# Homework 1

See Canvas for grade %

## Due Date

See Canvas for date

## Academic integrity pledge

I agree to complete this assignment without unauthorized assistance from any person, materials, or device. Fill in your full name, JHU email address, and today’s date in the table below.

|  |
| --- |
| Full name  JHU email address |

Deliverable -Academic integrity pledge

## Summary

Threat modeling is a technique meant to improve the effectiveness of a security assessment. By thinking from the perspective of the attacker, security analysts can identify components in a system that would have the highest risk of attack. These components should have priority in security assessments.

Network architectures support network security and are commonly described using network data flow diagrams. These diagrams include major network components (e.g., routers, switches, employee workstations, servers, firewalls, etc.) and the network data flow between them and include mechanisms for security.

### Part 1

Construct a threat model for the following simple network. Provide recommendations for mitigating risks associated with the identified attacks. You may neatly draw it by hand, or use a dedicated tool (Microsoft TMT or OWASP Threat Dragon).

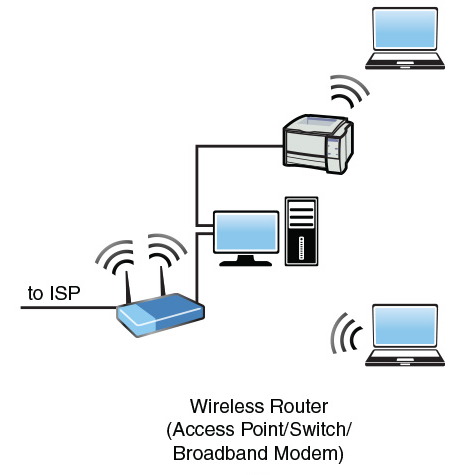


Figure -Simple network from Networking Essentials, Beasley and Nilkaew

### Part 2

Congratulations, you are responsible for conceptualizing the network architecture for a startup company that has created a novel, online, multi-player gaming concept!

First, draft a list of requirement statements that would go in a simple network security policy. Include high-level statements that specify what is allowed/not allowed on the networks by employees (distinguish between normal user and administrator) and customers. E.g., all devices connected to the University network must be properly registered.

Next, construct a conceptual network data flow diagram and separately, a functional description of the overall architecture, and functional descriptions of the individual nodes (for repetitive nodes, it is fine to describe a single instance and indicate that it repeats). The architecture should include external customer devices, externally connected employee workstations (e.g., employees telecommuting from home or connecting in when on business travel), and a corporate network. Furthermore, the functions and nodes should be vendor and OS agnostic. E.g., customer computer, employee laptop or workstation, wireless access point, router, switch, firewall, email server, web server, game server, authentication server (password and multifactor authentication tokens), intrusion detection system (packet inspection), policy server, DHCP server, DNS server, proxy server for employees accessing external websites, honeypot, SIEM (security information and event manager), logging server, archive server (e.g., development repository server), certificate authority (local CA, as well as external root, regional, and CAs), backup server, VPN server, VPN client applications running on corporate laptops that may be taken home or on business travel, multifactor authentication token generator applications (running on employee-owned devices), virus detection on devices, personal firewalls and host intrusion prevention software on devices, software update servers, etc.

When designing the architecture, consider threats to all of the security tenets and make the design resilient. E.g., what happens if there is a fire in a server facility and it is not usable for months, or if a particular server is undergoing a DDOS attack and cannot perform its functions? In addition to the obvious external threats, you should consider threats from insiders.

The following sequence is recommended for those unfamiliar with constructing a data flow diagram. First, review several example diagrams (e.g., some examples from Cisco design guides are below). Next, create a listing of everything that you want to include in the diagram. Then, on a whiteboard, start drawing nodes that represent things that will be included and what they connect to. Try to arrange nodes so that you don’t have intersecting lines and it is typically helpful to place nodes that have interconnecting data flows nearby each other. It is fine to describe the architecture using multiple diagrams (e.g., hierarchically decomposed or geographically segmented) and you may either provide scanned images of your hand-drawn diagrams, or alternately be creative in locating and using free diagramming tools to draw digitally (e.g., yEd is very nice and freely available, <https://www.yworks.com/products/yed>). For yEd, there is a set of network palettes available at <https://github.com/gowenrw/yEd_network_palettes>.

Additional advice:

1) consider the business needs for the scenario listed; construct a list of these needs (e.g., customers need to access the game server over the internet)

2) consider the attack scenarios discussed in class and in the readings; construct a list of viable attack scenarios (e.g., attacker could exploit the game server over the internet connection)

3) understand the functions of all the devices in the list provided; for devices that implement mechanisms that support security tenets, understand how these mechanisms are effective in mitigating security risks (at least at a high-level); for devices that implement general business needs, understand what devices support particular needs (e.g., an employee workstation that is attached to internal networks is needed for developers to create maintenance patches when a bug is identified)

4) conceptualize an architecture that a) provides the business needs and b) reduces security risks for viable attack scenarios

5) There are several example network diagrams at the end of this document

## Requirements

### Executive summary briefing

These summaries (5-8 minute briefing) are intended to be reference material for when you are performing threat modeling in practice and must contain an overview of the project, the project goals, project execution highlights (i.e., what was performed, with pertinent technical highlights), what goals were accomplished (and any that were not achieved), and what was learned from the project. For the presentations, you may choose your own style (PowerPoint is recommended) but you must submit recordings via Panopto and provide digital copies of the slides. Slides for summary briefing are submitted on Canvas with the deliverables in the \*.zip described below. Summary briefing recordings are submitted on Canvas via Panopto.

### Technical deliverables

For this assignment, place all products in a single zip file and submit it for the deliverables. Provide answers to any questions and requests outlined below in a copy of this Microsoft word document that is also included in the deliverables zip file. For example, place supplementary images (e.g., an image of the high-level threat model and your network architecture graphics) and any other answers where they are requested in this document. Include in the high-level threat model file and network architecture files (e.g., yEd project file) as attachments in the \*.zip as well.

### Deliverables

Part 1

Provide a scanned image of your threat model, or a screenshot of it, in the table below.

|  |
| --- |
|  |

Deliverable -Threat model

Using complete sentences, provide your bulleted list of recommendations for mitigating risks associated with the identified attacks in the table below.

|  |
| --- |
|  |

Deliverable -Recommendations

Part 2

Using complete sentences, provide your bulleted list of 15 requirement statements that would go in a simple network security policy in the table below.

|  |
| --- |
|  |

Deliverable -Requirement statements

Provide a scanned image of your conceptual network data flow diagram, or a screenshot of it, in the table below.

|  |
| --- |
|  |

Deliverable -Network diagram

Using paragraph form, provide a functional description of the overall architecture, and functional descriptions of the individual nodes in the table below.

|  |
| --- |
|  |

Deliverable -Functional description

## Grading Rubric

### Threat modeling deliverables (85% overall)

* Threat model – 15%
  + If using a tool, provide an attachment with the model in your deliverables.
  + Must include at least one generic data store (asset), one generic external interactor, one generic data flow, three generic processes, and one trust boundary. Each must be unique.
* Recommendations for mitigating risks associated with the identified attacks – 10%
  + Must include at least three risks and corresponding mitigations
* Provide a list of at least 15 requirement statements that would go in a simple network security policy – 25%
* Provide a conceptual network data flow diagram with at least 30 unique nodes – 20%
  + Include all the 25 node types listed in sensible locations – 5%
  + Provide an attachment for your diagram in your deliverables.
* Provide a functional description of the overall architecture, and functional descriptions of the individual nodes – 25%
  + At least 3 paragraphs, with 4-5 sentences per paragraph

### Executive briefing (15% overall)

**Table 0.1-Executive briefing grading rubric**

|  |  |  |  |
| --- | --- | --- | --- |
| **Objective** | **1 - Exemplary** | **2 - Proficient** | **3 - Apprentice** |
| Format / layout / organization | Brief is very clear, coherent with excellent transitions | Brief is clear and coherent, strong throughout | Brief has some gaps, some weak sections |
| Slides | All figures and tables are easy to understand, and are clearly linked to the brief.  Story can be told almost entirely through figures. | All figures and tables can be understood with information given and are linked to brief.  One or more need improvement. May need more figures to tell the story. | Figures and/or tables are hard to understand, are not all linked to brief.  Several need improvements.  Several more figures are needed to tell story. |
| References | All sources identified and referenced appropriately.  Evidence of careful and thorough research for outside information. | All sources identified and referenced appropriately.  Includes mostly readily available works. | All sources identified.  Only readily-available works included.  Some weaknesses in referencing, such as missing publisher information. |
| Typical Grade (average): | 90-100% | 80-90% | 70-80% |

## References and useful resources

* NIST Computer Security Resource Center SP-800 series publications, [website](https://csrc.nist.gov/publications/sp800)
* Cisco design guides with example network diagrams
  + [Campus LAN/WLAN Design Guide](https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Campus-LAN-WLAN-Design-Guide-2018JAN.pdf)
  + [Data Center Design Guide](https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-DataCenterDesignGuide-AUG14.pdf)
  + [Internet Edge Design Guide](https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Oct2015/Internet_Edge_Design_Oct2015.pdf)
* 2005a, Meier et al., Improving Web Application Security: Threats and Countermeasures, [Ch. 3, Threat Modeling](https://msdn.microsoft.com/en-us/library/ff648644.aspx)
* 2005b, Meier et al., Improving Web Application Security: Threats and Countermeasures, [Ch. 2, Threats and Countermeasures](https://msdn.microsoft.com/en-us/library/aa302418.aspx)
* [2014, Shostack, Threat Modeling: Designing for Security](http://proquestcombo.safaribooksonline.com.proxy1.library.jhu.edu/book/networking/security/9781118810057) (Safari)
* <https://github.com/matthiasrohr/OTMT> (Contains several example threat models)
* <http://cyberspaceandtime.com/Threat_Modeling_Lessons_from_Star_Wars_(and_Elsewhere)/KLpgaoD8ySM.video> (Shostack video on threat modeling)
* 2006, Leydens, Santi, “Optimizing Faculty Use of Writing as a Learning Tool in Geoscience Education” (provided the rubric specified for the executive summary report)
* 2016, Microsoft, Microsoft Threat Modeling Tool 2016 User Guide

## Example network diagrams

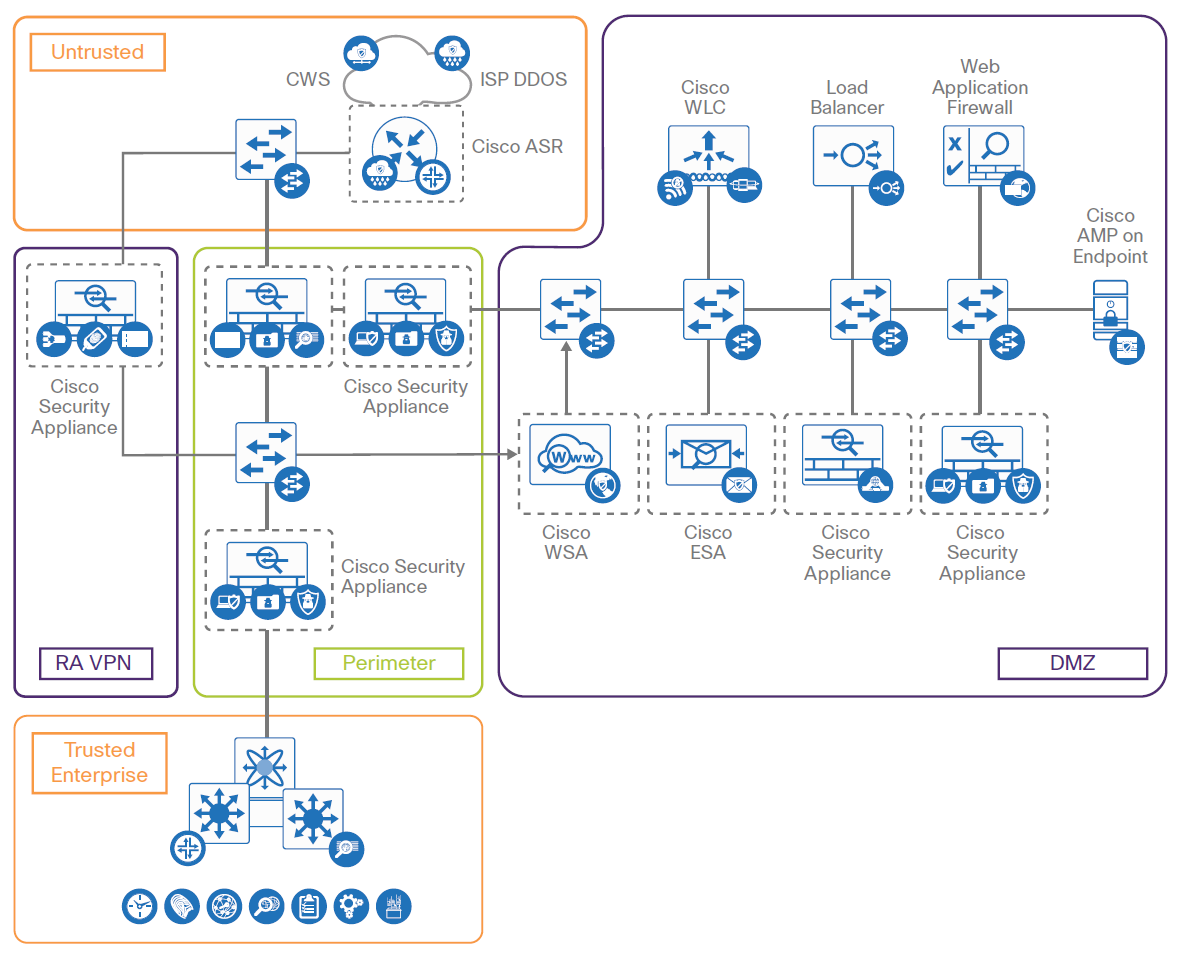


Figure -Internet edge design guide illustration

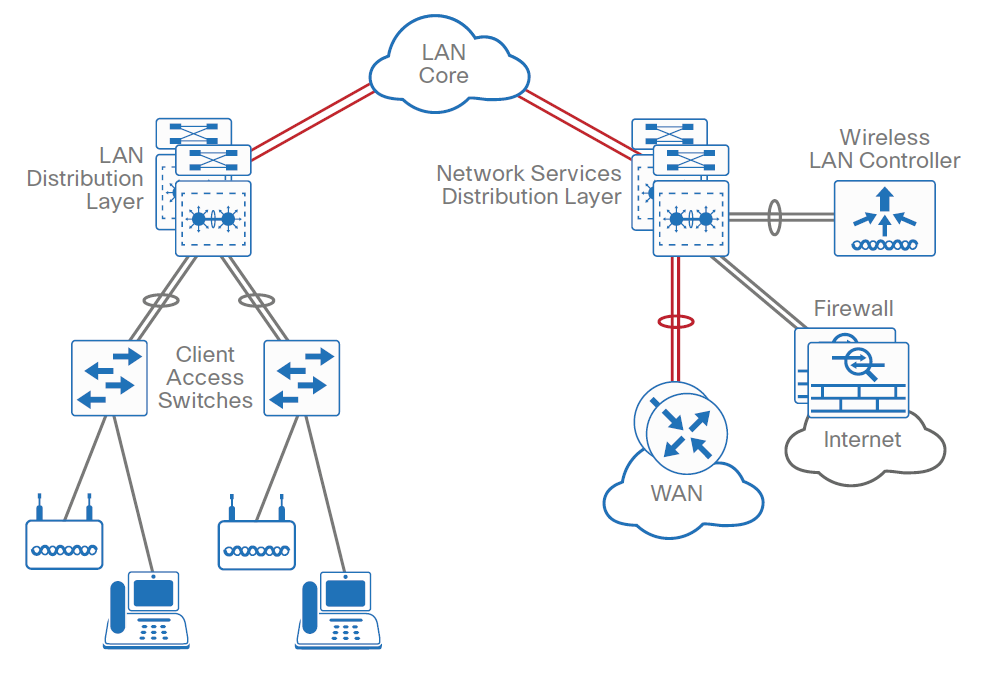


Figure -LAN/WAN design guide illustration

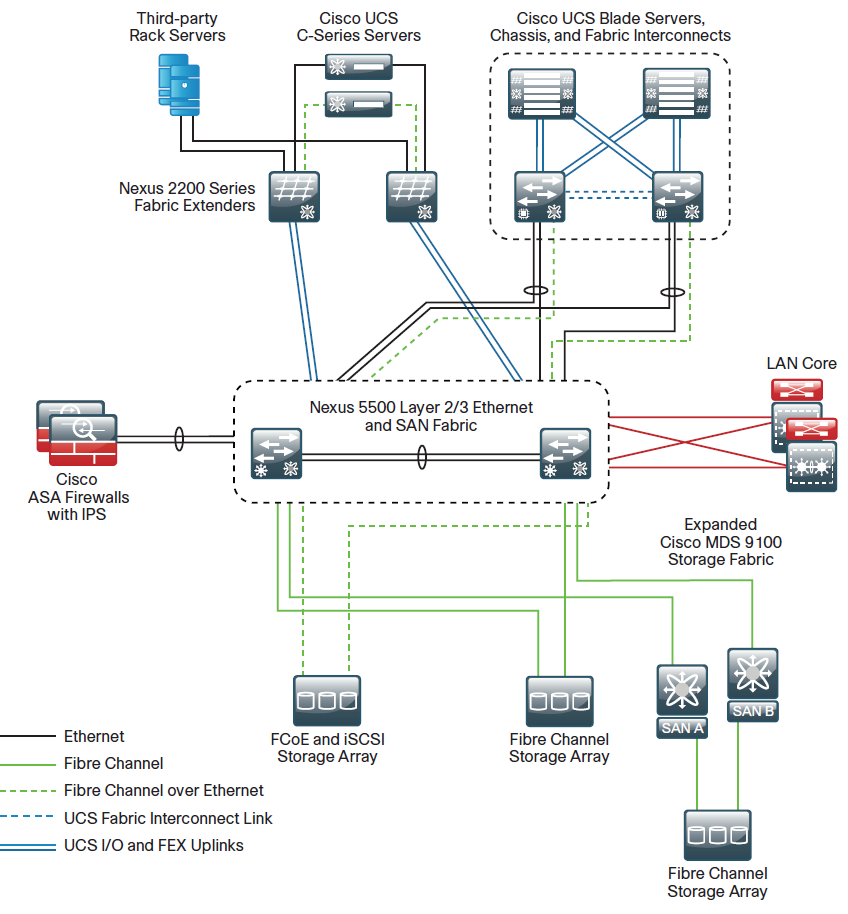


Figure -Data center design guide illustration