|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SERIAL NUMBER | HEADLINE OF RISK | DESCRIPTION OF RISK | INHERENT RISK FACTOR | RISK MITIGATION STEPS | LIKELIHOOD |
| 1 | Lack of standard wireless architecture | Inspite of some wireless IDPS can prevent some attacks in wireless networks, it cannot provide advanced architecture. It is different from a wired IPS whose location of detectors follows the logical structure of the network, detectors of wireless IDPS have to be placed based on physical location. So it makes sense to provide a standard architecture to make the implementation will be more easily. | Major | An excellent wireless network must have the following basic functions 1)Automatic detection and classification of wireless network threats.  2)Accurate plan recognition of continuing attacks by hackers.  3) Active response and prevention of the attack behavior that has happened, is happening or will happen. | Possible |
| 2 | Less Accurate with high rate of false positives | All real time IDPS system can suffer from issuing false alarms. Once intrusion is detected, wireless IDPS will abandon the data packets, which will form another type of denial of service. This leads to improperly reaction in facing the attack. | Moderate | Monitor the environment for change | Likely |
| 3 | Insufficient update of attack signatures | An attacker usually at first, need to collect as much as data traffic before attempting an intrusion. This type of passive sniffing is quite dangerous, but there is nothing to do in this direction except to use the proper protection through encryption [6]. In addition, the IDPS has a drawback since it only keeps signature files based on known attack pattern recognition files given to them. It only has protection against what are known to be attacks. It does not have sufficient intelligence to recognize all the attacks against the database application, and establishing its update agressively. | Major | Control the implementation to minimize the impact or likelihood of the risk b providing strong security mechanisms | Likely |