Good geospatial intrusion systems essay example

Law, Security

[Author Name(s), First M. Last, Omit Titles and Degrees]

[Institutional Affiliation(s)]

[Include any grant/funding information and a complete correspondence address.]

In Geospatial Information System (GIS), data is referred to a place, or a set of topographical points that can be joined together, used, and demonstrated in real time. An aspect of geospatial technology is the ability to analyze maps without actually looking at one, and track humans or animals round the clock by integrating a GPS (Global Positioning System) with spatial boundaries that describe political boundaries . Geospatial information systems associate geospatial information in special methods, either by using the layers or extracting new information. For example, GIS analysis may include the location of an international airport and the average number of planes that fly from that airport day and night, and extract information that is needed for tracing an airplane to avoid any intersection. GIS is anticipated as a procedure, as much as a physical unit for information.

Geospatial security

Geospatial security is provided by the National Geospatial Intelligence Agency (NGA), wherein the U. S. officials have set up information protection policies for strengthening homeland security. These policies reduce the prospects of potential attackers taking advantage of publicly available information, which they may receive from the central sources to plan attacks on the U. S. homeland locations. In U. S. numerous organizations and individuals create geospatial data that can be easily obtained by the public. Even with not much sensitive geospatial data available, these organizations have secured their geospatial data by using various techniques and measures. Geospatial technology supports of physical security such as situational awareness, data management, multiple intelligence (multi-INT) fusion, analysis, and information sharing. The organizations must take the guidance of the authorized counsel, facility operators, and security organizations in times of uncertainty in distributing geospatial information.

Examples of Attacks

A few examples of the attacks are the pirate attacks, terrorist attacks, cyber-attacks, web services attacks and suicide attacks. Organizational leaders are increasingly concerned about the threat posed by cyber-attack . Cyber-attacks comprises of cyber-crime, cyber-terrorism, or any disruption in network services that impact the operations. As stated by , attacks can be on a spectrum of critical infrastructure, military targets, cultural and social targets. When an attacker hijacks a web service, the service can forcibly be tampered with geospatial information that can impact the efficiency and damage the services. Interoperability technology recognizes collaboration of several Web services, but it also enables malicious Web service attacks to GIS without a user’s awareness .

The terrorist attacks and their networks are gradually complex systems for the people, economy, and the technology, and in real time they struggle for cell separation, and the absence of interdependency that offers resiliency and planned security benefits.

Defense methods against attacks. Cyber defense should be evaluated in terms of its direct involvement to the successful implementation of an organization's primary mission . ArcGIS platform is many used to help the technology to absorb the logical, physical, and geographic data layers to deliver complete situational attentiveness. In cases of terrorist attack activities the physical and the virtual location must also be considered. Geographic mapping and conception of the terrorist network must be established using the Geographic Information System.

The web services or application security can be defended by enhancing and implementing a demanding security model called threat modeling in which the organization assets are well-defined, and the features and working procedure of each application is defined with the assets, and by creating a security, recognizing and arranging possible threats for each application.

References

Baker, J. C. (2004). Mapping the Risks: Assessing Homeland Security Implications of Publicly Available Geospatial Information. Rand Corporation.

Esri. (2104). The Geospatial Approach to Cybersecurity: An Executive Overview. pp. 1-3. Retrieved from http://www. esri. com/~/media/Files/Pdfs/library/whitepapers/pdfs/geospatial-approach-cybersecurity. pdf

Hanashima, M. (2005). Consideration for Information Security Issues in Geospatial Information Services of Local Governments. IASSIST Quarterly Winter, 16-25. Retrieved from http://www. iassistdata. org/downloads/iqvol294hanashima. pdf

Longley, P. (2005). Geographic Information Systems and Science (2nd Illustrated ed.). John Wiley & Sons.