Tu Lam

CS 373 (Defense Against the Dark Arts)

Dr. Bram Lewis

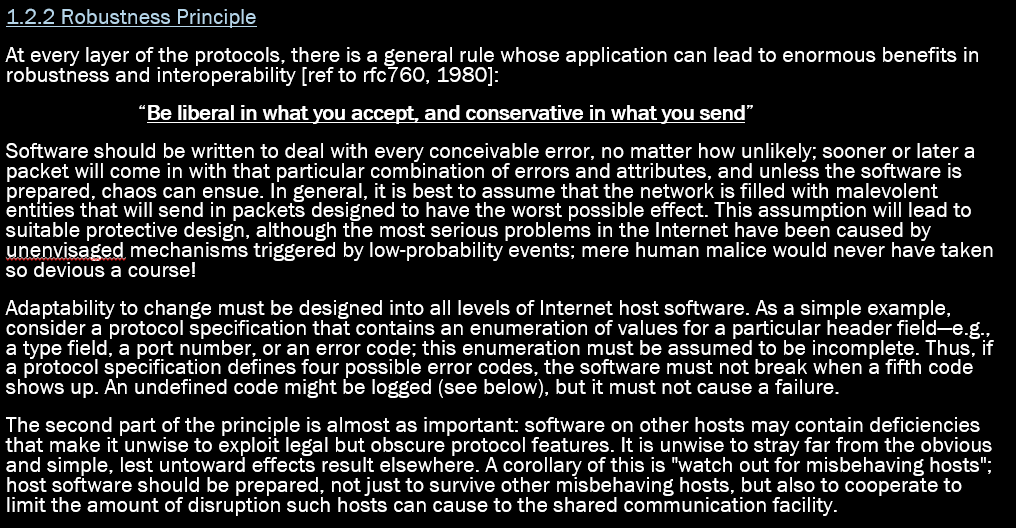
November 1st, 2021

# Homework #6 Write-Up

Week #6 of the class have two special guests; their name was Ram Venugopalan and Geoffrey Cooper. They both works for Intel as Intel Security. Through this week lecture, we will be dealing with the ***network security*** basic on the topic of the ***threats and defenses***. We will also dive into the topic of ***robustness principle***, and the ***firewall exercise*** they have as example.

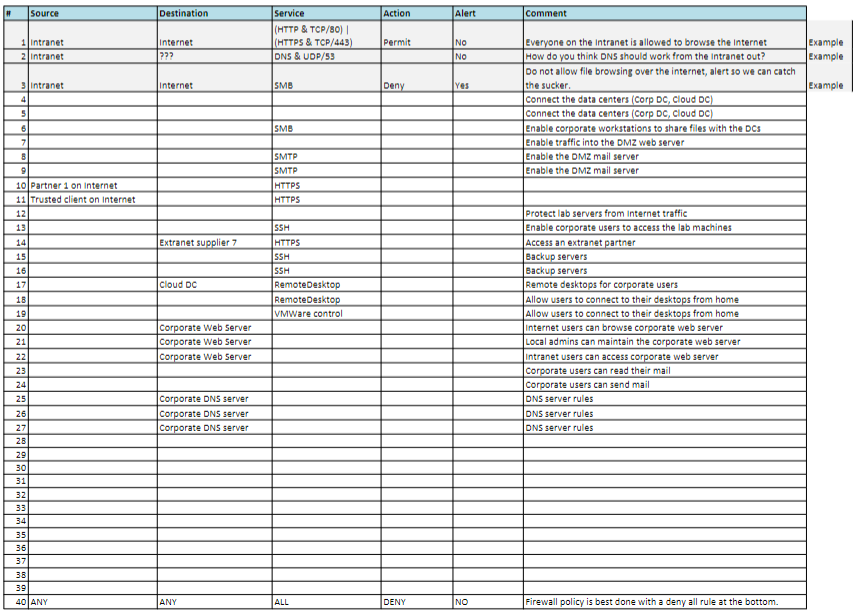
First, the duo introduces on the topic of general basic on how ***network security*** is important. The idea that network security is important is that they do ***host-based protections***,where it protects the system from being attack by outside host entering in the system. It also tries to protect harmful data entering in the system also, basically following the kindergarten’s rule. They identify that threat can come in two ways, ***in or on the network***. For the in network, this can come in form of DDoS, stack overflow, or Morris Worm. For on network, it is more on the worms, theft of network, botnets, and more. With these threats in mind, this is why defenses that we have right now is a good fit for protecting the network security. These are some of thing we will be seeing like ***Firewall / Security Zones***, ***Intrusion Detection***, ***Honeynets***, ***Quarantine***, and more.

Moving on, the lecture move onto the content of ***robustness principle***. This principle talks about the basic of computer and how they are supposed to be prepare as it comes to threat that it has to be able to adapt to change when things are being update on or prepare in the worst situation as possible. There’s a quote from this principle that said “***Be liberal in what you accept, and conservative in what you send***”. This basically detailing that be open-minded and on what you accept into the system, but be careful of what you send out. Below is a figure of the principle that will go into more detail about the robustness principle and see what is going on.



*Figure #1*: [**From Lecture**] *The basic of the robustness principle*

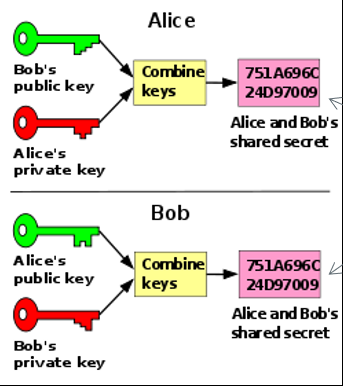
To the next topic, we talk about ***positive policy*** (AKA ***whitelisting***). This is a defense use for network where we define on what ***expect or allow to happen*** inside the system. This way we can give rule that will hopefully eliminate any threat/suspicious thing trying to enter the network. The rule with this is that it is still a policy and it is use to *detect* a threat, but cannot *name* them. Then onto the ***firewall / security zone***, we common implement this to define zones in the network with policy between the zones. With this, we can see that ***firewall*** sit in between the zone and the filter traffic for the policy. Using this, we can have a little fun on a firewall exercise to see what policy we can determine from it, through this exercise we were able to think and try to think what kind of policy per zone would do and what its limitation may be. Below will be a image of what the layout of the exercise will look like.



*Figure #2*: [**From Lecture**] *Displaying the example of the Firewall exercise*

Next, we look into the ***defense depth*** and how it looks like a castle and there is various way the network defense is build on top of each other. Then moving to ***intrusion detection***, this method is using signatures/anomaly detection to detect attack coming into the network. Then another way to protect ourselves from network harm is ***Honeynets***. Through this technique, we devise a phony network to distract the attacker and keep them distracted by slowing them down from entering into the real network. Then there’s the concept of ***quarantine*** where we place the infected part inside a space of containment and they can’t infect other while in this space. Finally, we have ***reputation*** as it collects data of list in good and bad thing from the attack and send it to the cloud to be further look at for later use down the road.

The next part in the lecture dive into detail about the ***middle man*** where the concept of someone in the middle that intercept the content and may change, add, or delete whatever the content has. Some middle man can be good and some can be bad. Some of the bad one is ARP poisoning and TCP hijacking, while the good one is HTTP proxy, mail proxy, SSL MITM, and more. There is a great example of a good middle man that was mention in lecture as you shared keys with each other. Each person will have the other person private key and then with their public key combine with the other person private key, they can unlock the content that was encrypted. Below is a figure showing the concept of the shared key system.



*Figure #3*: [**From Lecture**] *Showing the concept of shared keys*

Moving on, we have ***reconnaissance*** where it divides to being passive and active. The passive side looks at wanting to see data on the network, while the active side wants to attack vulnerable machines on a network. Some of the tools have reconnaissance where it does basic scanning and try to connect to network and try to find many hosts and services. Then we learn about ***spoofing***, this is where the attacker masquerades as another network entity in order to gain some advantage over the network defenses of the target. A way a defense has been able to protect this is through reverse path filter as a way of defending from spoofing.

To wrap it up, we then dive into some of the technologies that are out there and still in the stage of developing hoping to create a better future for the cybersecurity. We look at things from Evader tools, SDN, and more. Through this, we can develop a more powerful defense against attacker attacking on the network system and learn to protect them.

Overall, this week gave us a lot of glimpse into the power of network system and learning the control behind the scene work. With this in mind, we can take the time and dedication with some of these techniques that the world of cyber security has protected us from threats that could be harmful throughout our daily life usage of technology.

# References

1. Venugopalan, R., & Cooper, G. (2015). *OSU - Network Security* . Canvas - Oregon State University . Retrieved November 1, 2021, from <https://canvas.oregonstate.edu/courses/1877198/pages/module-6-learning-materials?module_item_id=21556814>.