IT Advancement and related threats

Student name

[Institutional Affiliation(s)]

**Investigating on SI Teachable dynamic calibration of instrumented charpy strikers – Activities performed at NIST in FY2019**

 In recent years, at NIST investigations have been conducted towards an SI-traceable dynamic calibration of instrumented charpy strikers. Though, these tests last only for a few milliseconds, pointing towards the phenomenon. Different approaches have been considered for dynamic calibration that includes methods which were implemented in NIST previously and these methods have become common due to their use as standard. One of the key purposes of investigations is that calibration could be traceable to international systems of units (Vlajic & Chijioke, 2016). Accomplishments and activities of this project are given in detail in the Technical Note, during FY2019. A Summary of processes and activities conducted has been mentioned in the NIST, TN that was issued in May 2018 under the title “Investigation on SI-Traceable Dynamic Calibration of instrumented Charpy Stickers. Second aim that has been presented in this article is assuring the optimization of the design of the instrumented Charpy Stickers. In this paper author claims, “*Design Considerations to Optimize Charpy Instrumented Strikers”*

**Facebook improve political Ad transparency but refuses ban**

 In this article, new capabilities of Facebook and criticism on them have been highlighted. Increasing number of the political and social ads would be controlled by the social media users as they could remove the ads from the list that are not of their interest. This option has been introduced as most of the political campaigns were using Facebook for targeting the voters are influencing to vote for them, but the social networks refuse such ads to join and were banned as users were against such ads that were in favor of n certain political campaigns (Browne, 2020). Twitter has also banned political ads and Leathern doubled down this refusal and said “*Frankly, we believe the soon Facebook and other companies are subject to democratically accountable rules on this the better”*. Different negative aspects of online political advertising could also chip away at the legitimacy of election results, particularly in case of micro-targeted ads. According to the rights groups there is a check on the accuracy and rules applied to advertisers so that baseless political agendas without repercussions could be checked upon social media.

**Juniper networks releases security updates**

 Juniper Network has released updates so that it could address multiple vulnerabilities in different Juniper products. There are chances and the affected system could be attacked by remote attacker who may exploit some of the vulnerabilities for taking over the control of the whole system. Juniper Identity Management Service aims to collect and maintain database of the user, group and the device from Active Directory domains. In this article, the author also claims that Juniper obtain identity information so that it could enforce the appropriate policy for securing the confidential information before taking decision to deny or permit access (Juniper Networks Releases Security Updates, 2020). Central purpose of Juniper is to protect corporate internet and resources. It does not deconflict certain notifications and states, “*synchronize directory service data*”. Juniper protects against certain denial-of-service (DoS) flood attacks which are trigger by SRX Series device due to bursts of the queries linked to the unknown IP addresses.

**Privacy-preserving detection of Inter-Domain SDN Rules overlaps**

 SND approaches to inter-domain routing promise to deliver the best of the services i.e. better traffic engineering, higher automation and enhanced security etc. Though SDN has been introduced in internet field yet there has been mentioned dangers of its use as it allows fine-grained rules which deflect traffic from BGP’s default routes. This negative aspect would lead towards mismatching and results in forwarding black holes and loops etc., ultimately hindering the SDN deployment at inter domain level as safety comes first. This work is about the steps taken for the verification of the correctness of inter-domain so that loop freedom could be focused while considering the SDN rules (Dethise, Chiesa, & Canini, 2017). At the end of this study, a primitive but powerful and simple design has been given that would verify whether there is overlapping of the SDN rules or not. Objective of this experimentation is to introduce advancement in Secure Multi-Party Computation which is then detailed as the building block for designing a system for detecting internet-wide forwarding loops among any of the set of SDN-enabled Internet eXchange Points. “*A privacy-preserving primitive to the rescue!”*

**Interpol reduces cryptojacking infection by 78%**

 Interpol is celebrating reduction in the numbers of the routers that were infected with cryptomining malware. In this article, details have been given regarding operation Goldfish Alpha which begin in June 2019 after the confirmation of the compromised routers in the ASEAN region blamed for almost 18% of global infection (Muncaster, 2020). Aim of launching this operation was to locate the infected routers along with alerting the victims so that harms could be minimized to its best by patching the devices. All these efforts led to the reduction of the 78% infected routers and police also supported Cyber Defense Institute and Trend Mirco for collecting and analyzing the information. Police also provided necessary guidelines for patching the compromised routers and avoiding the future infections. Craig Jones said, “*When faced with emerging cybercrimes like cryptojacking, the importance of strong partnerships between police and cybercrime industry cannot be overstated”.* According to this study, hackers may use and manipulate the data as malware infection involves different type of risks. Footprint could also be used in hacking the homes machines by the hackers.

**Outline**

*Introduction*

* First of all a topic has been selected linked to IT field (IT advancement and related threats).
* IT is advancing in world as today there is not even a single field where information technology, its approaches, its tools and instruments are not used.

*Discussion*

* In this assignment, different articles have been selected linked with IT, its use and possible threats.
* Considering the advancement of IT, it could be said that threats are equally increasing as it could be misused.
* Different IT houses are selected as it system are getting hacked.
* Confidential information but different software houses are tiring their best to secure users.
* Articles selected are linked with privacy, challenged use of IT in different fields.

Conclusion

* In the selected articles, suggestions and solutions are given in one way around.
* IT infection has been spotted and treated as per the possibility.
* Cyber issues are also highlighted that points towards threats of IT advancement.

References

Vlajic, N., & Chijioke, A. (2016). Traceable dynamic calibration of force transducers by primary means. *Metrologia*, *53*(4), S136.

Browne, R. (2020). Facebook says it will let users see fewer political ads — but still refuses to fact-check them. Retrieved 10 January 2020, from <https://www.cnbc.com/2020/01/09/facebook-will-let-people-see-fewer-political-ads-ahead-of-us-election.html>

#### Juniper Networks Releases Security Updates | CISA. (2020). Retrieved 10 January 2020, from <https://www.us-cert.gov/ncas/current-activity/2020/01/09/juniper-networks-releases-security-updates>

Dethise, A., Chiesa, M., & Canini, M. (2017, August). Privacy-Preserving Detection of Inter-Domain SDN Rules Overlaps. In *Proceedings of the SIGCOMM Posters and Demos* (pp. 6-8). ACM.

#### Muncaster, P. (2020). Interpol Operation Reduces Cryptojacking Infections by 78%. Retrieved 10 January 2020, from <https://www.infosecurity-magazine.com/news/interpol-operation-reduces/>