorothy E. Denning, 1999, Information Warfare and Security. Addison-Wesley

Journals

Websites
- http://www.opengroup.org/jericho
- http://www.appgates.com/knowledge_center/70_Deperimeterisation_Knowledge_Base/
- https://www.trustedcomputinggroup.org/home
- http://www.opentc.net/
- http://www.owasp.org/index.php/Main_Page

Questionnaires
- Depends upon level of response

Interviews
- Depends upon level of response

Architecture Revies
- Depends upon level of response

3. The work plan
Key milestones in the project.
TO BE COMPLETED BY THE PROJECT CANDIDATE

Name

Contact email address:

Provisional Title of Project: Defence in Depth: Is The Perimeter Working?

1. Statement of Objectives

a. I intend to achieve the following objectives

Introduction to the Perimeter

a. Introduce the basic principles of Defence in Depth
b. Introduce the ideology of Deperemiterisation
c. Introduce Malware attack methodologies.

Part 1 (Defence in Depth)

Discuss the current approaches to Defence in Depth incorporating the technological and business perspective and the drivers for this approach.

a. The Business and Information Security drivers of Defence in Depth
b. The requirements for Defence in Depth
c. The Methodology of Defence in Depth
d. Advances in Defence in Depth techniques
e. An analysis with regard to current attack trends within this scope.
f. The future of defence in Depth.

Part 2 (De-parameterisation)

Discuss the concept of de-parameterisation and why the concept is being discussed with regard to the industry and security drivers for it. Furthermore, if possible, review implementations of de-parameterisation within industry.

a. The concept and thinking behind DP
b. The drivers for DP
c. Evaluate the Jericho Ten Commandments
d. Review Open Group White Papers
e. Investigate current market implementations and solutions of DP
f. Discuss the slow uptake of DP and the reasons for this reluctance.
Part 3 (Attack Trends)

Evaluate the advantages and disadvantages of both defence models. Analyse the attack models to which both approaches are susceptible.

a. Review current attack trends (OWASP Top Ten)
b. Investigate whether Defence in Depth protects adequately, in the context of Part 1, with regard to OWASP.
c. Hypothesize and investigate whether DP meets the security demands of OWASP
d. Evaluate the data and review

Part 4 (The Future)

Propose my thoughts and ideas to this problem.

a. Is Defence in Depth working in the context of this project and the future of this methodology
b. Is DP a viable solution and what is the future in this field
c. Do the two methodologies work in tandem and review this concept
d. Personal judgment and ideas within the realms of Information Security to a workable solution-time permitting

Conclusion

Provide a conclusion to the stated introduction and summarise the key parts within the project. Outline whether the expected results from the Project mirrored the actual results achieved. Provide predictions within the project scope for the future.

b. Why have you chosen the proposed project?

I chose this project for many several reasons, these being:

a) During several of last semester’s lectures there have been interesting thoughts and ideas on how organizations should defend their assets. I feel this would be an interesting avenue to investigate.

b) There is and has been a lot of discussion in the industry press as to how solving this problem to which there seem to be two separate camps. I feel that by investigating the two ideas would be the basis of a good and interesting project.

2. Methods to be used
The objectives highlighted in the Introduction, Defence in Depth, De-perimeterisation, Attack Trends, The Future and Conclusion to Defence in Depth: Is the Perimeter working will be achieved by:

1) Read resource material on Defence in Depth.
2) Read Standards on Defence in Depth technologies and frameworks
3) Read resource material and Standards on Deperimetrisation. Main resources for this material are the Open Group/Jericho Website.
4) Review the OWASP Top Ten
5) Investigate and review literature on the latest attack models within the context of the objectives.
6) Liase with industry professionals.
7) Issue questionnaires to relevant professionals in relation to the specified objectives.
8) Interview personnel with regard to questionnaires and discuss their ideas and experiences on the subject matter within their scope.
9) Analyse and compile a report on all the information obtained within the earlier objectives
10) Outline and format Objectives (Parts 1 –3)
11) Investigate Objective 4 (The Future).

b. What is your strategy for getting started?

a) The strategy for getting started is to carefully plan the project within the main chapters outlined within the Statement of Objectives. This will formalise the structure of the argument an keep the scope of the project within reasonable and manageable limits.

b) The introduction will provide the reader with an overview of the different concepts being discussed to provide a baseline to which the reader can be inticed and engrossed to further delve into the main topic headers.

c) The main topics of discussion will then be further investigates within the context of the objectives to give the reader a more in depth understanding of the project argument.

d) To achieve this I will perform review the relevant material on a header by header case so as to build up a comprehensive understanding of the content and to aid the reader in understanding the chapter subject.
e) To provide analysis and review of the project and to add weight to the argument I will be liaising with industry, issuing questionnaires aranging interviews and where permitting review current infrastructures in industry. This is dependant upon response from Industry. I aim to achieve this by using prior industry exposure and ISG resources.

Gather resources and information

Books
- Stephen Northcutt and Judy Novak, 2000, Network Intrusion Detection. New Riders
- Dorothy E. Denning, 1999, Information Warfare and Security. Addison-Wesley

Journals

Websites
- http://www.opengroup.org/jericho
- http://www.appgate.com/knowledge_center/70_Deperimeterisation_Knowledge_Base/
- https://www.trustedcomputinggroup.org/home
- http://www.opentc.net/
- http://www.owasp.org/index.php/Main_Page

Questionnaires
- Depends upon level of response

Interviews
- Depends upon level of response

Architecture Revies
- Depends upon level of response

3. The work plan
Key milestones in the project.
January to June 2007
Read resource materials and liase with Project Supervisor.
Compile questionnaires
Approach industry and issue questionnaires.
Interview industry personnel
Compile reports from industry feedback.

July 2007
Compile draft copy and submit to Project Supervisor
Liase once fortnightly with Project Supervisor with regard to project review and development.

August 2007
Resubmit edited copy and obtain feedback from Supervisor
Liase once fortnightly with Project Supervisor

September 2007
Submit final draft

4. Additional Information

Use this section to make extra comments on the proposal on matters not covered above (use extra space if necessary). Include details of any involvement of external organisations.

The gathering of information from Industry is not a key element to this project and has been planned as such. However, with input from Industry and depending upon feedback and response I feel will increase depth of this project. This will assist in the researching of De-perimeterisation as it is a relatively new concept with limited literature available.
As stated though Industry input will be beneficial but the Objectives stated can be met without Industry input.
TO BE COMPLETED BY THE PROJECT SUPERVISOR

I approve the attached project plan.

Signed:

Name:

Date: