Review on Network Architecture with Trustworthiness, Controllability and Security

Abdullah Nayaf Shafi

Electrical & Electronics Engineer, Birla Institute of technology, Pilani, Dubai Campus

Abstract- This paper focuses on network architecture with trust-worthiness, controllability and security. The major focus is on to build an infrastructure of the network with these three main functionalities. It specifies about the threats to the network, the control mechanisms of these threats, the requirements of a network for improved security, trustworthiness and controllability, the mechanisms to increase the trustworthiness, controllability and security. This paper then talks about two types of architecture: Switch ware architecture and SANE architecture, which possess all the three functionalities and provides maximum security.

I. INTRODUCTION

This paper deals with the topic of network architecture with trustworthiness, controllability and security. the term network architecture describes abstract principles of the technical de-sign of protocols and mechanisms for computer communication. There are many design alternatives, out of which a design is chosen which is informed by an understanding of requirements. Today's networks are fragile with a great deal of security threats such as junk mail, malicious attack, computer virus, etc. The basic reason for these attacks is security flaws which are introduced in any phase of constructing the system. Thus it is important to make the network secure and this can be done by applying security mechanisms while designing the network architecture. This paper focuses on trustworthiness, controllability and security. It describes about the requirements of a network to become secure, the threats to the network and how to control them, the mechanisms to achieve trustworthiness and controllability. it describes two major architectures namely Switch ware and SANE. These architectures provide the network with all the three function-alities namely trustworthiness, controllability and security.

II. REQUIREMENTS AND APPROACH

Our aim is to achieve a network with trustworthiness, controllability and security. For this, we need to design the network architecture in a way such that the above goal is achieved. To do this we first need to understand the re-quirements of the network. Thus, this section focuses on the trustworthiness requirements[1], controllability require-ments[1] and overall security requirements[2].

1) Trustworthiness : Trustworthiness is a property that can be measured or analyzed qualitatively as well as quantitatively. The basic requirements for a network trustworthiness design are as follows :

   a) Access from a resource should strictly not harm the network.
   b) Information transmission should be protected and secured.
   c) The credibility and usability of the server of the network should be enough.

2) Controllability : The requirements of a controllable network is that it should have high efficiency for packet transmission which can be achieved by using some control mechanism for monitoring the states and imple-menting the efficient mechanism when any attack occurs.

3) Security :
   a) Confidentiality- ability to keep the message pro-tected i.e. data transfer protection. No unauthorized person can view these messages.
   b) Integrity-to ensure if any message has been altered or if any misbehavior has occurred with that mes-sage.
   c) Authentication-it checks the reliability of the mes-sage and also checks from where the message has been produced.
   d) Availability-it checks the network traffic and con-firms if the message can enter the network or not.
   e) Data Freshness- it ensures that the data is fresh and that is has not been played back by any unauthorized person.
   f) Self-Organization- the independency and flexibility of a node.
   g) Time Synchronization-turning off some nodes at specific time intervals to improve efficiency.
   h) Secure Localization- identification of the location of other nodes in the network.
   i) Authorization- not all nodes can access the re-sources of a network, only the authorized ones can.

j.)Robustness against attacks- to remove or minimize

k) Resilience- it is allowing a protocol to work well even if some nodes are being compromised.
l) Broadcast Authentication- the ability to not allow the attacker to forge the broadcast command.
m) Scalability- protection of the new nodes added to the network.

III. TARGETS TO BE ACHIEVED FOR DESIGNING A NETWORK ARCHITECTURE

To design a network architecture, we need to achieve some targets[1] to get an improved network in terms of security. This section consists of the targets to be achieved for designing a network architecture with security. They are as follows :

1) Trustworthiness and controllability should be met together harmoniously. These two aspects are interdependent-dent on each other and work hand in hand.
2) To build a network and update the network in time, so that whatever change of trustworthiness has occurred can be reflected and also controlled.
3) For building and developing a network architecture with trustworthiness, controllability and security, direct control should be provided i.e. cross layer correlative mechanisms should be built such as gathering the network information, configuring the network parameters,etc.

IV. THREATS TO THE NETWORK AND ITS DEFENSIVEMEASURES

In this section, the types of threats that can attack a network is described. Also, some defensive measures for these threats are mentioned. This will give the basic idea as to why the requirements mentioned above are important and to be aware of the kinds of threats that can harm the network. The types of threats[2] along with their defensive mechanisms are described below

1.)Denial of service- This attack aims at reducing the capability of a network to provide service. It sends useless packets to a node and does not allow even the authorized users to access the packets and nodes. Defence : applying authentication streams to the network will help prevent this attack.

2.)Node capturing- If a node is captured and it has some stored information, then it can be obtained by an ad-versary. Defense: use of a protocol called LEAP i.e. Localized Encryption and Authentication protocol which takes care of the inter-node traffic authentication.

3) Wormhole attack- The process of sending a message from a starting node to some other node which sends it further to its neighbours, such that the other nodes consider the sender node as the starting node and try to send the message to the actual starting node which is never accomplished because the starting node is far away from the current node. Defence: use of DAWSEN rout-ing protocol which follows the hierarchical tree method.

3.)Sinkhole attack- This attack tries to clear the traffic using a compromised node and makes that node appear attractive to other nodes with respect to the routing algorithm. Defence: use of geographic routing protocols will help prevent this attack.

4) Passive information gathering- An unauthorized user can gather data from the stream if it has a powerful receiver and an antenna. The messages can be leaked and the message IDs can be revealed from those nodes. Defence: use of well-built encryption techniques can prevent this attack.

5) Hello flood attack- When a node with very high power sends a hello packet such that, even far away nodes receive it and consider it as their parent. Due to this the delay increases because the messages need to be routed multi-hop to the parent. Defence: this can be prevented by checking the bi-direction link which ensures that they reach their parent in one hop itself.

6) False or malicious node This attack is caused by Addition of false nodes in the network. Defence: it needs to be checked in the routing layer for prevention.

V. TRUSTWORTHINESS & AND CONTROLLABLE MECHANISM

In the above sections we studied about the threats to the network, the requirements and approach and the targets to design a network architecture. In this section we will study about mechanisms[1], that can be implemented in the network architectural design to enhance the trustworthiness, controlLability and security of a network. These mechanisms majorly focus on improving the three aspects mentioned above. We are going to study certain types of architecture designs ahead, where these mechanism are applicable.

A. Divison of functionalities of a network

To improve the trustworthiness and controllability of a network and for better management of the network, its functionalities can be divided into the following planes.

1) data plane- it performs the dame function as of the traditional data plane i.e packet forwarding. It also handles individual packets sent by the trustworthy decision plane which is based on control instructions.
2) trustworthy monitor plane- it identifies and searches the physical components of a network, manages the trustworthiness relationships among network components, collects the proofs that are required for the evaluation of trustworthiness of the components and ultimately forms a network connection view.

B. Collecting and processing trustworthy information

This mechanism focuses on the design of a trustworthiness model that aims at improving the access control system. Here, the trustworthiness information is divided into three types:

1) Identifier- It is the root of evaluation of trustworthiness. If the variable of the identifier is untrustworthy, then the result of the network is untrustworthy.
2) Defense ability- Defense ability is nothing but to be able to defend the network from the threats by adding patches and by the availability of an anti-virus software.
3) User behavior- This refers to attempting to access the prohibited network services, peeping through the access networks and the recommendations made by other authority points, etc.

Thus a network for every requirement point can be built and the trustworthiness value can be computed based on the model.

C. Trustworthy and controllable path computing mode

In this mechanism, the combination of centralized and distributed path-computation is used that is, putting together the

common functions of the sophisticated systems and implementing the functions in a centralized way. There is a server called TPCS (trustworthy path computing server). The routers focus on forwarding the packets to TPCS , provide topology information to it and receive instructions from it.

1. Protocols in the trustworthy monitor plane collect network states, trustworthiness information and reach ability information.
2. The trustworthy transmission plane transmits these states to the TPCS.
3. The TPCS computes the routing tables based on certain trustworthy goals such as security.
4. Finally, the trustworthy transmission plane configures the results in the routers.

D. Direct control design with cross layer

Its main target is to establish an integrated framework of sharing and analyzing network states, and making decisions among various protocol layers. It aims at the unified trustwor-thy and controllable network goals. In cross layer design, some control mechanisms implemented in several protocol layers should be harmonized to deal with a common event, and the upper layer can respond rapidly to the changing of network states. It decreases resource consumption for computing and transmission and it speeds up the procedure of processing emergent events

VI. TWO TYPES OF NETWORK ARCHITECTURES

In the above sections we have studied the basic concepts required for designing a network architecture. We understood the requirements of the network, the approach and the target, the threats to the network and the trustworthiness and control-lable mechanisms that can be implemented while designing the network architecture. In this section we will focus on two specific types of architecture namely the switch ware architecture and SANE architecture. We will understand how these architectures focus on security and enhance the security of the network. Their major focus is to enhance the security of the network which will indirectly enhance the trustworthiness and controllability of the network.

VII. TYPE 1 : SWITCH WARE ARCHITECTURE

The switch ware network architecture[3] is a layered architecture which focuses on improving the security of the network. This architecture allows the user to use different approaches for improving the security of the network , without disturbing the network and keeping it in use at the same time. These approaches include :

1) Cryptography based security to maintain trustworthiness.
2) Using verification techniques such has type checking and program verification for secure functionality.[3]

These approaches are applied on the three layers namely Active packets, active extensions and active routers. Language based approach : To design a secured model the following approaches to security in an active network can be used :

1. Public facilities- These facilities are available to everyone because accessing them will not be very risky.
2. Authenticated facilities- These facilities require authorization for use. An identity check is important after which the facilities can be utilized. Not everyone can use these facilities. The users who have the authorization only they can use it. For Example, login facility where we require a password for access. Forms of authentication based on cryptographic keys are used to access these facilities.
3. Verified facilities- These facilities go beyond the public and authenticated facilities. If a node is formally able to verify certain properties, only then these facilities can be provided to that node.

A. Verification

The technology is well advanced in all the contexts, which makes the use of verification in improving security, a major advantage. Safety in operating systems, safety in program-ming languages is a very good example of modern security techniques which influences the verification criteria which is actually used to improve the security. The best example is Java which has a dynamic verifier to enforce host security policies for execution of the complied byte code of the web applets. To apply these technologies to the network, some challenges are being faced :

1) There is a limit to the value of verification when using traditional approaches.
2) Experience is needed in integrating verification with authorization.

B. When to check types

The reason behind strongly typing the switch ware routers is that their integrity is maintained. But when there is down-loadable code or mobile code, they cannot be considered trustworthy. Thus the routers should type check the programs themselves so that the routers remain strongly typed. The code for active packets and active extensions will be executed remotely by the programmer, so it is important for all the errors to be checked and solved before the code goes to the router. This is because the router will perform its type check and send it in the network but statically checking for errors will help the programmer know that the routers type check is accurate. Thus for active packets and active extensions, the programming language should be strongly type checked. This process of detecting the errors at programming level as well as router level type checking is done for improved security and this is the main approach.

C. Active packets

In switch ware architecture, the active packets consist of the code as well as the data in traditional data packets there were two parts header and payload which are replaced in switch ware by code and data. The code takes the destination address of its

data. It is responsible for data transport. It checks for the next hop in the outing table and then forwards the entire packet to the next hop. The code then delivers the payload part of the data at the destination.

D. PLAN

PLAN is known as programming language for active net-works. As the name suggests, it is a programming language designed to meet the design goals of a secure switch ware architecture. PLAN is simply typed lambda calculus with extensions to support remote evaluation. It only supports very simple data and control structures and thus it is easy to compile and interpret. It cannot be executed without authentication and it cannot leave behind or change a state on a router. It is strongly typed to maintain the integrity of the router. It helps in combating denial of service attacks.

E. CAML

CAML provides several of the design goals outlined for PLAN. It lacks the resource bounding and the special remote execution facilities. There are many applications which will **require** authentication in any language. In these instances, there is a simplicity gained by programming the active packets and the active extensions in a single language. In the case of remote execution facilities, CAML has provided the interface necessary to dynamically load code which has allowed us to build a general remote execution facility.

F. Active Extensions

Active extensions is the second layer of the switch ware architecture which when combined with the active packets, provide us with a power which makes it possible to implement arbitrary protocols and functionalities. Active packets can call active extensions to provide authenticated services, making it possible to avoid default authentication for active packets. Active extensions have more security checks as compared to active packets. The active extensions arrive on the routers, they are statically type checked and then provide services to the active packets. The active extensions might carry some credentials with them too.

G. Secure Active Routers

The switch ware architecture depends on the language systems to assure the safety and security of the network. It is also crucial to analyze the requirements to build an active and secure router. The goals for our secure active router infrastructure are:

1) To support the language-oriented model used at higher layers of the Switch Ware architecture
2) To incur minimal costs while the system is an operational state. This is done by migrating costs to an infrequently performed preoperational phase.

3) To maximize system security under a minimal set of assumptions about trusted components.[3]

VIII. TYPE 2 : SANE NETWORK ARCHITECTURE

This section talks about the second type of architecture which is known as Secure and Active network environment (SANE) network architecture[4]. This architecture provides secure network level solutions. It is based on the AEGIS secure bootstrap architecture. The system remains in a trusted state by having done the integrity checks in the network. It also applies node to node authentication whenever needed. Let us study this architecture in detail which gives us the security, trustworthiness and controllability solutions.

A. High level view

It follows the principle of levels of abstraction where each layer is separated from the other and on these layers the higher layers are constructed. It presumes that the underlying layers are treated axiomatic and when this is true, then the system is said to possess integrity. Without integrity, no system can be made secure. Therefore, integrity of the lower layers need to be checked and the transition to higher layers occur only when the integrity checks are complete. For this architecture, there are concerns which are divided into types namely static and dynamic. Static concerns are the ones that can be checked once or not very often while dynamic concerns need to be checked timely to maintain the operational state of the system.

B. Integrity and Trust

Integrity is a way of saying that a system is what we expect it to be, it is unmodified. Trust is a more complex relationship, as something can be unmodified, but not trusted, while if a system is trusted, it must remain unmodified for the trust relationship to hold in true sense. Integrity and Trust relationships in an active network setting are of several types. In a layered architecture, each layer in a system trusts the layer below it. For an active network node, a trusted node architecture can be constructed by making the lowest layers of the system trusted, and then ensuring that higher layers depend on the integrity of these lower layers. Therefore any architecture for system security in an Active Network must use a combination of static checks and dynamic checks to remain secure.

C. About the architecture

This sections gives us the basic idea of the SANE network infrastructure. The lower layers of the architecture expect that the system starts in an expected state. The design utilizes a secure bootstrap architecture called AEGIS to reach dynamic integrity checks on a prepacket, or preuser basis. This archi-tecture maintains security in several ways namely performing remote authentication; provides environment for evaluation of switchlets; and a naming scheme for partitioning the node's services name space between users.

D. Aegis overview

This section gives an overview to the AEGIS boot process. It modifies the boot process such that all the code is verified before execution. In every code there is a small part of the trusted code which is excluded by using a digital signature which is accomplished by modifying the BIOS (basic input output system). The BIOS contains the verification code, and public key certificate. . In the AEGIS boot process, either the active network element is started, or a recovery process is entered to repair any

integrity failure detected. Once the repair is completed, the system is restarted to ensure that the system boots. This entire process occurs without user intervention. AEGIS also maintains the hardware and software configuration of a machine. It also maintains a copy of the signature for each expansion card. The integrity test will fail for other cards.

E. Aegis boot process

This section talks about the boot process which every computer follows. This process is divided into four levels of abstraction. Each level is a phase of bootstrap operation. The first phase is the Power on Self Test or POST. POST is invoked in one of four ways:

1) Applying power to the computer automatically invokes POST.
2) Hardware reset.
3) Warm boot invokes POST without testing.
4) Software programs, if permitted by the operating system.

In each of the cases above, a sequence of tests are conducted. All of these tests, except for the initial processor self test, are under the control of the system BIOS. Once the BIOS has performed all of its power on tests, it begins searching for expansion card ROMs which are identified in memory by a specific signature. Once a valid ROM signature is found by the BIOS, control is immediately passed to it. When the ROM completes its execution, control is returned to the BIOS.The final step of the POST process calls the BIOS operating system bootstrap interrupt.

F. Layered boot process

This section specifies the boot process divided into the following layers to simply the AEGIS BIOS modifications. The higher levels have greater functionality.

1) Level 0 contains the small section of trusted software, digital signatures, public key certificates, and recovery code. The integrity of this level is assumed to be valid.
2) The first level contains the remainder of the usual BIOS code, and the CMOS.
3) The second level contains all of the expansion cards and their associated ROMs, if any.
4) The third level contains the operating system boot block. These are resident on the bootable device and are responsible for loading the operating system kernel.
5) The fourth level contains the operating system, and the fifth and final level contains user level programs and any network hosts.[4]

The transition between levels in a traditional boot process is accomplished with a jump or a call instruction without any attempt at verifying the integrity of the next level.

G. Recovery process and Protocol

This section deals with the recovery process and the recovery protocol which is applicable when there is an integrity failure in the network host. In the case of integrity failure the system boots into a recovery kernel which is on the network card ROM. The recovery kernel contacts to a trusted host through the secured recovery protocol to recover the falied component, and then the failed component is repaired and the system is restarted. The protocol used is based on the station to station protocol. The basis of the protocol is the Diffie-Hellman exchange for key establishment, and public key signatures for authentication. In our architecture we use DSA digital signature standard, but other algorithms can be used.

H. Bootstrapping a SANE network

Now our main concern is how to bootstrap a SANE network. A node is brought up in a secure manner and it attempts to develop trust relationship with its peer. They exchange certificates and establish a shared secret key. The certificates exchanged at this stage are used to verify the neighbours and build trust relations with the domains. The trust relations are used to minimize the setup costs, allow mobile type of applications where authentication is necessary, secure message exchange between peer active nodes, establish authenticated packet forwarding channels and deter link traffic analysis.

IX. CONCLUSION

Since the current network architecture was designed based on some assumptions, which are disappearing with the rapid development of the network, the network is suffering more and more severe threats of security and issues of ensuring QOS. Thus, we proposed that trustworthiness, controllability and security should be taken in account in a holistic mode when designing new network architectures. We introduced two types of architectures namely Switch ware network architecture and SANE network architecture. These architectures are a common solution for achieving trustworthiness, controllability and security.

.

ACKNOWLEDGMENT

I would like to thank Dr.Jagdish Nayak for the guidance and my parents.

REFERENCES

[1] ChuangLin and Xue-HaiPeng,Research on network architecture with trustworthiness and controllability,J.Comput.Sci Technol.,Vol.21,No.5,September,2006.

[2] Abdul Azeem, Dr.Khaleel-ur-Rahman khan, A.V.Pramod,Security Architecture Framework and Secure Routing Protocols in Networks-Survey,International Journal of Computer science Engineering Survey(IJCSES),Vol.2,No.4,November,2011.

[3] D. Scott Alexander, William A. Arbaugh, Michael W. Hicks, PankajKakkar, Angelos D. Keromytis, Jonathan T. Moore, Carl A. Gunter, Scott M. Nettles, and Jonathan M. Smith, The SwitchWare Active Network Architecture, University of Pennsylvania ,Vol,June 6,1998.

[4] D. Scott Alexander, William A. Arbaugh, Angelos D. Keromytis, and Jonathan M. Smith, The Secure Active Network Architecture, University of Pennsylvania ,Paper 114,January,1997.

AUTHORS

First Author – Abdullah Nayaf Shafi, Electrical & Electronics engineer, Birla Institute of Technology Pilani, Dubai Campus, nayafshafi@gmail.com

Correspondence Author – Abdullah Nayaf Shafi, nayafshafi@gmail.com, nayaf_shafi@gmail.com,+9710505467340