MINDS
MOBILISATION DES IDÉES NOUVELLES EN MATIÈRE DE DÉFENSE ET DE SÉCURITÉ

Security-Policy NET Nexus of Emerging Technologies

NOTE FOR NATIONAL DEFENCE: Defence Policies on Zero Trust Model for Battlefield Applications

Authors: R. Bahrevar[1] and K. Khorasani[2]

[1] Graduate Student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- The utilization of the zero-trust network architecture is crucial and beneficial as a security-enhancing strategy for the protection of sensitive information, maintaining operational security, and defusing manipulation of sending and receiving data.

- Improving network security through zero trust architecture has been implemented by projects such as BeyondCorp (by Google), as an example. However, integration of AI, human, and network trust structures for applications in military environments have been less considered.

- Development of this structure can be followed by and pursued through improvements in the principles of zero-trust network structure by employing emerging technologies for maintaining, monitoring, and improving communications and security.

- Our goal is to describe the zero-trust network concept, how it is defined through network security, and how it can be extended to various military application.

CONTEXT

- A zero-trust model encompasses security assessments such as identity verification, access management, and traffic management [1].

- The zero trust model is already established for network security. However, considering military applications, it needs some adaptative laws, extensions, and considerations based on new variables that can situationally change on the battleground.

- A simple example of zero trust architecture can be found in preventing VPN-based access to highly critical websites [2].

- According to IBM, a zero-trust network environment is concerned with assessing incoming data from various sources and connecting the information to make a comprehensible decision about the validity and authenticity of the incoming info. In other words, the connection of disconnected environments.

- Achieving zero-trust assessment in its true form is not yet feasible. However, this should not hinder us to establish different possible zero-trust models. Therefore, this strategy can still be established while the technology catches up and advances are made [2].

- A zero-trust model needs to consider all the available resources in addition to the human-AI collaboration and interactions.

- A trust management system should include all the three layers of IoT, that is: perception, network, and application [3].

- With the power of edge computing and 5G communication networks, one can assume that one of the main obstacles or zero-trust models can be elevated, where the processing power from the modern distributed and fast IoT would allow the higher trust level by selecting and limiting communication lines with a fewer chances of network dis-connectivity.

- Therefore, one has to push for an optimal zero trust architecture for the battleground applications.

- However, how one should start, what are the possible policies, models, elements, and applications that should be looked into require further analysis. In this Briefing Note, we will analyze a few of these elements.

CONSIDERATIONS

- Fundamentals of zero-trust network [4] can be summarized as:

    - Verify and secure all resources,
    - Limit and strictly enforce access control, and
    - Inspect and log all network traffic.

- Essential changes toward zero trust can be stated as follows:

- In [4], another important aspect of a zero-trust network is described as network analysis and visibility tools. These include tools that can analyze flow of data, dissect packet captures, and examine the data. They also state that announcing the implementation of the zero-trust and monitoring network will decrease the likelihood of insider attack.

- Aligning security upgrade budgets with the concept of zero trust allows one to ensure that the security system embrace the changes [4].

NEXT STEPS

In the following a few recommendations for a zero trust military application are provided.

- The first step in achieving a zero-trust architecture is to implement an advanced IoT structure such as the integrated 5G and edge-computing. These upgrades can enhance the network quality, its latency, and prevent the disruption in connectivity of the deployed agents.

    - Many companies such as CISCO and IBM are pushing for integration of 5G and edge computing. However, there may be a need for Canadian-based companies to invest in this technology. Otherwise, an important aspect of the futuristic military operations may be solely reliant on the U.S.

    - According to BusinessWire, hundred 5G driving edge computing projects are running in 40 cities of China.

    - For an operation that needs distributed collaboration, if multiple communication lines are to be ignored due to lack of trust, a 5G and edge computing integration can provide the optimal rooting path that connects the device to the operator that is located at a moving/stationery fog node.

- Define the network variables in the battleground. These variables can be an operator's command, a visual image, a coded message by a unite and its neighboring devices, or previous information sent from the concerned area. For example, establishing and standardizing the type of information that is required to locate an object, to command an offensive signal, to identify an area, or to access information. Consequently, a rule-based or intelligent analysis can be made based on the available variables to authorize the appropriate course of action.

- Dynamic policy. Having a dynamic policy is not ideal when it comes to zero-trust architecture in civil applications due to high privacy concerns [5]. For example, accessing information of different individuals or companies for verifying an action. However, in a military chain of command, in terms of information access, a dynamic policy can evaluate the incoming flow from a device, request additional info from the device, its nearby operators, or the main operators to verify the incoming command, request, or information, with less concern over ethical issues such as the privacy.

- Need to establish international policy for authentication and verification of information that are gathered by allied assets.

- Battleground AIoT devices should not fully trust their IoT-received information. Therefore, one needs built-in technologies that are capable of security assessments from different resources. This implies push for technologies such as cognitive AI. This also implies need to push for technologies that can increase the processing power of AIoT devices while not reducing their operational capability.

- Intentional or unintentional insider threat. The human-AI collaboration on the battlefield should itself follow a trust model that can engage and incorporate AI resources such that it preserves the safety of human operators, network, and operational security. Over-trust in AI networks can jeopardize safety of AI operators, security of operation, and under-trust can have deficiencies such as non-optimal performance of battleground units that can also cause and lead to compromising the safety factor.

- Expanding the knowledge of human-AI interaction in universities, and development of supervisory methodologies that are model agnostics, that implies despite the type of machine learning algorithm, the supervisory AI can interpret the decision of AI systems.

References

[1] Stewart, A., 2020. Three Emerging Innovative Technologies Required for Cyber Operations to Execute Commander's Intent at Machine Speed. *Military Cyber Affairs*, *4*(2), p.3.

[2] Campbell, M., 2020. Beyond Zero Trust: Trust Is a Vulnerability. *Computer*, *53*(10), pp.110-113.

[3] Samaniego, M. and Deters, R., 2018, July. Zero-trust hierarchical management in IoT. In *2018 IEEE international congress on Internet of Things (ICIOT)* (pp. 88-95). IEEE.
Kindervag, J., 2016. No more chewy centers: the zero-trust model of information security. *Forrester Research, Inc., dated Mar*, *23*.

[4] Kindervag, J., 2016. No more chewy centers: the zero-trust model of information security. *Forrester Research, Inc., dated Mar*, *23*.

[5] Minu, B., McMiller, E., Kyser, J., Zenone, F., Walker, G., Cilenti, S., Sturzinger, E. and Duncan, K., 2020, March. Establishing and Maintaining Multivariate Trust in a Hierarchical SDN. In *2020 SoutheastCon* (pp. 1-7). IEEE.