Building Secure Network Infrastructure For LANs

Yeung, K., Hau; and Leung, T., Chuen

Abstract— ***This paper discusses the building of secure network infrastructure for local area networks. It first gives the main reason why by nature today's network infrastructure is insecure. A new kind of Ethernet switches, called Network Infrastructure Switches (NI-Switches), is then proposed for building secure network infrastructure for LANs. NI-Switches effectively isolate important network signaling from being accessed by unauthorized end computers of a network. To study the feasibility of the proposed techniques, a prototype of NI-Switch was developed by using a Linksys broadband router. Experiments on the NI-Switch were carried out under different networking situations. The results show that without disturbing the normal network operations, the NI-Switch can effectively filter out network infrastructure signals. The results also show that although most signaling protocols (like Hot Standby Router Protocol) were designed with the inband assumption, NI-Switches can still effectively isolate them from being access by end computers.***

Index Terms—***Network Infrastructure, Network Security, Ethernet Switches***

1. Problem Statement: Unauthorized Access of Network Infrastructure Signaling

Computer networks have traditionally been defined as a group of computers connecting together for resource sharing. In [1], a network is defined as "a group of computers and other peripheral devices connected together so that they can communicate with each other." A network therefore includes both the computers and the communication system. However, the term "Network Infrastructure" becomes more and more popular in the literature recently. The term clearly distinguishes the communication part of a network from the computers being connected. The network infrastructure of a network can be thought as the network infrastructure devices (NI devices) plus the physical connections of a network. NI devices include routers, switches, and network infrastructure servers like Domain Name Systems (DNS), Dynamic Host Configuration Protocol (DHCP) and Authentication, Authorization and Auditing (AAA). The main function of network infrastructure is to provide connectivity between end computers. At the same time the infrastructure should be manageable, highly available, secure, and reliable.

The authors of this paper believe that one major security problem of today's network infrastructure is the easy access of network infrastructure signaling (NI signaling) by end computers. NI signaling is the signaling between NI devices. Its main function is to maintain a smooth operation of the network infrastructure. Routing protocols are examples of NI signaling – they provide layer 3 signaling between routers in order to make packet forwarding possible. Another example on NI signaling is Spanning Tree Protocol (STP). It is a layer 2 signaling protocol between switches for maintaining a loop-free frame transmission. In an earlier work of the first author of this paper [2], we discuss that the access of NI signaling by hackers is the key security hole of today's network infrastructure. In this paper, we try to solve this problem by introducing a new kind of Ethernet switches called Network Infrastructure Switches (NI-Switches). NI-Switches will be discussed later in section 3 of this paper.

2. Related Works

Due to the growing attention on network infrastructure, researchers and network administrators become aware of the importance of network infrastructure security. In [3], a taxonomy of security attacks on Internet infrastructure is given. The attacks can broadly be classified into four categories, namely DNS hacking, routing table poisoning, packet mistreatment, and denial of service. A good list of references on Internet infrastructure security is also provided. Currently, researchers are still working on how to detect various kinds of malicious attacks to network infrastructure. Examples include packet dropping [4] and malicious routing [5-7]. At the practical side, a guide on securing the network infrastructure is given in [8].

The research discussed above focuses mainly on the security of network infrastructure at layer 3. In fact, layer 2 is considered as the weakest link of a network by some vendors [9]. In [10], the

Manuscript received April 7, 2006. This work was supported by City University Strategic Research Grant numbered 7001764.

K. H. Yeung and T. C. Leung are with the Department of Electronic Engineering, City University of Hong Kong (e-mail: eeayeung@cityu.edu.hk).

author challenges the traditional belief that infrastructure at layer 2 can be trusted. He also studies how layer 2 attacks can be launched. There are many known methods of layer 2 attacks. Examples are MAC flooding and the attacks to various kinds of layer 2 protocols including STP, VLAN, VLAN Trunking Protocol (VTP), Cisco Discovery Protocol (CDP), Address Resolution Protocol (ARP), DHCP and HSRP. All these only show that both layer 2 and layer 3 should be considered in building a secure network infrastructure[1]. As discussed above, the access of these NI signaling by unauthorized computers is one of the key security problems of network infrastructure.

There exist techniques that indirectly address the problem as discussed above. The first is the use of VLANs to isolate network devices (like routers) from some of the end computers. Since all network devices use inband signaling, this method cannot isolate all network devices from all end computers. The second one is to use layer 3 switches to filter out the NI signaling. Although this method is effective, it requires tedious configuration on the switches. The method is also not scalable because any change on the network topology requires reconfiguration on the layer 3 switches. The third method is to use encryption techniques or VPN tunnels to protect the NI signaling. However, this method requires changes in all routers, switches and the signaling protocols, and is therefore not feasible.

The first reported work that directly addresses the problem as stated above is given in [2]. Recommendation on how to solve the problem is given and is repeated here: "NI signaling should be protected for the sole access by NI devices only. If possible, it is more secure to transmit NI signaling through a separated NI network." In the reference, a layer 2 switching network is suggested to be partitioned into two parts: a network for data traffic and a network for NI signaling. This is illustrated in Figure 1. The interconnection of these two partitioned switching networks is made possible by means of a new kind of Ethernet switches. In this paper, this kind of new switches, called NI-Switches, will be discussed. NI-Switches perform efficient layer 2 filtering based on MAC addresses. This filtering will protect the NI signaling from being access from the network for data traffic.

3. NI-SWITCHES: DEVICES THAT SECURE THE NETWORK INFRASTRUCTURE

3.1 NI-Switches

[1] Although upper layers are also important in network security in general, layers 2 and 3 are particularly important for network *infrastructure* security.

NI-Switches are Ethernet switches. They are, however, different from ordinary Ethernet switches in one major aspect: two types of ports are defined. The first type is called Network Infrastructure Ports, or NI-Ports. These ports are used to connect NI devices including routers and other NI-Switches. The second type of ports is called Non-Network Infrastructure Ports, or NNI-Ports. These ports are used to connect computers other than the NI devices. These ports are the interfacing ports of the NI network to the outside world. At these ports, layer 2 filtering based on the MAC addresses is performed. Figure 2 shows a NI-Switch. As shown, no matter which type of port it is (either NI-Port or NNI-Port), every port can either be a trunk port (multiple VLANs) or an access port (single VLAN). Note also in the figure that layer 2 filtering is performed at NNI-Ports only, not at NI-Ports.

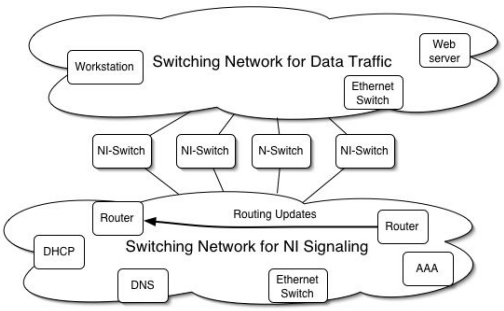


Figure 1 – The partitioning on a layer 2 LAN.

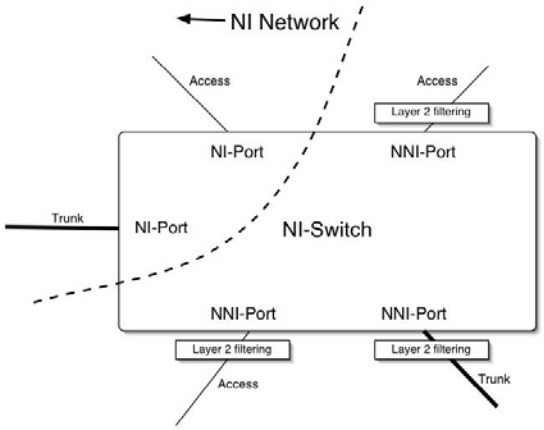


Figure 2 – A NI-Switch

The reason why layer 2 filtering is performed at NNI-Ports is both to prevent NI signaling from leaking out to the outside network, and to prevent outside computers from sending NI signaling to the NI network. At will be discussed later, the filtering is purely based on the MAC addresses of the frames. The frame filters can also be implemented by hardware.

To facilitate frame filtering, two kinds of MAC addresses are defined. They are called Non-Network Infrastructure MAC addresses (NNI-MAC) and Network Infrastructure MAC addresses (NI-MAC). NNI-MAC addresses are

ordinary Burn-In Ethernet addresses of network interface cards of end computers and servers. Each of them consists of a 24-bit Organizational Unique Identifier (OUI) and a 24-bit vendor assigned part. NI-MAC addresses, however, are the MAC addresses of NI devices like routers or switches. The OUIs of these NI-MAC addresses must be configured at the NI-Switches for MAC filtering. For example there are totally 10 routers plus switches in an NI network. Then at most there are 10 NI-MAC OUIs need to be configured at the NI-Switches. The actual number, however, depends on the vendors of these NI devices. Since the devices from the same vendor may share the same OUI, it is possible that only one NI-MAC OUI is needed for these 10 devices. Note that this is the key difference from the design discussed in [2]. With this new design, all existing NI devices can work with the NI-Switches without any firmware modification[2].

After specifying the NI-MAC addresses in a network, frame filtering will then be made at the NNI-Ports of the NI-Switches. Table 1 shows how frame filtering is performed for different kinds of traffic. The detail operations of NI-Switches are discussed in follow.

	Inbound traffic to a NI-Switch	Outbound traffic from a NI-Switch
Unicast	Drop all frames with source MAC address = NI-MAC	Drop all frames with destination MAC address = NI-MAC
Broadcast	Drop all frames with source MAC address = NI-MAC	Drop all frames with source MAC address = NI-MAC, except ARP requests
Multicast	Drop all frames with source MAC address = NI-MAC	Drop all frames with source MAC address = NI-MAC

Table 1 – Frame filtering at NNI-Ports.

3.2 Operations of NI-Switches

Unicast Traffic

There are two type of unicast traffic: Unicast-NI and Unicast-NNI. Unicast-NI traffic is traffic sent between two NI devices. Examples include Border Gateway Protocol (BGP) messages, AAA messages, and SNMP packets sent from an agent to a SNMP monitor. As shown in Figure 3, this kind of traffic will be blocked by all NNI-Ports[3]. On the other hand, unicast-NNI traffic (like a packet sent from a workstation to a web server) will not be filtered out at NNI-Ports.

Broadcast Traffic

Figure 4 shows two kinds of broadcast traffic: Broadcast-NI and Broadcast-NNI. Both of them have a destination address of all F's. However, they can be differentiated by the source address of a frame. As shown in the figure a Broadcast-NI frame (like a Routing Information Protocol version 1 (RIPv1) broadcast) will be filtered at all NNI-Ports. Even with the sniffer program, hackers outside the NI network cannot access to this sensitive NI information. This explains why we can use NI-Switches to build a secure NI network. Figure 4 also illustrates the operation of NI-Switches for Broadcast-NNI traffic. Like ordinary Ethernet switches a broadcast frame of this kind is flooded to all ports of a NI-Switch.

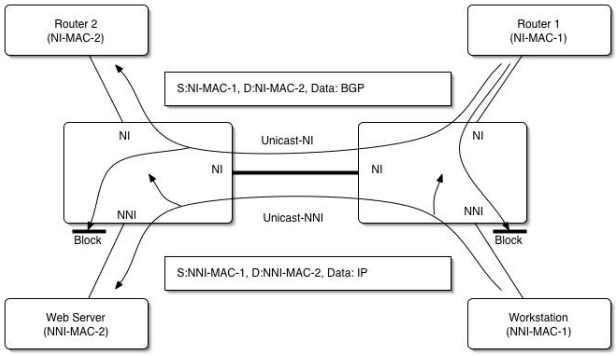
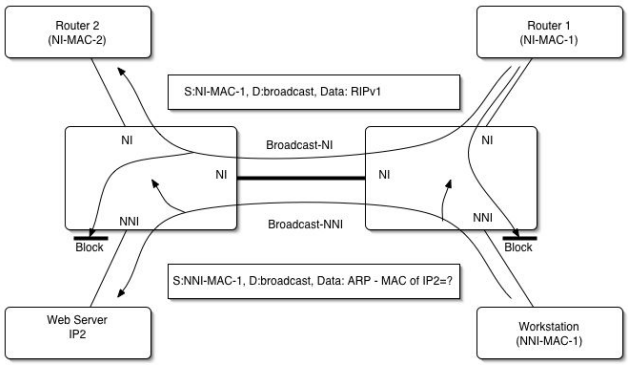


Figure 3 – Transmission of unicast traffic by NI-Switches.



[2] In our earlier design as discussed in [2], a unique OUI is used for all NI devices. Existing routers and switches may need to change their MAC addresses by firmware upgrade.

[3] Note that an ordinary switch *will* forward unicast packets to all ports when the destination MAC address is unknown to it. A switch will also operate like a hub if it is attacked by attacks like MAC flooding.

Figure 4 – Transmission of broadcast traffic by NI-Switches

Multicast Traffic

Many NI signaling protocols use multicast for delivery. These include routing protocols (e.g. RIPv2 and Open Shortest Path First (OSPF)), multicast protocols, layer 2 protocols (VTP, CDP and STP) and others (HSRP). When a NI device uses its NI-MAC address to send out these signaling messages, these messages will not be leaked to the outside network through the NNI-Ports.

Figure 5 shows how multicast traffic is sent through NI-Switches. An example on HSRP is used. As shown routers 1 and 2 will exchange HSRP messages. These messages are sent in multicast address 224.0.0.2. The exchange in these messages results in the election of an active router and a standby router, and the appearance of a virtual router. The virtual router doesn't really exist. It simply represents a consistently available router with a consistent IP address and MAC address to the workstations on a network. Packets from workstations will be sent to the virtual router (via the virtual router's IP address and MAC address). The active router will be the actual router to receive these packets (i.e. the active router will have two receiving MAC addresses: its own MAC address or the NI-MAC address in Figure 5; and the virtual router's MAC address). When the active router downs, the standby router will take up the role as the active router of the network. As shown in Figure 5, HSRP messages will not be leaked outside through an NNI-Port. This is because the routers will use their NI-MAC addresses to send out the HSRP messages. The normal data packets sent to the virtual router, however, are not affected. The reason is the virtual router uses a MAC address that is always not an NI-MAC one.

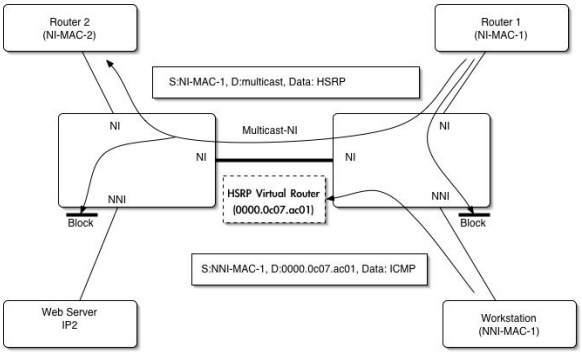


Figure 5 – Transmission of multicast-NNI traffic by NI-Switches.

4. *EXPERIMENTS*

In order to demonstrate the feasibility of the proposed techniques, a prototype NI-Switch was developed by modifying the firmware of a Linksys WRT54GS broadband router. The NI-Switch can perform NI-MAC filtering as described in Table 1. Figure 6 shows the experimental setup being used. As shown, three Cisco routers and one Linksys switch are connected together to form a network with 4 subnets. The subnet 192.168.3.0/24 is further partitioned into two layer 2 network by the Linksys switch. The OUI of the two routers connected to this subnet, namely "00:30:94", is configured in the Linksys switch as the prefix of NI-MAC addresses. On R3, a web server application is run. The PC will access this web server during the experiments. Table 2 shows the experiments being carried out and their corresponding purposes. Due to the limitation on the length of this paper, we only present the results on the third experiment.

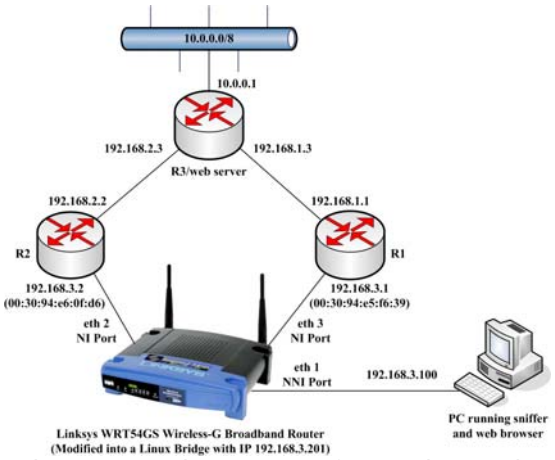


Figure 6 – Equipment setup for carrying out the experiments described in this paper.

Exp.	Protocols used by the Cisco routers	Purpose of this experiment
1	RIP version 1	The purpose of the experiment is to show that broadcast type NI signaling can effectively be filtered by the NI-Switch.
2	RIP version 2	The purpose of the experiment is to show that multicast type NI signaling can also be effectively filtered by the NI-Switch.
3	RIP version 2, HSRP	The purpose of the experiment is to show that the NI-Switch proposed in the paper can on one hand effectively filter out NI signaling (like HSRP), and on the other hand does not affect normal network operations as seen by user workstations.

Table 2 – Experiments being run.

In the third experiment RIPv2 was run on the routers. HSRP was also run on routers R1 and R2 based on the instructions as described in [11]. After the NI-Switch is up, a sniffer program was run on the PC. This was followed by three actions on the PC: i) sent a ping to the virtual router (192.168.3.10); ii) waited for a while to see whether HSRP or RIPv2 messages can be captured; and iii) used a browser to access the web server of R3. After these actions we first checked on the routers' consoles, and found that the routing protocol and HSRP were running properly. Next, we inspected on the packets captured by the sniffer program and the result is shown in Figure 7.

From Figure 7, several important observations can be made. First, as expected, the sniffer program could not capture any NI signaling including RIPv2 and HSRP messages. This verifies that the NI-Switch can effectively filter out the NI signaling. Second, the PC can successfully ping the virtual router (192.168.3.10). This proves that the NI-Switch will not block normal traffic like ICMP and ARP. Third, from the captured packets carrying HTTP messages we can conclude that the network was running properly.

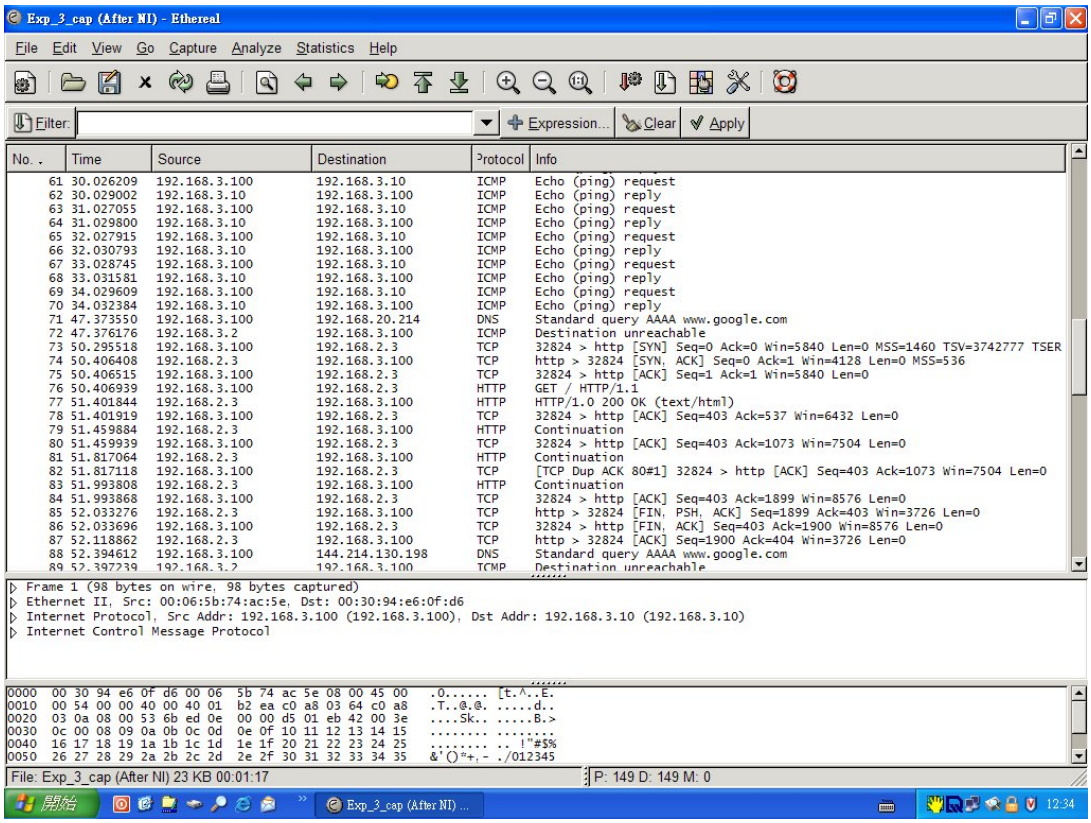


Figure 7 – Packets captured by sniffer after running HSRP in the experimental network.

5. *Discussions on Building A Robust and Secure Network Infrastructure*

Before the end of the paper we would like to make some discussions on building a robust and secure network infrastructure. Although we have already shown that the use of NI-Switches can effectively secure the network infrastructure in LANs, more works are actually needed. The first is on the WAN connections. A network will usually consist of WAN side besides the LAN side. Therefore, NI signaling across WAN links should also be considered in the design of a secure network infrastructure. To follow the recommendations as suggested in [2], a separate WAN for NI signaling may be the most secured design. However, this is very costly and may not be feasible in most situations. It is also not necessary in most cases because the WAN links are usually private to an organization. We recommend the following in WAN design instead. Firstly, minimum bandwidth on WAN links should be reserved for NI signaling – the minimum bandwidth that can keep the network infrastructure running. Secondly, a separate VPN may be set up to carry NI signaling in each WAN link. Thirdly, NI signaling traffic should be treated differently from data traffic in encryption (e.g. different passwords or encryption methods).

The second thing that needed to be done is on the design and development of new NI security devices like NI Intrusion Detection Systems (IDS). Unlike ordinary IDS, NI IDS mainly detects all possible attacks to the NI network. The attacks include DNS hacking, routing table poisoning, packet mistreatment, and denial of service. Although these attacks cannot be launched outside the NI network, they can be launched if a machine inside the NI network is compromised (even though this is less likely than

the case which a machine outside the NI network is compromised). In order to achieve the detection function, NI IDS has to monitor all NI signaling messages passing through the NI network. Alarms will be set when attacks are detected, with malicious devices being identified. Since there remain open problems in the detection of some network infrastructure attacks, research efforts in this area is needed in order to build an effective NI IDS. Currently the authors of this paper are working on the design of this new security device.

6. CONCLUSION

In conclusion, NI-Switches discussed in this paper can effectively filter out NI signaling. This in turn secures the network infrastructure as NI-Switches protect the signaling from being accessed by unauthorized end computers. The implementation on the proposed method based on Linksys broadband routers also show that it is cost effective to produce NI-Switches for production networks.

REFERENCES

[1] Nader J. C., "Prentice Hall's Illustrated Dictionary of Computing," 3Ed, *Prentice Hall*, 1998, p.457.

[2] Yeung K. H., "Building Secure Network Infrastructure," IPSI conference, Bled, December 2005.

[3] Chakrabarti A. and Manimaran G., "Internet Infrastructure Security: A Taxonomy," *IEEE Network*, November/December 2002, pp.13-21.

[4] Zhang X., Wu S. F., Fu Z. and Wu T., "Malicious Packet Dropping: How it Might Impact the TCP Performance and How We Can Detect It," Proceedings of Symp. Security Privacy, May 1998, pp.263-272.

[5] Chakrabarti A. and Manimaran G., "A Scalable Method for Router Attack Detection and Location in Link State Routing," Proceedings of IEEE International Conference on Local Computer Networks, 2003.

[6] Padmanabhan V. N. and Simon D. R., "Secure Traceroute to Detect Faulty or Malicious Routing," ACM SIGMOD Workshop on Hop Topic in Network, October 2002.

[7] Yeung K. H. and Fung D., "Attacking Routers by Packet Misrouting," WSEAS Transactions on Communications, Issue 2, Vol.3, April 2004, pp.493-498.

[8] Noonan W. J., "Hardening Network Infrastructure," *McGraw-Hill*, 2004.

[9] Howard C., "Layer 2 – The Weakest Link," *Cisco Systems, Inc.*, Packet Magazine, First Quarter 2003, pp.30-33.

[10] Marro G. M., "Attacks At the Data Link Layer," *Master Thesis, Department of Computer Science, University of California*, 2003.

[11] Menga J., "CCNP Practical Studies: Switching," *Cisco Press* 2004.

K. H. Yeung is currently an associate professor of Department of Electronic Engineering, City University of Hong Kong. He is also a Certified Cisco Network Professional (CCNP) and a Certified Cisco Academy Instructor (CCAI). His research interests include network infrastructure security, 4G mobile communications systems and Internet caching systems.

T. C. Leung is a graduate of BEng Information Engineering from City University of Hong Kong.