Quantifying the Role of Access Control in End-to-End Network Security

A. Usama Ahmed, B. Ammar Masood, C. Liaquat Ali Khan
Security and Cryptology Cell, Air University, Islamabad, Pakistan

Abstract - *Modern day networks consist of a mix and match of technologies with varying capabilities. Securing such networks is a tedious task and demands a lot of contribution from security professionals. However, failing to conduct an in depth and standardized analysis may result in an imperfect network security design. ITU-T provides recommendation for end-to-end network security in its standard X.805 which precisely lays down the foundation for the assessment of network security. Keeping X.805 requirements and the current network in view, the next thing that security professionals face is the correlation of both and its practical implementation. This paper contributes to answer the same and gives a comprehensive methodology for practical implementation of X.805 architecture. Also this paper takes into account the current trend of Network Access Control solution and its quantitative contribution towards achieving the desired goals set by X.805 standard.*

Keywords: X.805; Network Access Control; end-to-end security; Compliance; ISO-18028;

1 Introduction

Entities participating in the information flow from one end to the other are distinct in their characteristics and so are vulnerable in their own perspective. Strengthening the security of individual entities often leave gaps that are overlooked and that becomes the cause of denial, destruction and even loss of information vital to the communicating parties. Planning, implementing and maintaining the security of a network need precise efforts. Security professionals had always faced a usual challenge of enhancing the security capabilities of the network to meet the need of the day.

Conventional methods of network security had been simple and undemanding. There had been simple networks with unsophisticated applications and so had their vulnerabilities. The best possible way had been to have a perimeter defense with a border firewall and a user provisioning system for access control. As the networks grew, and enhanced capabilities were introduced in the equipments as well as the applications, the job of a security professional meant more than planning a perimeter defense.

The fast paced growth in the capabilities of the network and the variance in technologies let the professionals deal with security in a more elaborate way than ever. For the same the security professionals has followed best practices for the information security as per their requirements and needs of network. These requirements revolve around the overall objective of organization's information security policy. Adhering to the best practices may suffice but still leave the security professionals with a question in mind. What were the objectives set at the start of the day? What have been achieved and what has been left out?

1.1 ITU-T X.805

A standard and definite approach is, therefore, required to be used so that a quantifiable effect of security endeavors can be realized. The well known and distinguished set of recommendations is given by ITU-T as X.805 standard [1] for end-to-end security of a network infrastructure. It aims to achieve an overall safe and secure network by answering the most common security concerns that often arise when one talks about end-to-end security.

The type of threats, respective protections required, the elements and activities within a network that need protection are the primary focus of X.805standard. This standard, in itself fulfills the needs of a network's security and plays a crucial role in achieving the overall objectives of Information Security Management System (ISMS) of the organization.

1.2 Information Security Management System

International Standard Organization (ISO) has finalized a security management standard ISO 27001[2], and its expanded details "Code of Practice for ISMS" in ISO 27002[3]. Information Security Management System (ISMS) focuses on detailed aspects of entire information security within an organization.

Network security is one of the main concerns of the entire cycle of ISMS. The clause for network security expands on a detailed architecture standard ISO-18028 (IT Network Security), which is further divided into five parts. The first part, ISO-18028/1 elaborates the best practices used for managing network security. This document bridges the gap which arises between the administrators and the management personnel responsible for network security. ISO 18028-2 provides recommendation for the planning, design and implementation of the network security architecture and is infact the ITU-T X.805 standard adopted by ISO.

The Fig 1 below illustrates the mapping between the ISO 27001, ISO 27002 and ISO 18028 standards. Both X.805 and ISO 18028-2 are used in this paper interchangeably to represent the standard security architecture.

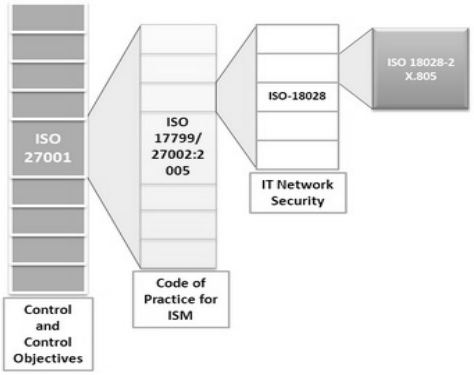

Figure 2. Mapping of 18028-2 to ISO 27001

ITU-T X.805 covers eight dimensions of security namely Authentication, Access Control, Non-repudiation, Data Confidentiality, Communication Security, Integrity, Availability and Privacy. These dimensions are then applied to a hierarchy of network elements and facilities spread across three layers namely Infrastructure, Services and Application layer. The activities that take place within the network are divided into three planes namely Management, Control and End User planes and lie within each of the three security layers described above. The above mentioned eight dimensions are applied to each intersection of these three planes across each of the three layers. The details of each dimension as described by the standard specify the requirements to be fulfilled by the network for compliance.

Despite all the deliberations made on security in the X.805 standard, the question that security professionals face is "*how to best implement X.805 standard*?" Although X.805 sets the requirements; yet, it does not describe the way to link and practically implement it on a network infrastructure for end-to-end security. This paper not only addresses the practical aspects in implementation of the ITU-T X.805 standard, but also exemplifies the process by taking into account the solution for Network Access Control.

1.3 Network Access Control

The current trend in the network security products indicates a strong inclination towards the development of integrated products. The trend offers an advantage of ease of management and lesser interoperability issues. The Network Access Control (NAC) solution is one such integrated product which is being increasingly used in support of authentication, access control and non-repudiation. It is a revolutionary security strategy that aims to ensure a safe network environment by unifying end point security technologies like antivirus, anti-spyware, security patches and updates along with end-user authentication strictly based on compliance to an end point security policy. NAC allows network access based on assessment of behaviour to only compliant and trusted endpoint devices (PC or non-PC devices), and restricts the access of noncompliant devices until they become compliant.

In legacy network architecture, end users and devices are authorized based on as to who or what they are. NAC offers a more elaborate mechanism to make sure that only those end points become the part of network whose identity as well as status of health has been verified. A precise definition of NAC technology is somewhat challenging due to the evolving nature of this product; however, the principle objectives of the NAC can be viewed as [4]

- Endpoints that lack up-to-date antivirus, security patches or firewall softwares are denied network access to avoid contaminating the entire network.
- Network operators can define policies, regarding user roles, level of access and areas of network where those roles are permitted access.
- Identity management and user provisioning system acting as a part of NAC to ensure seamless implementation.

There are various versions of NAC available in the market, each from different vendor but all working toward the goals as defined above. Based on the functionality; however, there are two main categories of NAC. One is the software based, with the liberty to use any recommended type of underlying hardware and operating system, and the other is the hardware (Appliance) based, that avail a dedicated underlying hardware with an operating system desired for the same. Both the solutions have their pros and cons, and deciding the best to be implemented in the network depends upon the need and requirement of the network in question. The wide range of products available in the market makes it difficult to compare the products on point to point basis; yet, on the other hand, the same variety and wide range of products help to easily identify the one precisely suitable for the needs of an organization [4].

In this paper an attempt has been made to consider the practical implementation of X.805 standard across an organizational network while quantifying the security posture resulting through the addition of a NAC solution. The novelty of approach lies in quantification of the security posture. This quantification aims to bridge the gap that is often always present between the management and technical team dealing with network security within an organization.

2 Related Work

Although the standardized and systematic method of planning and assessment of network security is precisely defined in ITU-T X.805 standard, but not much work has

been reported in regards to issues related to practical implementation of this architecture in a real network. In [5] Richard, Ahmad and Kiseon have worked on the assessment of security natively offered by IEEE 802.15.4 standard for Low Rate Wireless Personal Area Networks in the light of X.805 architecture. Their assessment is more theoretical than practical and that too belongs to a different domain of network. Application of X.805 framework on a model of banking network has been attempted by Ramirez in [6]. This approach has only elaborated the standard specifically in terms of banking network requirements. It fails to address the methods of meeting those requirements and in fact also lacks the methodology for assessment of said network after the requirements are fulfilled. A similar theoretical concept is given in [6] explaining the effectiveness of X.805 architecture in terms of Return on Investment (ROI) for any enterprise. Both the works only subjectively address the application of X.805 standard as compared to the detailed objective analysis attempted by us. Moreover, our research has presented a generic method for planning, assessment and quantification of network security. It is equally applicable to any kind of network, including banking, education, health care and defense.

3 Proposed Work

In this section we discuss in detail our proposed approach to plan and assess the security of a network in the light of ITU-T X.805 architecture. The practical realization of X.805 architecture is described and also the possible quantifiable outcome in case of an example scenario when NAC is introduced in the network. The approach used in this analysis is to precisely break down the network into entities, and then fit those entities into each of the modules offered by X.805 and then assess the capability of each entity gained through NAC against the required capability as per X.805 specification. The deficiency, therefore leads to the introduction of external components that may be software or hardware, entity based or network wide to meet the standard requirements.

The quantitative results from this analysis are presented later in the section and are based on a legend in which a control can be in any of the four states as explained in Table I. NAC offers satisfactory compliance for a control, when it provides the required feature solely on the basis of its configuration. Partial compliance is offered when the control objectives are not fully met by the NAC solution and there is a requirement of additional effort to be put into it. This requirement may be hardware or a software upgrade to the end user device. The scope of this research does not precisely deal with the method of fulfilling this requirement. Whenever there is no need for an upgrade and merely policy enforcement can offer the compliance by forcing the element to pass through NAC, it is mentioned as Implicit Compliance. If NAC is totally unable to meet control objectives, it is marked as Not Applicable.

TABLE I. LEGEND AND DESCRIPTION

Key	Description
F	Satisfactory Compliance
P	Partial Compliance
I	Implicitly Compliance by virtue of network design
×	Not Applicable

In the perspective of NAC, the main focus is on end user devices. In today's network, most common end user devices are PCs, Laptops, and PDAs, non-PC devices like IP Phones and printers, which constitute the infrastructure layer of X.805 framework. Similarly, the services layer consists of those services running on any of the end terminal devices. Most common services used by a host PC are likely DHCP, POP3, SMTP, HTTP(S), NAC Agent, Antivirus, Firewall, Security Center and IPSec to name a few. The Application layer consists of any and all the applications present at the user terminal. The main focus is on the applications that directly interact with the lower layers without any need of other applications such as email clients, web browser or any other custom built.

TABLE II. NAC COVERAGE OF ACCESS CONTROL DIMENSION

Access Control Security Dimension										
Security Planes	***Security Layers***									
	Infrastructure			***Services***			***Application***			
	PC, Laptop	***IP Phone***	***Printer***	***POP3, HTTP(S), NAC Agent, Antivirus, Firewall, Security Center***	***SIP,RTP, SRTP,SIPS***	***LPD/LPR, IPP***	***Email Client, Web browser, custom Built.***	***Call Manager***	***Print Manager***
End User	F	×	F	F	×	F	P	×	F
Control	F	×	F	F	×	F	P	×	F
Management	F	I	F	F	I	F	I	I	F

Table II shows the coverage of NAC across all layers and planes with respect to the Access Control security dimension. This dimension deals with the protection against unauthorized access to network resources. One method of achieving this objective is the role based access to elements of network infrastructure, like devices, services, application etc. The contribution of NAC for access control of each entity participating in our network is precisely laid down in table II.

NAC shows limited contribution towards Access Control of IP Phone and its services. IP Phones may or may not offer functionality of restricting access to its End User plane as a built-in feature but it's a fact that they lack contribution from NAC. Similarly the control plane containing all signaling and call control information may have an access control mechanism on part of the protocol or the IP Phone itself but

eventually it lacks contribution from NAC. Management activities performed on an IP Phone can however be implicitly forced to pass through NAC. In this scenario the personnel or devices originating management commands have to be authenticated and compliant to network policies. The same functionality of NAC can be perceived for the other entities in the network. NAC offers full coverage for Access control in case of PCs and printers with the exception of being partially supportive for applications running on the PCs. The applications depend on NAC for authorized access but defining levels of access within the application is entirely on the discretion of application itself. Access control levels for PCs, printers and their services can be defined in the user provisioning subsystem of the NAC solution. NAC fully ensures that only authorized personnel and devices have access to the End User, Control and Management Plane of the PCs, Printers and their services.

It is evident from the table II that NAC does not show much contribution to access control of IP Phones and its services, which might need device level software upgrades. The same approach has been followed for the analysis of other security dimensions described throughout this section.

TABLE III. NAC COVERAGE OF AUTHENTICATION DIMENSION

Authentication Security Dimension										
Security Planes	***Security Layers***									
	Infrastructure			***Services***			***Application***			
	PC, Laptop	***IP Phone***	***Printer***	***POP3, HTTP(S), NAC Agent, Antivirus, Firewall, Security Center***	***SIP,RTP, SRTP,SIPS***	***LPD/LPR, IPP***	***Email Client, Web browser, custom Built.***	***Call Manager***	***Print Manager***
End User	F	I	F	F	×	F	F	I	F
Control	F	P	F	F	P	F	F	×	F
Management	F	I	F	F	I	F	F	I	F

Table III explains the NAC coverage with respect to Authentication security dimension. In this regard X.805 specifies the requirement for confirming the validity of the claimed identities of the communicating entities. Table III shows the strength of a NAC solution in fulfilling the overall objectives of Authentication security dimension. NAC shows a great amount of contribution for authentication security dimension; however, for IP Phone and its protocols, it still offers a limited support. There is need of software level upgrade at device level for full compliance to X.805 requirements.

Table IV highlights the NAC coverage for Non-repudiation dimension. Preventing an individual or entity from denying a committed action is the key objective of this control.

TABLE IV. NAC COVERAGE OF NON-REPUDIATION DIMENSION

Non-Repudiation Security Dimension									
Security Planes	***Security Layers***								
	Infrastructure			***Services***			***Application***		
	PC, Laptop	***IP Phone***	***Printer***	***POP3, HTTP(S), NAC Agent, Antivirus, Firewall, Security Center***	***SIP,RTP, SRTP,SIPS***	***LPD/LPR, IPP***	***Email Client, Web browser, custom Built.***	***Call Manager***	***Print Manager***
End User	P	×	P	P	P	P	P	×	P
Control	P	×	P	P	P	P	P	×	P
Management	P	I	P	P	I	P	P	I	P

The overall impact drawn from a quick analysis of the table is that NAC only offers a part of non-repudiation and that is related to network joining, leaving, and connection establishment between two peers and their status at the said time. For full compliance there might be a need of a software upgrade at device or at network level.

Although X.805 also considers Data Confidentiality and Communication security dimensions; yet, they are not included in the analysis as NAC does not offer any capability to address these dimensions across any of the layers or planes of X.805 architecture. The services and applications may have their inherent capability to offer data confidentiality but this does not count for increasing the score of NAC solution. Communication security is also not addressed by the NAC solution. Intermediate network elements like switches, routers and gateways etc offers the capacity to ensure communication security and can be achieved by appropriate configuration and integration of these network elements.

TABLE V. NAC COVERAGE OF DATA INTEGRITY DIMENSION

Data Integrity Security Dimension									
Security Planes	***Security Layers***								
	Infrastructure			***Services***			***Application***		
	PC, Laptop	***IP Phone***	***Printer***	***POP3, HTTP(S), NAC Agent, Antivirus, Firewall, Security Center***	***SIP,RTP, SRTP,SIPS***	***LPD/LPR, IPP***	***Email Client, Web browser, custom Built.***	***Call Manager***	***Print Manager***
End User	P	×	×	P	×	×	P	×	P
Control	P	×	P	P	×	P	P	×	P
Management	P	×	P	P	×	P	P	×	P

Table V explains the data integrity dimension of X.805. NAC solution offers limited data integrity and that too is offered by

its capability of ensuring up-to-date and active anti-malware application and security updates. NAC solution currently lacks capability to ensure data integrity for IP Phone. Keeping in view the current trends in NAC solution, it can be foresighted that this capacity may be incorporated soon.

ITU-T X.805 deals with the constant availability of resources to the authorized users in Availability security dimension and specifies that there must be no denial of authorized access to the network resources whether it is infrastructure, service, application or stored information. NAC ensures partial availability for whole infrastructure as shown in Table VI. To ensure full compliance to availability security dimension there might be a need for network level upgrade like Intrusion Detection/Prevention systems, firewall appliances etc.

TABLE VI. NAC COVERAGE OF AVAILABILITY SECURITY DIMENSION

Availability Security Dimension									
Security Planes	***Security Layers***								
	Infrastructure			***Services***			***Application***		
	PC, Laptop	***IP Phone***	***Printer***	***POP3, HTTP(S), NAC Agent, Antivirus, Firewall, Security Center***	***SIP,RTP, SRTP,SIPS***	***LPD/LPR, IPP***	***Email Client, Web browser, custom Built.***	***Call Manager***	***Print Manager***
End User	P	P	P	P	P	P	P	P	P
Control	P	P	P	P	P	P	P	P	P
Management	P	P	P	P	P	P	P	P	P

The privacy dimension of ITU-T X.805 states that the Information related to user or device activities must not be viewable to unauthorized entities and they must not be able to deduce the scope of activity performed on the element in question. Authentication and Access Control security dimensions are helpful in providing compliance to the Privacy security dimension and therefore yields the same insight as for Authentication and Access Control dimensions.

Table VII summarizes our analysis. Data Confidentiality, Communication Security and Privacy are not covered by NAC and hence are not included in the summary. The table provides a quantitative analysis of the overall coverage of X.805 dimensions by NAC and the same is depicted as percentage overall score of NAC solution in the Fig.2.

TABLE VII. ANALYSIS SUMMARY

Summary of NAC coverage of X.805 architecture				
End User Device	***Covered***	***Partially Covered***	***Implicitly covered***	***Not Covered***
PC, Laptop	15	29	1	0
IP Phones	0	13	11	21
Printers	18	25	0	2

It is evident from Table VII that the NAC solution offers good support for PCs, Laptops and Printers either by full compliance or by partially helping the entities achieve the said status. It is also a matter of fact that the contemporary NAC solutions single handedly provide a good amount of contribution towards achieving X.805 compliance. However, NAC shows limited support for IP Phones, which are rapidly proliferating the existing networks.

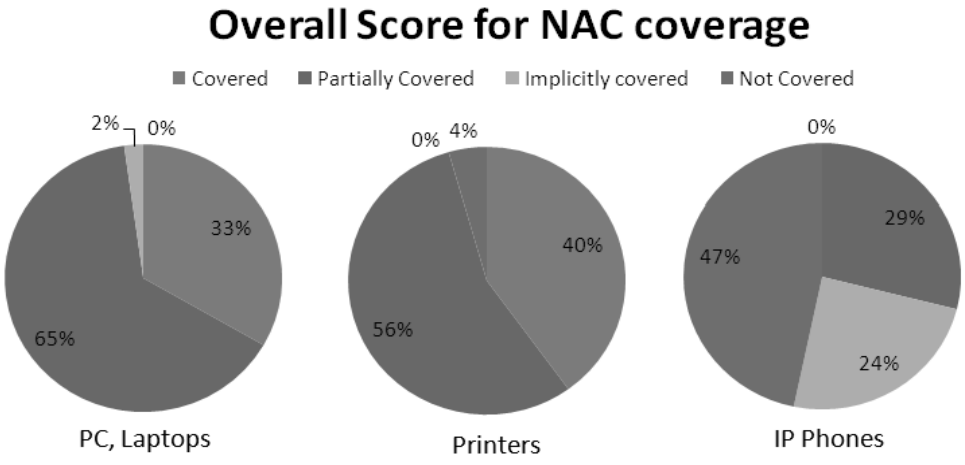

Figure 2. Overall Percentage score for NAC coverage of X.805

4 Conclusion

In this paper we have presented an approach for practical implementation of ITU-T X.805 standard for achieving end to end network security, while also considering the impact of a generic Network Access Control solution. The objective analysis as covered in Tables II – VI and summarized in Table VII quantifies the impact of NAC solution on overall network security and helps in developing better understanding of the assessment of a network's security. The analysis indicates that NAC contributes tremendously towards achieving X.805 compliance for any network. The remaining requirements where it lacks contribution can be satisfied by introducing other solutions and their contribution can be adjudged on the same pattern before bringing them into the network. By contributing a quantified security posture assessment approach, the proposed work is expected to open new horizons in network security management.

5 References

[1] "ITU-T Recommendation X.805", http://www.itu.int/ itudoc/itu-t/aap/sg17aap/history/x805/x805.html, [Dec. 11, 2009]

[2] "Information security management systems – Requirements", http://www.iso.org/iso/catalogue_detail? csnumber=42103, [Nov. 29, 2009]

[3] "Code of practice for information security management", http://www.iso.org/iso/iso_catalogue/catalogue_tc/ catalogue_detail. htm?csnumber=50297 [Nov. 29, 2009]

[4] J. Edwards. "The Essential Guide to NAC":, http://www.itsecurity.com/ features/essential-guide-nac-062308/, Jun. 23, 2008 [Apr. 05, 2010].

[5] A. O. Richard, A. Ahmad, K. Kiseon, "Security assessments of IEEE 802.15.4 standard based on X.805 framework". *Int. J. Secur. Netw.* 5, 2/3, 188-197 (Mar. 2010). DOI=http://dx.doi.org/10.1504/IJSN. 2010.032217

[6] D. Ramirez, . "Case study: ITU-T recommendation X.805 applied to an enterprise environment—banking" *Bell Labs Techical Journal,* Vol., Iss., 12-3, pp 55-64, Sep. 2007, DOI= http://dx.doi.org/ 10.1002/bltj.v12:3

[7] A.R. McGee, U. Chandrashekhar, S.H. Richman, "Using ITU-T X.805 for comprehensive network security assessment and planning", in *Proc. Telecommunications Network Strategy and Planning Symposium. NETWORKS* 2004, 11th International, Vol., Iss., 13-16, pp273- 278, June 2004.