Rethinking the link security approach to manage large scale Ethernet network

Khan Ferdous Wahid
Department of Information and Communication Technologies
Universitat Pompeu Fabra, Barcelona 08018, Spain
Email: khan.ferdous@upf.edu

Abstract—The expansion of Ethernet in service provider domain requires modification of its service models and management issues. Works are underway inside research community, but their main focuses on Quality of Service, failure recovery, scalability, reliable connectivity, resource utilization and traffic monitoring put security in isolation. As developed initially for a shared link communication, Ethernet lacks security feature. Standardized Media Access Control security (MACsec) provides segment-based security. Its link-constrained feature is constructed mainly for scalability, key-agreement simplicity and traffic analysis, but unsupported multi-segment confidentiality and integrity make the MACsec vulnerable and disqualify it for large Ethernet deployment where switches reside outside of secure premises. In this paper we pinpoint vulnerabilities remained in existing mechanism, and further classify security requirements for unicast and multicast frames. Moreover, we present arguments to support our classification and propose new security approaches using existing Ethernet-based protocols. Finally, we evaluate the performance of our secure data transmission.

I. INTRODUCTION

Ethernet was built for the efficient communication on a shared link, but its simplicity, cost-effectiveness and easy management incite the researchers and organizations to put their endless efforts to spread the technology for more than 30 years. Now its growth covers almost all domains of networking and its tremendous speed lures the service providers to deploy new services (voice, video etc.) to million users. Large scale deployments are connected by wide area network (WAN) links (e.g., T1, E1, Frame Relay), but the data and error rate supplied in these links introduce bottlenecks when every internal network consists of high-speed Ethernet. Now almost all data traffic (98 percent) in enterprise networks start and end their journey on Ethernet Local Area Networks (LANs) [1], so service providers should not introduce bottlenecks when they move data from one LAN to another. Moreover, WAN links cost money because they are leased from service providers along with costly equipments, whereas bandwidth in LAN is completely free with Layer-2 based high-speed communication devices. Also experts are required to manage WAN devices (e.g., routers, ATM switch, multiplexers). Therefore, the large scale networks are converging in Ethernet-based simple solution and Metro Ethernet Networks (Ethernet-based metropolitan area networks) are coming into existence [2], [3].

Service providers generate profits using their networks, so they try to provide as many services as they can with reasonable cost, and security is one of the main features they need to integrate into their services, because they cannot offer an open solution to their customers where data can be accessed by any one. Customers want reliable connection to send their sensitive data, so service providers must guarantee to protect the data along the way in their infrastructure, otherwise unauthorized access to data by outsiders cause stiff penalties to the service provider. Virtually non-existing security of native switched Ethernet (IEEE 802.1D switched Ethernet) [4] makes the network vulnerable. Therefore, inside intruders can access the clear data even inside secure premises. On 2006, Media Access Control security (MACsec) [5] was standardized to secure the layer-2 communication between adjacent authorized devices, but such link-constrained protection introduced for the scalability of key-agreement and Ethernet forces the data to travel in clear inside intermediate devices. Hence the switches inside the network provide vulnerable points to get data in clear. In large scale deployment, these switches can reside in public places where physical access to the devices is feasible. Thus the security gap puts the infrastructure at risk. As Ethernet has evolved towards metro network, we need to start rethinking about its security before being deployed in cities all over the world.

In this paper, inspired by recent advances in cryptography, silicon technology and Ethernet, we propose new design concepts to overcome the existing vulnerabilities in Ethernet. At first we clearly justify the necessity of Layer-2 security (our motivation) in section 2. Then we classify the security requirements for unicast and multicast frames, and propose the security approaches in section 3. Our proposals aim to secure the point-to-point and point-to-multipoint communication in an efficient manner, so that they can exonerate the links from new message exchange overloads. How we can achieve this is described in detail at section 3. Furthermore, we evaluate and compare the performance and secureness of data transmission of MACsec with our solution, and guide future research at section 4. Lastly, we conclude our paper in section 5.

II. MOTIVATION

A. Why Do We Need Layer-2 Security?

As service providers are going towards the metro Ethernet network, the convergence in simple and high-speed Ethernet simplifies the topology and multiple-access operation of network. The ultimate simplicity introduced by the full-duplex...
operation replaces the traditional shared medium Ethernet feature, because the Carrier Sense Multiple Access with Collisions Detection (CSMA/CD) restricts the maximum collision domain diameter to 200 meters, whereas the full-duplex Gigabit Ethernet is only restricted by the underlying physical layer technology [6]. Now every end station has point-to-point connection to the Switch (such setup is called micro-segmentation [7]), because full-duplex capability necessitates simultaneous transmission and reception. MACsec provides a point-to-point security between adjacent devices to secure such direct communication. The unencrypted frames relayed internally from one port to another inside a switch facilitate traffic analysis at those connection points, but leaves data in clear for everyone who has access rights or has exploitation capabilities. Moreover, the high-speed transport services using Layer-2 mechanism require simplified operations, but if we use upper layer security, then several networking layers need several management elements, hence inter-layer coordination brings complexity and cost.

MACsec ensures key-agreement simplicity by the local initiation and management of a secure association. It also generalizes scalability, but the hop-by-hop secure domains introduced by the local key-agreement schemes force a switch to decrypt a frame at the input port and encrypt at the output port. So any error generated during the inter-port relay operation goes undetected. Moreover, MACsec cannot put two particular end stations in a point-to-point and group secure domain at the same time, because it selects the secure domain by the MAC address. So one MAC address cannot point to two domains at the same time and there is no flag bit to help. Furthermore, security breaches at the lower layer can be undiscovered at the upper layers.

Thus multi-segment confidentiality and integrity can address all shortcomings mentioned above. Also no Layer-2 security approach requires a change in the upper layer applications. Hence, such transparent security is best suited for business applications.

B. Other existing approaches that motivate us

Although the Layer 2 Tunnel Protocol (L2TP) contains the term Layer-2, it is actually a session protocol and it does not provide protection and firm authentication [8]. So it requires support from external security mechanisms (e.g., IPSec), and this protocol actually works between two routers. Thus L2TP is not a good candidate for our scenario. Cryptographic Link Layer (CLL) [9] provides several cryptographic algorithms (e.g., MD5, Twofish, SHA-1, AES, RSA) for link layer security, and uses different security mechanisms in request and response messages. In our opinion, it is hard to provide such large number of modules inside a small network interface card (NIC) and CLL also requires unnecessary time to select the appropriate algorithm. Secure LAN (SLAN) [10] uses Address Resolution Protocol (ARP) to initiate the secure channel, but their online communication with the key distribution center (KDC) during the transmission of ARP request and response message generates extra communication overhead and disqualifies the scheme for large scale Ethernet. Furthermore, SLAN does not provide any performance evaluation to judge its fruitfulness. Switch-based single secure domain [11] depends on the secure device identity [12] for the safety of its global domain, so failure of the secure device identity puts the total infrastructure in danger. Moreover, this approach is applicable only in the internal network of a service provider.

So we need an on-demand, scalable and multi-segment security solution that can efficiently secure the data transmission across the switched network (including service provider) and alleviate the complex computation inside switches.

III. OUR SECURITY APPROACHES

A. Requirements

Recent researches [13], [14], [15] on Ethernet have discovered that the broadcast mechanism used in service and resource discovery is one of the main drawbacks to deploy Ethernet in large area. Their proposed functionalities to overcome this drawback by limiting broadcast at the edge level suggest us to consider only the unicast and multicast communication in future Ethernet. For this reason, in this section, we are proposing our concepts to secure the Layer-2 unicast and multicast communication. But before explaining our concepts, we should classify the security requirements of unicast and multicast messages. Unicast messages are used for point-to-point communication. So we need a point-to-point secure channel between the sender and receiver to securely transmit such messages. Thus end-to-end confidentiality and integrity, data origin authenticity and replay protection are the major concerns. As MACsec provides all of these in a link constrained manner, we need to build an end-to-end secure channel across multiple segments by sharing a secret key. Finally, we can follow the similar procedures to those currently used in MACsec.

Multicast messages require same secure functionalities for a group, but we cannot guarantee the data origin authenticity because all group members obtain the same symmetric key to communicate securely, hence the originator of the message could be any authenticated member. It is possible to get data origin authenticity here using public key cryptography, but avoidance of such computationally complex and slow mechanism for continuous data transmission is the unanimous decision.

Although control or management messages are time and link constrained in nature, their sporadic use by different protocols (e.g., MMRP, MVRP, SNMP, MACsec, IEEE802.1X-2010) in near future will consume bandwidth. So we use the unused space of existing protocols to diminish new control messages generated by the security protocol.

B. ARP-based security for unicast communication

The Address Resolution Protocol (ARP) request is initiated by the sender to obtain the Layer-2 address of the receiver for transmitting unicast messages. So the intention of point-to-point communication is expressed by the initiation of ARP
request message. Also ARP messages are 42 bytes long without the padding and Cyclic Redundancy Check (CRC). Hence it is possible to integrate the key-agreement messages inside the ARP messages to build a point-to-point secure channel between two end stations before the beginning of actual communication, but ARP’s two way message exchange forces us to look for a plug-n-play key agreement mechanism that can build the secure channel on demand. So identity (ID) based cryptography has a great potential to provide security in our scenario because the ID (in our case the MAC address) itself is the public key and there is no need of a central certificate authority to authenticate the public keys. The received ARP request message acquires the ID of the sender to the destination, so it is possible to randomly generate a secret key at the receiver side and encrypt the key using the ID based cryptography to insert into the ARP reply message. We could use an ID-based key agreement protocol like [16]. The sender can get the secret key protected inside ARP reply message, so both systems have the shared secret in their possession for secure communication. In the secure communication phase, each system should use the advance encryption standard (AES) because it is standardized in MACsec. They must include an incremental sequence number in every frame to prevent replay attacks as MACsec provides with packet number.

There are several issues we need to correctly consider for deploying the above mentioned security. First, every device should support Elliptic Curve Cryptography as it is needed for ID based schemes. The IEEE draft standard secure device identity is trying to manufacture each system with a built-in public key cryptographic module, so that the device can be authenticated to become a trusted component in the network. This cryptographic module inside each device has support for RSA and ECC algorithms. So we can easily take advantage of this module, but the key generation phase should be initiated immediately after the successful authentication of the secure device identity. In this way we can save the public keys from MAC spoofing attacks.

Second, a local key generation center (KGC) or trusted third party (TPP) or KDC is required to generate the ID based private keys and other parameters for the secure communication inside a service provider. The MACsec needs an Authentication Server (AS) to provide authorization to each device, so the same machine could be used for KGC. Although we assume the KGC is totally trusted like the AS, it can decrypt any cipher text message or can forge other entities, so non-repudiation is not provided in our model. Actually we do not require any non-repudiation capability at the Ethernet level. Also MACsec does not support any non-repudiation. Moreover, the secure device identity requires a local public key infrastructure (PKI) where the built-in certificates can be registered. So the local certificate authority (CA) could act as KGC.

Third, a global KGC (Forum of all service providers) is required to generate ID based keys to all networking devices of all service providers for inter-provider communication, as depicted in Fig. 1. The forum needs to be equally trusted by all service providers. We separate the central domain from local domains, so that global key generation never collides with local KGCs and internal traffic of a service provider never can be intercepted by the Forum. The keys generated by the Forum will only be used during provider-to-provider communication. The internal communication of a service provider will always be depended on the local KGC. If all providers agree, they can implement hierarchical ID based encryption (HIBE) mechanism [17] without any modification in the infrastructure, they only need to store the keys computed by the root key generator into their local KGC instead of generating their own keys. It simplifies the key management and usage scenarios because each system needs to store only one set of ID-based keys.

Fourth, when a sender sends an ARP request message, it should sign the message with global ID based key, because it does not know the location of the other end. So the border switch should intercept that message to set flags before transmitting to other service provider domain. The destination can check the flags to determine the location of the sender and the appropriate key. The ARP reply from other domain should be analyzed at the border switch to check the correct settings of the flag bits. This is required only in non-HIBE infrastructure.

Fifth, the destination randomly generates the secret key in our model, so the server could overwhelm by excessive computation when thousands of users send their requests. In that case the attached switch of the server can serve the proxy ARP operation. As servers are always connected with high-end switches, it is not a critical task for such powerful devices.

Sixth, if one host does not support our protocol then the adjacent switch (first hop switch) should take the responsibility to build a secure channel to the other end. If both hosts do not support our model, then the secure channel should start from first-hop switch and end at the last-hop switch because all switches must support our protocol.

IEEE always provides backward compatibility, so in MACsec, every port of a switch needs to support shared medium although microsegmentation will always be present in high speed network. Hence each physical port unnecessarily supports several virtual ports (65534 virtual ports [18]) to accommodate several secure channels for the shared end stations, which require a significant amount of unused memory. But in our proposal each switch (not each port) needs to store two sets of identity based keys (need to store only one set if
HIBE is present), one for its own domain and another for the global domain. Also the integration of ID based cryptographic module inside a device is feasible because ECC is already supported in secure device identity and pairing based operation time reaches $\mu s$ [19]. Moreover, we have at least 1464 bytes (IEEE802.3 Ethernet frame, 1472 bytes in Ethernet II) free in ARP message to put our protocol information, so it is feasible to integrate. As ARP cache generally timeouts in 20 minutes, the point-to-point secure connection could last such short time. It is good from the security perspective because an attacker gets limited time span. We should consider one issue here, as two end-stations may reside far away from each other, they could be non-synchronized, and counting of 20 minutes for ARP cache starts differently in two machines. So one machine can delete the cache and the related secret key much earlier than the other end, which brings inconsistency.

Thus our system should store the few minutes more to correctly receive encrypted frames from the other end. The machine could store the key and the MAC address of the other end in a temporary cache after elapse of 20 minutes. To force the key revocation, the machine can send an UNARP [20] like message as soon as it receives a frame encrypted with a key of temporary cache.

C. MRP based security for multicast communication

The multiple registration protocol (MRP) [21], formerly known as Generic Attribute Registration Protocol (GARP), is the generic protocol that facilitates the networking devices to declare, register or deregister their attribute values. Currently, it supports Multiple MAC Registration Protocol (MMRP) and Multiple VLAN Registration Protocol (MVRP). MMRP is required for multicast communication. When host B (Fig. 2) wants to receive a multicast address, it declares its intention. Switch one receives the declaration at port one, so it register the address at that port and declares through all other ports. Every switch on the path registers the address at the input port and declares on other ports. So when the declaration reaches to the server S (who provides the multicast service), it knows that there is an end station who wants to receive the service. So it can transmit the multicast message. The MMRP frame format (Fig. 3) contains variable number of Messages, and each message contains attribute type and attribute list, where each attribute list contains variable number of attributes. Moreover, each attribute has variable length. Such variable number of messages, attributes and variable length of attributes provide us great flexibility to integrate our key-agreement parameters inside MMRP frames.

We should integrate our parameters inside the attribute whose type is "Group Membership (value 0x01)". because this attribute is used to register a multicast address [7]. Similar ID based schemes (as in ARP) can be used for building secure channels, but the server should send the same secret key to all members, so that everyone inside the multicast group can decrypt frames. There is one exception that requires extra operation. If both host B and host A declare for the same multicast registration, switch one registers them in the appropriate input ports but declares only one message to other ports because both hosts need the same registration. In that case the switch can build a secure channel to the server and send the secret key to hosts upon receiving the key from the server, but such operation initiates $n$ unicast messages inside the switch for $n$ hosts. So our proposal here to use the “Extension to multiple recipients” algorithms described in [22]. This scheme avoids the pairing based encryption at the sender part, so the switch can efficiently (without much computation) send the encrypted secret key to multiple hosts.

IV. EVALUATION AND FUTURE WORK

For our evaluation, we assume that the sender and the receiver already get their shared secret for the point-to-point communication across the switched network, because our future plans contain the implementation of ARP and MRP based key-agreement protocols. We think the possible communication overhead introduced by our scheme will not exceed the MACsec operation, because MACsec requires secure device identity mechanism for the device authentication and also necessitates Extensible Authentication Protocol (EAP) to get the shared secret key from the server, whereas our system could get the ID-based keys during the authentication phase (only requires one more frame in addition to the replied authentication frames). We keep such performance evaluation steps for our future study. Furthermore, the key expires in every 5 minutes for the exhaustion of the MACsec sequence number, whereas ARP and MRP based keys can last longer, because the key can be used as long as the cache retains the ID.

When the sender gets the shared secret in our model, it encrypts the data and sends to the destination. The destination decrypts the data using the same shared secret. On the other hand, MACsec-enabled sender sends the encrypted data and all switches on the path decrypt the data at their input ports and encrypt again at the output ports. Finally, the destination decrypts the frame upon reception. So if we try to compare the number of required operations of our model to MACsec, we get the result of Table 1. If $n$ numbers of switches are present between the hosts in a MACsec network, then $2n$ operations
are required, because each switch does two operations. Moreover, the sender encrypts and receiver decrypts, so we have two more operations. On the other hand, our model requires only the last two operations.

We use Barreto’s High-speed AES implementation in C [23] to test the time required in a round trip travel of data. We put one to four switches between the hosts during the tests, as graphically described in Fig. 4. The switches are actually coded in C with raw sockets and open source libraries. The sender is running on Fedora kernel-2.6.22.1-41.fc7 and it comprises Intel Core 2 Duo 3.16 GHz processor, 3.584 GB random access memory (RAM) and 1Gb Ethernet card. Three switches and the receiver have the same specification. They are running on CentOS Linux 5.0 kernel-2.6.18-128.1.6.el5. Each one comprises a 3GHz AMD Athlon 64 Dual Core processor, 2GB RAM and 1Gb network interface. Another switch contains Ubuntu 9.04 kernel-2.6.28-18-generic and comprises Intel Core 2 Duo 2.40 GHz processor, 1.92 GB RAM and 1Gb Ethernet card. We use the Ubuntu switch only in our four switches scenario (Fig. 4(d)). For this test, we ignore the encryption and decryption operations of the sender. So we get the results of Table 2 for \(4n + 2\) operations in the round trip travel of data, where the receiver decrypts the data upon reception and encrypts before transmission. The results are in nanoseconds.

We get the results of Table 2 from round trip travel of 64, 128, 256, 512, 1024 and 1504 bytes of Ethernet frames. We send each size of frame 1000 times and then do the average of total time. We get some high value for the four switches scenario. In our opinion, this is caused by the Ubuntu switch. When we plot the data (Fig. 5 and 6) only for three and four switches scenario for simplicity, we can easily find that our solution is very efficient compared to MACsec and it protects the data on the path, whereas MACsec leaves data in clear inside each switch and we get that clear data during the test.

Although the IEEE 802.1D standard [24] provides necessary parameters to concatenate 20 switch hops and our proposed scheme gets performance benefits from longer paths, we are not interested in such profit. Here we put our effort to secure the data transmission rather than increasing the performance of the encryption operations, but the evaluation of our proposed system depicts that it can perform better than the existing mechanism. So our solution eliminates the barrier between security and performance.

V. CONCLUSION

Our paper has presented security approaches for unicast and multicast Ethernet frames to overcome the insecurities induced by hop-by-hop feature of MACsec. We have demonstrated our concepts and argued that it is possible to generate on demand pair-wise or group keys across the switched network...
to protect all real-time communications. Our solution can avoid the computational complexity of switches while protecting the data along the way. Also our evaluation results perfectly support our arguments.

REFERENCES


