Research at WSU

I would like to work in research under (Zhe Dang) they primarily studied computer science, and their recent main work publications seem to be on the topic of RFID systems. RFID systems seem to be a form of identification such as a bar code. The publication used for the introduction of RFID systems is "*RFID systems: Research trends and challenges*" (Boliac et al, 2010). RFID identification technology seems to have an advantage which pushed for its advancement. The use of RFID has a variety of applications that it can range from.

What exactly is an RFID system and what does it do? In (Boliac, 2) the author states "RFID is a wireless technology that allows for automated remote identification of objects". This wireless technology alike to the barcode because both use some sort of identifying signature and a reader which confirms it. The main difference between these two is RFID uses radio frequencies and a barcode uses infrared frequencies. An RFID system in this case should be able to operate faster since it outputs radio frequencies.

One of Zhe dang recent publications I have read is "*A Near-Optimal for the Grouping Problems in RFID Systems".* What I understood from this publication is that an issue occurring with RFID systems is the grouping of an unexpected tag. This issue gives unexpected tags low accuracy of being identified correctly and seem to have a delay because of how much utilization they have on servers. Current designed protocols for this are still lacking, which is an issue because on some occasions where there is a well sized batch of tags entering and leaving leads to new arriving tags not being identified slowing down the process. In common of presented protocols, they share similarity of not being able to handle 3 major drawbacks such as unexpected tags and server utilization. The optimal solution for the tag protocol seemed to be theoretical which ends up using less networking resources and the ability to work in a higher scale and was faster.

This Reasearch about Rfid systems is fascinating to me because using a scanner with radio frequencies which has a range of meters identifying tags. While it still did have issues the research proposed a protocol which could fix or improve the major drawbacks of previous protocol. The research was able to solve the issue with unexpected tags and grouping ID's which could cause an unexpected time delay attempting to identify. It's also fascinating how they were able to lessen the computational burden on the servers.

Another person I would like to work under is Ananth Jillepalli. They work in computer science with some computer engineering. Going through the description of their recent publications I can infer his line of interest lies within cyber security. Cyber security is mainly about how to keep yourself or others safe while on the internet. The reading I am obtaining a greater understanding of cyber security and how it happens is "A survey of emerging threats in cybersecurity" (Julian, et al). Cyber-attacks can cause disruption and information leaks depending on what is being attacked the more troublesome it is. The attacks target information and can range from government, business, personal, video games and more.

When a company or government gets attacked by hackers of some sort, they can end up losing money because of it. Why do they happen? Well in short, as explained by the author within the introduction of a survey of emerging threats in cybersecurity cyber-attacks are less costly than real attacks because the main access point of a cyber-attack is accessibility to the internet. The factor of the internet gives them a wide range of places to attack. These attacks can come as malware, ransomware, as well as vulnerabilities from applications, websites, and your own operating system. It is always good to have a way to check for possible threats such as windows defender and check for software you don't remember installing. After time, like a real virus attackers can find other entries after being blocked also as software's updates, they may also bring new vulnerabilities.

One of their recent publications of Ananth Jillepalli that I have read is "*Trustworthy High-Performance Multiplayer Games with Trust-but-Verify Protocol Sensor Validation*" what I understood from this publication is although the video game industry is big developers of multiplayer online games sacrifice security for performance goals which opens space for exploits, and cheats. Depending on the game these cheaters could either use it for their own fun or to make some money from it. Different games have their own corresponding response time usually called ticks which shows how many times the server receives and sends information to update for all players. A way game companies make up for the low security in their games is by using clients' games such as War Thunder, Apex legends, call of duty, two examples of anti-cheat clients are easy anti-cheat and Ricochet. The proposed anti cheat sensor is efficient while having low delays and won't affect game experience the anti-cheat system takes a look at inputted keys and looks for unnatural behaviors and I believe the system tracks offences you have committed and decides on its own to ban or penalize the player.

This fascinating to me because I did not know video game anti cheat systems differ in protection on what the tick server rate is. It was also not to my attention that developers' lower security in a game to improve performance. A system such as the one proposed is interesting because it accounts for the users' inputs and hides the Ip of the player using encryption. There is an interesting false positive included such as rage clicking, this could end up being an issue since players may end up clicking buttons repeatedly depending on the game. Also, because it is only looking at input's cheater may still be able to use different exploits such as noclip or flying since it's not looking at the player location it may still be seen as a regular input.

Bibliography

Bolić, Miodrag. *RFID Systems: Research Trends and Challenges*. Edited by David Simplot-Ryl and Ivan Stojmenović, Wiley, 2010.

https://books.google.com/books?hl=en&lr=&id=VansInOpixEC&oi=fnd&pg=PP9&dq=RFID+systems:+Research+trends+and+challenges&ots=eUPPwTBiVK&sig=CgZmswgHhqU0fWYB85A-ipV-lSU#v=onepage&q=RFID%20systems%3A%20Research%20trends%20and%20challenges&f=false

Jang-Jaccard, Julian. “A Survey of Emerging Threats in Cybersecurity.” Edited by Surya Nepal, Journal of Computer and System Sciences, Academic Press, 10 Feb. 2014,

www.sciencedirect.com/science/article/pii/S0022000014000178. Accessed 04 Oct. 2024.