# A Prototypical Solution for Cyber Space

Ms. Neha. D. Mistri.
Research Scholar, Karpagam University, Coimbatore
Assistant Professor, S.V. Institute. Of Computer Studies, Kadi - 382 715. Gujarat - India
nehamistry27@rediffmail.com

Dr. Nilesh. K. Modi
Professor & Head of the Department,
S V Institute of Computer Studies, Kadi- 382 715, Gujarat - India
drnileshmodi@yahoo.com

**ABSTRACT—** Many things have been written and told about cyber security and its importance around the world during these recent years. To establish Secure Cyber Space an effective communication network is needed. The cognitive networks are effective networks for communication. These networks are also changeable. This network is constructed of network terminals, and wired and wireless connections among them. This network is capable of being aware of the network's intrinsic and external situation. CN has feature to operate standalone, frame decisions and set itself according to the mentioned goal. A key ability is learning which means that the network can use last made decisions during a CN process. The research focuses on architectural security aspects of network. The main objective of the research is to see how the features of CN could be used for building and framing a cyber security model. The cyber security detailed makeup describes all the security functionalities and controls that are required when implementing the high-secure network. Cognitive tone will create more knowledge on networks. Increasing cyber security threat seeks that security requirements are already taken care of the beginning of framing the network process. Hence, it is obvious and compulsory to build a proposed model that could be used at an initial point when latest networks are thought about and brought into implementation.

**Index terms** – Cognitive Network (CN), Cyber Security, Security Control Element, network node.

## I. INTRODUCTION

Many things have been written and told about cyber security and its importance around the world during these recent years. It has been expressed by many experts that how significant the cyber security is. Cyber security policies have been taken up by many countries. One question always comes up that how can we take precautions for cyber threats. In everyone's daily life Cyber security is important. It is not only for governmental or business actors, but Cyber Security is related to everyone's daily activities too. Cyberspace has become an important field where tactical or operational benefits of business can be won or lost. Cyberspace is so dynamic in nature that events in cyberspace occur at high speed. Critical infrastructure and services may require more than traditional responses. Although risks in cyberspace can be managed in numerous ways, they do not often match this difficult and unstable environment. Threat also comes in its way when dependency on cyberspace increases. Cyber interruptions and attacks have increased severely over the period of time, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. While cyberspace raises open markets and open societies, this very openness can also make business and military actors more threatened to criminals, attackers, and foreign intelligence services that try to compromise or damage the critical systems.

To establish Secure Cyber Space an effective communication network is needed. The cognitive networks are effective networks for communication. These networks are also changeable. This network is constructed of network terminals, and wired and wireless connections among them. This network is capable of being aware of the network's intrinsic and external situation. CN has feature to operate standalone, frame decisions and set itself according to the mentioned goal. A key ability is learning which means that the network can use last made decisions during a CN process.

The research focuses on architectural security aspects of network. The main objective of the research is to see how the features of CN could be used for building and framing a cyber security model. The cyber security detailed makeup describes all the security functionalities and controls that are required when implementing the high-secure network. Cognitive tone will create more knowledge on networks. Increasing cyber security threat seeks that security requirements are already taken care of the beginning of framing the network process. Hence, it is obvious and compulsory to build a proposed model that could be used at an initial point when latest networks are thought about and brought into implementation.

## II. COGNITIVE NETWORK AND CYBER SPACE

The cognitive networks are simply smart communications networks that are able to be aware of the network's internal and environmental situation. CN has an ability to operate independently, make decisions and adapt according to the given goal. A key feature is learning which means that the network can exploit previously made decisions during a cognitive process. Cognitive network is defined as a network with a cognitive process that can perceive current network conditions, plan, decide, act on those conditions, learn from the consequences of its actions, all while following end-to-end goals. The cognition loop senses the environment, plans actions according to sensor input data and network policies, decides which scenario fits best its end-to-end purpose using a reasoning engine, and finally acts on the chosen scenario as discussed in the previous section. The system learns from the past (situations, plans, decisions, actions) and uses this knowledge to improve the decisions in the future.

Cyberspace consists of computers (including programmable circuits), and the connections between them forming a virtual dimension. Cyberspace is the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems. In cyberspace, individuals can interact, exchange ideas, share information, provide social support, trade, create various types of media, play games, participate in policy debate, etc, using the global network.

Cyber Security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

## III. RELATED RESEARCH

Related work consists of published books and research papers about cognitive networks, cyber security and network security. Cognitive networks are currently studied in various research programs. Previously, research was focusing more on the cognitive radios and spectral efficiency and usage of them, but now cognitive features are spread to an entire communication system and all the layers of a networking device. Cognitive networks research focuses largely on the decision-making mechanisms, and communication and optimization between the layers (cross-layer functionality). The basic idea behind the cognitive network is presented in the research papers by R. Thomas et al [1], [2], [3]. A book called Cognitive radio communications and networks: principles and practice explores the state-of-the art in cognitive networks, compiling a roadmap to future research. It also covers cognitive radios with semantic aspects.

Lots of cyber security and cyber threat related research papers are published during last year's. Naturally, this research has also produced several books. Many of the books consider other than technical aspects of cyber security but we can find a few that focus on technology.

## IV. NEED FOR NEW ARCHITECTURE

Looking at the review of the architecture frameworks and models, the following conclusions can be drawn:

1. Few of the models (MODAF, DoDAF) are high-level architecture frameworks, and they do not basically include any security related views. Generally they are uniquely designed for military organizations, but the focus is little more on command and control of applications than on communications networking.

2. The presented security architectures (SABSA, iCode) are all in all security architectures, and they attempt to explain enterprise-level management security and controls. The architecture models are complicated to use for explaining cyber security architecture of military networks, because the models do not put forward any functional or component-level features.

3. Technical security architectures (e.g. Cisco Security Framework) are made to support the network devices of a few manufacturers. These architectures generally describe how the devices are to be configured to provide a security level which is desired. The architectures are not dependent and open, but they are based on few technologies and devices.

4. ITU-T references are more promising. They describe requirements of technical security and mechanisms in many different scenarios. Main challenge is that the ITU-T architecture documentation only presents the technical requirements at every system layer, but does not shows how the architecture layers are constructed with blocks that are smaller and security elements.

5. No architecture models or framework do introduce any cognitive processing.

## V. PROPOSED SECURITY ARCHITECTURE

Security architecture refers to cohesive security design, which takes into account security requirements and objectives (e.g. confidentiality, non-repudiation, authentication, authorization, etc.). The architecture addresses the risks of a particular environment/scenario, and specifies what security controls are to be applied where. The design process must be repeatable.

Figure 1 shows the cyber security model for the cognitive networks. The model of the architecture is actually based on a block figure that explains functional element at around five functional layers. The architecture models that have been reviewed are unable to resolve existing problems. The present architecture model is not based on any past model or framework. However, the layered technique of the ITU-T X.805 is used in the architecture design.

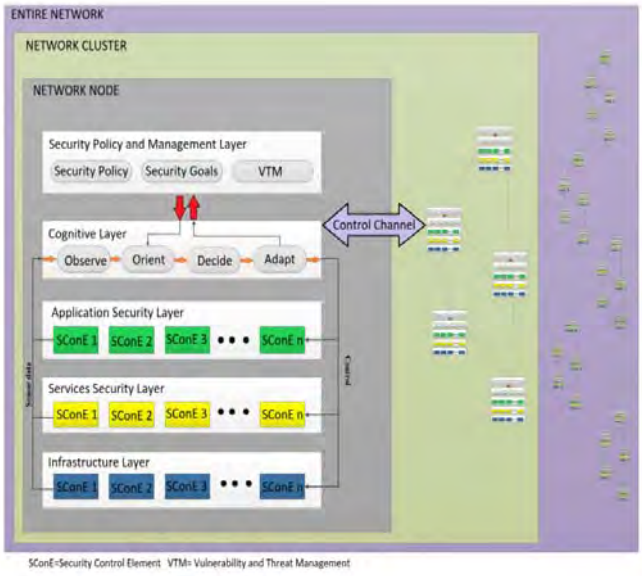


Figure 1 Cyber Security Model

Different layers of the architecture are Infrastructure Security Layer, Security Policy and Management Layer, Cognitive Layer, Service Security Layer, and Application Security Layer. The layers are brought to use in each network node right through the network. The nodes may be man-packed, mobile node, fixed node or vehicle-mounted. Security controls and settings are managed and optimized from three viewpoints; a single node of network, a network group, and whole network. At the initial point of the architecture, security policies and goals are set and carried out at the Security Policy and Management Layer which then directs and controls the Cognitive Layer. Vulnerability and Threat Management supplies libraries of cyber security threat and vulnerability to the Cognitive Layer. This input comprises of security goals for user admittance i.e. authorization and authentication, data classification levels, cryptography algorithms, key patterns, security requirements for data transport, etc. The security policies and goals are physically set in at starting phase of network operation. The vulnerability and threat libraries are revised constantly during the operational phase of the network. Security Management Layer also gets information from the Cognitive Layer. This information has data regarding network adaptation conclusions, present setup, and detected anomalies.

The most important task of second layer is to present a process for decision making and to run the security adaptations in a network node. This layer is connected to the subsequent three layers. This layer controls and adjusts Security Control Elements of these three layers according to the adjustment orders. It also takes care of all the Security Controls Elements and gets status data from them. The infrastructure Security Layer contains the security controls of network transmission services, and single networking element. Network components that belong to this layer include individual routers, switches, servers, and the communication links between these routers, switches and servers.

The Services Security Layer describes security of services that a network gives to the user. The Application Security Layer focuses on security of the network-based applications admittances by end-users. The end-user applications are allowed by network services and infrastructure and they contains basic application, file transport/storage applications, voice messaging and email etc.

Security Control Elements give appropriate security controls at all of the three layers. The controls can be divided into three categories according to the timescale of an event. Ahead of the incidence, preventive controls are intended to avoid an incident from occurring by e.g. jamming user access that are not authorized. Detective

controls act during the event, and they are arranged to identify and characterize an incident which is going on, and to make aware other security controls or network security personnel. Subsequent to the event, remedial controls are used to control any damages caused by the incident e.g. by differentiating damaged network segments, filtering traffic or recovering damaged services. The implementation of cognitive security features requires the security controls to be fully software-controlled. All the security elements are controlled by software. Another requirement is an ability to collect status information from the security control elements.

The Security Control Elements provided by the security architecture include the following components of security protection:

- Integrity protection components generate and authenticate the digital signatures and authentication messages for the purpose of entity and data integrity.
- Confidentiality protection components encrypt and decrypt data to protect the confidentiality of data in all processing or transferring phases.
- Vulnerability management components automatically scan and update the system vulnerability of network nodes and patch the security holes.
- Authentication components provide authentication services for network nodes. For example, negotiate the session key required by secure communication.
- Access control components receive and request access control lists and authenticate the access control requirements of network nodes.
- Communication insulation components configure and manage network communication connections and implement traffic monitoring. For example packet filtering.
- Malware protection components automatically scan and remove viruses and automatically update malware libraries.
- Security audit components automatically follow and record the operation logs of network infrastructure, applications and services.
- Intrusion detection components automatically detect and record hostile intrusion events and cyber attacks, and distribute warning information to related control components.

## VI. EVALUATION OF RESEARCH ARCHITECTURE

Evaluation is a key process to prove compliance of the resultant cyber security architecture. The purpose is to show how existing methods inadequately support the evaluation of security architecture. Here we propose a scenario based security evaluation framework. The scenario-based security evaluation provides both an assessment of quality attributes and explores the interactions and interdependencies of those quality attributes, highlighting tradeoff mechanisms and opportunities between quality attributes. Another factor is the combination of a risk analysis. The goal is to identify potential risks.

Integrating security patterns to the framework enhances the quality of security components in the architecture. The framework includes security patterns not only for the risk analysis, but also as a core component of each security scenarios that contains the security profile. The scenario-based evaluation framework includes six phases that are defining the evaluation goal, generating security scenarios, creating the security profile, describing the architecture, evaluating scenarios and analyzing results. The evaluation process is illustrated in Figure 2.

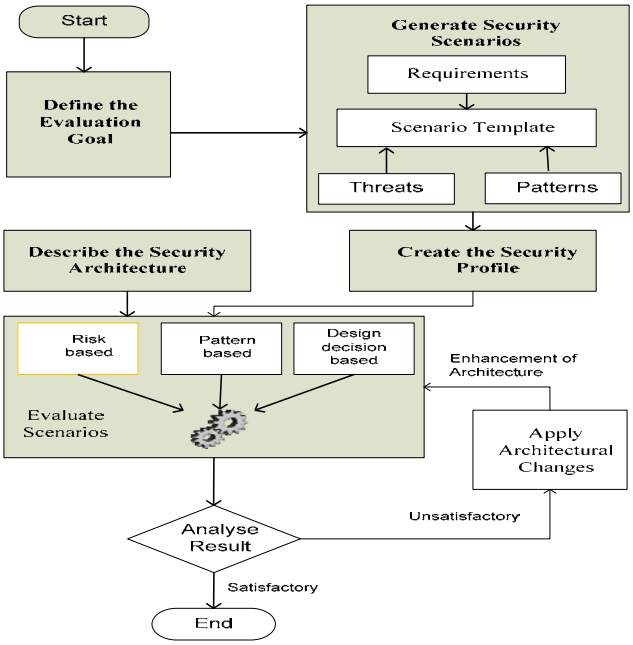


Figure 2 Security Evaluation framework

Evaluating cyber security architecture is a very challenging issue. A problem in existing evaluation method is that different evaluation criteria are created for auditing existing devices. They are not designed for evaluating high level security architecture with functional properties. The results of the scenario based evaluation show that the proposed architecture mitigates the most of the threats. The risk level with most of the threats is low or very low. Cryptography, access control and traffic monitoring are key enables to mitigate the threats.

## VII. CONCLUSION

Cyberspace is growing all the time. New devices and systems are connected to the internet every day. Internet is on high demand which is the connection of computers. There are many physical devices like routers, computers, wireless base stations, optical fiber cables and servers with databases. And Cyberspace is dependent on the physical devices.

The resultant model has tremendous potential for the security in Cyber Space. The implementation result of the model showcases that the proposed model work efficiently in compare to other models for the security in Cyber Space.

The purpose of the new cyber security model is to determine the structure of security controls and management of network from a functional perspective. Many existing architecture and frameworks were studied for describing this proposed architecture. The main objective was to find a suitable architecture for the cyber security. The analyzed architectures included interconnected models and enterprise related frameworks.

The model which has been proposed is meant to meet the present day's requirements for cyber security. The design of the model permits that the security elements are athletically added, deleted, or can be modified. The step by step approach allows security protection in depth. A smart, cognitive procedure enables risk management automatically and updates the system. The proposed architecture is contains different layers. It also includes the management layer. The end-to-end security objective is set by the management layer in the cyber security model which provides security to the processed information and sharing. The threat, weakness and vulnerability library which are available in the management layer is a main part of security. It ensures the security elements are secured and they are configured to protect against latest threats and attacking scenarios.

## REFERENCES

[1] Thomas R. W., DaSilva L. A. and MacKenzie A. B., Cognitive Networks, In Proceedings of First IEEE International Symposium on New Frontiers in DynamicSpectrum Access Networks (DySPAN), 2005.
[2] Thomas R. W., DaSilva L. A., Marathe M. V. and Wood K. N., Critical Design Decisions for Cognitive Networks, In Proceedings of IEEE ICC 2007, pp. 3993-3998, June 2007.
[3] Thomas R. W., Friend D. H., DaSilva L. A. and MacKenzie A. B., Cognitive Networks: Adaptation and Learning to Achieve End-to-End Performance Objectives, IEEE Communication Magazine, vol. 44, pp. 51-57, Dec. 2006.
[4] Alberts D. S. and Hayes R. E., Understanding Commandand Control, CCRP publication series, USA, 2006.
[5] Clancy T. C., and Goergen N., Security in cognitive radio networks: threats and mitigation, 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), pp 1 – 8, 2008.
[6] Security architecture for systems providing end-to-end communications, Series X: Data Networks and Open System Communications and Security, ITU-T Recommendation X.805, ITU-T Study Group, October 2003.

**Authors Profile**

Neha D Mistri has completed her B.Sc. (Physics) from Gujarat University and M.C.A. from Nirma University, Ahmedabad. Her area of interest includes Networking, Management Information System, Enterprise Resource Planning and E-commerce and Internet Security. She is pursuing Ph.D. in the area of "Cyber Security" under the guidance of Prof. (Dr.) Nilesh Modi, from Karpagam University, Coimbatore, Tamilnadu. She has presented and published number of research papers in National/International Conferences.

Prof. (Dr.) Nilesh K. Modi has completed M.Phil and Ph.d. He is having his active involvement as a life member of CSI, IEEE, IACSIT, laeng apart from his academic and industrial career. Dr. Modi having experience of around 8 years in academics and industry, holding Doctorate in E-Security (Computer Science and Application), continuing his research on information and communication security, presently he is pursuing post doctoral research on Wireless Communication and Security and pursuing for the Certification as an Ethical Hacker. He is working as a recognized research supervisors for Ph.D. and M.Phil. Programme from more than 03 universities of India.He has good number of research under his name and presented more than 65 research papers in International and National Journals and Conferences. He is working as a manuscript reviewer for the international journal & conference at computer science department auburn university, Alabama, USA. ofGuarat. He is also working as a reviewer for number of national and international journals. He has delivered number of expert talk on eSecuritY and hacking fi National Conferences He is also the member of board of studies and selection committee of different universities. He is working as district coordinator for SANDHAN Program initiated by Government.