Ground-to-Air Communications and Secure Networks

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**Ground-to-Air Communications and Secure Networks**

1. **Ground-to-Air Communications risk:**

Since the communication from route to air is through Radio waves. There is some risk such as the signal is not transmitted, APT actors access to the system or capturing the radio waves, and APT actors jamming the radio waves…

The required infrastructure for ground-to-air communication should be building new air-traffic-control centers or using existing infrastructure such as civilian or government/military airports or military air solutions centers. GTSI can also use the signals from satellites for data communication but make sure we have backup towers (in case one is jammed, we can activate other communications methods). A net of Satellites is recommended if choosing the satellite methods.

1. **Designing a Secure Network:**

A modern secure network should build upon the concept of zero-trust in defense-in-depth strategy as well as increasing adoption of code-define systems and infrastructure. While complete zero-trust environments remain rare, zero-trust elements are increasingly appearing in architecture design where they can make a significant difference. To combat advanced persistent threat actors with long-term high-level access to the system, network, and account, and zero trust offer a corrected chain of preventing compromise from becoming long-term, ongoing issues.

Moreover, our secure network must make use of many traditional information security design elements layered with government and military-specific procedures, policies, and technologies. The additional consideration the design takes into account must reflect the need for the military operation (the chain of command, classification, and resistance to electronic warfare,…). The hardware operating system and software they are deployed on may be significantly different from their civilian counterpart ( or civilian version configured to meet the Modern CND requirement).

As the result, the conceptual layer of our Secure Network must start with policies, procedures, training, and awareness; Physical security; Data security, and encryption; Application and software security; Host security; Network security; and end with Network Edge security.

References

Chapple, M., & Seidl, D. (2023). Chapter 9: Defense-in-Depth Strategies In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 103–124). essay, Jones & Bartlett Learning. (1)

Wikipedia (n.d.) Edward Snowden. Retrieved from <https://en.wikipedia.org/wiki/Edward_Snowden> (2)