Although the computing devices in today's era can be compromised in a variety of ways, this research paper delves deep into different types of cyber attacks that strip out security from the innocent clients. The impact of these attacks depend more on the broad spectrum of opportunities that a novice user serves to an attacker unknowingly. Though a client sometimes has minimum power to withstand the technical prowess of a skilled attacker, still the probability of such attacks can be nullified by reducing the vulnerabilities of a particular computing system. Thus conscious risk management strategies need to be implemented to save organizations and billions of users across the world surfing the web wirelessly. The paper starts with a brief introduction about various wireless attacks that are frequently carried out in a local area network and their classifications. The research presents several schemes for detecting, mitigating and preventing such type of precarious attacks. Role of user awareness in diminishing the threatening effects of such assaults has been specially taken into consideration. The important
features and limitations of the already reported methods against protection of such attacks have been examined.

References

5. Predrag Tasevski, ”Password Attacks And Generating Strategies“
7. Dove Chiu, Shih-Hao Weng, and Joseph Chiu, "Backdoor use in Trageted Attacks"
16. Marco Antônio Carnut and João J. C. Gondim, ”ARP spoofing detection on switched ethernet networks: a feasibility study,” 5th Symposium on Security in Informatics held at Brazilian Air Force Technology Institute, November 2003


Index Terms

Computer Science Security

Keywords

Cyber Assaults, User Awareness, Risk Management, Local Area Networks.