Edith Cowan University

Research Online

Australian Information Security Management Conference

Conferences, Symposia and Campus Events

2015

Innovating additional Layer 2 security requirements for a protected stack

Brian Cusack
Auckland University of Technology

Raymond Lutui
Auckland University of Technology

Follow this and additional works at: https://ro.ecu.edu.au/ism

 Part of the Information Security Commons

DOI: 10.4225/75/57b69e28d938f
13th Australian Information Security Management Conference, held from the 30 November – 2 December, 2015 (pp. 81-86), Edith Cowan University Joondalup Campus, Perth, Western Australia.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ism/184

INNOVATING ADDITIONAL LAYER 2 SECURITY REQUIREMENTS FOR A PROTECTED STACK

Brian Cusack; Raymond Lutui
Auckland University of Technology, Auckland, New Zealand
{brian.cusack; raymond.lutui} aut.ac.nz

Abstract

The OSI and the TCP/IP models divide computing communications into specific groups of activities that facilitate networking and communication. The models represent a theoretical and a pragmatic representation respectively of the systems and both provide security schema for protecting the services. In this exploratory literature research we asked; What are the security requirements for protection at OSI Layer 2? The hypothesis is that low level vulnerability adversely affects higher Layer security. The OSI model is selected to theoretically test the hypothesis and to answer the research question. The research shows that the precautions advocated in the OSI model are helpful but developing forensic capability and obfuscation within Layer 2 further reduces the impact of unplanned events. A survey of attacks confirms previous literature that suggest Layer 2 has vulnerabilities and innovative solutions are required.

Keywords
Layer 2, Security, Innovation, Obfuscation, Protection

INTRODUCTION

Security is only as good as the weakest link and if the weakness is at a low level in the communication stack then every other Layer has potential to inherit the problem. The OSI Layer model has defined the theoretical architecture for network communications (ISO/IEC 7498-1). Standardisation assures that each element of an internetwork uses the same model and hence a message can be moved intelligibly and correctly between participants. The OSI model divides communications into seven hierarchical Layers that provide the necessary services from the application Layer through to the physical Layer of electricity (ISO/IEC 7498-2). Each Layer is dependent on the one below to provide the more primitive functions and is hence interconnected from top to bottom in a communication chain. The four Layer TCP/IP pragmatic model conveys a similar relationship of dependant services for communication that have inter-dependence (Comer, 1995). The consequence is that no matter how a communication stack is looked at – theoretically or in practice – problems low down impact higher Layers. In this research we looked specifically at the OSI Data Link Layer (2) not only because so much has been written on security issues at this Layer, but also because it is the first Layer where serious abstraction in terms of logics and protocols is made from the primitive physical impulses (Altunbasak et al., 2005; NIST, 2013). These theoretical abstractions offer opportunity for proper and improper manipulation that may either better facilitate communication or impede effective communication. The data link Layer also gives opportunity for a range of logical attacks that may exploit the effective communication but not always for the intended purposes. Such vulnerabilities occur elsewhere in the communication stack but Layer 2 is the first real opportunity for logical attacks (Shanmug et al, 2010; Altunbasak, et al., 2005).
This paper is structured to briefly review current literature and define the implications of OSI Layer 2 security vulnerabilities. The OSI model is selected in preference over the TCP/IP model as it has greater clarity around specific layers and reference detail. Two gaps in the literature are identified and theoretical solutions proposed for Layer 2 security.

LAYER 2 VULNERABILITY

The data link layer (2) is positioned to make the bits received from the physical layer (1) reliable and useable in the Layer 2 and network layer (3). This is principally achieved by enforcing security in the layer protocols that assure error detection and control. The five pervasive security requirements for each communication are (Nikkel, 2007):

- Authentication – insurance of the identity of what is being communicated and the parties communicating.
- Access Control – pertaining to the level of availability of information based upon security credentials
- Data Confidentiality – the means of assurance that no unauthorized party can gain access to information either in transit or stasis.
- Data Integrity – when information is accessed or transmitted, this security measure ensures that the communication confirms the data has not been tampered with.
- Nonrepudiation – ensures that the data was received by the proper party involved with the communication and that access to the information cannot be denied by an entity involved in the transfer.

There are also specific security mechanisms implemented at the protocol level of a service in Layer 2. These include synchronisation recognition; flow control; error correction; address audit; control and data links; and, link management procedures (Convey, 2014).

There are at least 14 published and documented attacks on Layer 2 communications (Singh et al., 2015; .Senecal, 2006). Some of the more publicised ones are MAC address spoofing and VLAN hopping. Layer 2 can be influenced by simplistic attacks at layer 1 which in themselves are passed up the stack. These attacks can include attacks on the physical Ethernet cables, signal jamming, eavesdropping or injections; and theft or damage of equipment. Layer 2 however is more sophisticated and logical in construction. A layer 2 attack requires a high level of intelligence and good knowledge of what is going on in the communication actions. Some attacks simply put the network into an unstable state and effectively disrupt the communications. This type of attack is irritating and resource costly rather than disclosing message contents. It can also open other vulnerabilities for exploitation. The MAC flooding attack is an example. More intelligent message attacks are designed to learn legitimate media access control (MAC) addresses and then exploit the knowledge by substituting fake addresses, substituting information or gaining access to a LAN device. Similarly the spanning tree protocol (RSTP) can be exploited by spoofed frames that manipulate the bridging number. Such an attack allows traffic sniffing. Probably the second most widely publicised vulnerability is VLAN hopping. This attack allows the adversary to send traffic from one VLAN to another without the use of a router and the usual security features. A VLAN is a virtualised local area network that has been created to logically (rather than physically) divide a network into efficient service units. These VLANS contain the controls for network devices and protocols that are rich targets for hackers. The success of such an attack opens a network to resource exploitation, data leakage and service hijacking. An incomplete list of Layer 2 attacks would include (Reed, 2004):

- Frame spoofing
- Frame forwarding
- Spanning Tree injection
- Device removal or destruction
- Link unplugging
- MAC Flooding
- MAC Spoofing
- Root Hijacking
- Root injection
- Topology refits
- VLAN hopping
- Admin Hijacking
- Filter injection
- Port mapping and disabling

INNOVATIVE SOLUTIONS

Two innovative solutions are proposed based on the vulnerabilities for Layer 2 reported in the literature. The security solutions are in addition to those reported in the literature and reflect directions more recent network management practice has moved in responses to relentless cyber-attacks. It is inevitable that security breaches will occur at Layer 2 given the number of possibilities, the value of the target, and the challenges network security managers face to protect the Layer. Consequently the first innovation is to develop forensic (post-event) capabilities so that the system may learn from successful attacks and attempt to identify attackers (Endicott et al., 2007; Kushik et al., 2010; Nikkel, 2005; Rowlinson, 2004). Secondly if the Layer is masked or obscured from external communications then the possibility of compromise is reduced. These two innovative solutions are specified in the following two sub-sections.

Forensic Capabilities

Layer 2 has a range of forensic opportunities that may be structured for the retention and interrogation of data. Each of the standardised actions in Layer 2 have the potential for evidence retention. For example, the primitive bits sent up from Layer 1 are framed at Layer 2 and these frames may be sent to another host on Layer 2 or passed up to Layer 3 for routing. The exact time a frame is moved can be established, the content of the frame noted, the way the frame is to travel through the network, and the time it is received. Such information is helpful in a digital investigation and useful for tracing information flow in a network. The data can report the tracing and tracking of both legitimate and malicious uses of the network. In the first instance factual information on the use of devices

connected to a LAN or VLAN may be obtained to see and to manage optimal pathways for higher users and others on the network. When malicious traffic is detected such as floods and spoofs of MAC addresses then evidence can be retained for future attack proofing. The Layer 2 forensic opportunities require preparation and a secure system can benefit retrospectively from the innovation of such a capability.

The forensic analysis of Layer 2 security vulnerabilities shows that much evidence is left after an attack that can be used to harden the system or to track down offenders. Tracking offenders is not always an option on account of network irregularities and obfuscation used by skilled attackers but in some instances trace-back methodologies and footprint histories can be followed. One of the fundamental actions of the data link Layer is to enframe bits and to send the frame to other hosts in the Layer. This action has many useful forensic properties. The properties include the origination time, the header and payload content, the network path, and the receiving time. If the frame is captured at the target host then exact times may be gained but if this is not possible then a time period may be calculated. The filter database retains timestamp information that shows when particular MAC addresses sent traffic and on which port it was received. The filter database aging time also provides a metric that reports when a MAC address last sent traffic (subtract the time it was removed from the database). In this way a communication between any two addresses can be established. The Spanning Tree also retains the path a frame took and this can be verified against data in the filter database of all network switches. Allowing for exceptions, redundancies in the filter database and the spanning tree; and the flooding effect of a new MAC address, the method provides evidential retention once coded and implemented.

MAC flooding is the sending of an excessive number of frames with different source MAC addresses that overflow the Filter Database of a switch. A switch usually recognises each new MAC address and enters it into the database. However the attack is designed to overwhelm the usual activity and to disrupt the normal network actions. Defence against the attack also provides a forensic capability. When a normal frequency is benchmarked for the Layer 2 the abnormal may be detected and immediately traced back to the source. The source may not always be the perpetrator but it will always lead to the vulnerability and the protocol breach. By monitoring the number of changes in the database for each port the attacker port can be identified and shut down. Some proprietary switches defend and provide forensic evidence by sending a log message when the number of learned MAC addresses on a port exceeds a specified number. This feature allows rapid detection and trace back without the use of the database filter information. Similarly MAC address spoofing provides forensic capability for an investigator and a network administrator. The vulnerability can be retraced with the Filter Database and is visible in MAC addresses that keep switching between two ports. The rate of the switching is determined by how often the victim is sending the traffic. A similar effect is observed when a host is disconnected and then reconnected. However, the Link Operational Status changes from up to down before the MAC appears in the Filter Database under a new port in a disconnection; but in a spoofing attack the old interface stays in an up state and the MAC switches between two ports. The access port for the attack can be traced by the chronological order of entries in the Filter Database. The first entry is the genuine client and the later the attacker. In some instances an attacker stages a series of ploys to disrupt this pattern (for example does a disconnection before attack) and skilful detection and forensic analysis is dependent on the network administrator knowing the benchmark metrics for the network. Similar analysis can be applied to other attack scenarios and the variations within the Layer 2 processes noted. For example VLAN hopping, flooding and topology refit forensic analysis. For each of the attacks listed the following data should be retained for forensic capability.

VLAN hopping

- Interface role
- Interface VLAN ID
- Implementation version
- Traffic filter

Ethernet protocol

- Frame header
- Interface address
- Duplex
- Link operation status
- Speed
- Physical Layout
- Traffic filter
- Implementation version
- Traffic counter

Address bridging

- Aging time
- Bridge address
- Bridge identifier
- Bridge priority
- Filter database
- Port identifier
- Port number
- Port path
- Port priority
- Port state
- Root path
- TNC received
- Port role
- Root bridge
- Implementation version
- Bridge log

Hiding Layer 2 from View

Much literature is found regarding hiding of data and network components. Some of the literature concerns fake files and others architectural ploys to obfuscate the communication from critical network components. Honey pots for example are configured to trap and observe user behaviour before access is authorised to secure resources. Firewalls are a common network device that is deployed to filter communications and to prevent malicious or adversary communications from entering the LAN or private network. Cryptographic methods are also widely used to protect data and to maintain the security of communications. At Layer 2 however many attacks can circumvent the best laid defences and alternative strategies are required. One possibility is to mask an entire network at Layer 2 (LAN or VLAN) so that the network is invisible. There are several architectural designs to achieve the obfuscation and relatively few additional components or preparation to be applied.

One solution is to buffer a LAN or VLAN by receiving each native MAC address from the network and cryptographically replace the native MAC with a substitute MAC. The mechanism maintains the key and algorithm so that any request for the related service can be correctly matched in decryption but no agency can penetrate the design within the Layer 2. The mechanism also provides traffic management for Layer 2 so that a flooding attack or tree poisoning could be prevented before inception or rapidly stopped if started. This type of security within the Layer 2 functionality is not well developed in the security literature and yet it has great potential to protect and secure the stack low down. The primary inhibitors of these counter measures at such a low level has been the unavailability of sufficient processing power (and memory) and hence the addition would add potential costs to switches and/or routers. However, recent availability of Layer 3 switches (incorporating Layer 2 functionality) and the improvement of materials for information storage and processing, make the concept viable. Protection within the layer is achieved at Layer 6 with SSL/TSL security protocols and it would appear from the literature reviewed that appropriate security features can be added to Layer 2. The concept has the potential to design multiple virtual security walls around any network. For example multiple fake LANs can be host either inside or outside firewalls based on the substitute MAC addresses. Similarly multiple fake VLANs can be hosted to protect a VLAN that is only accessible by authorised keys. The conceptual design is not new for security architecture but the application within Layer 2 is innovative. Similarly the concept of developing multiple LANs/VLANs to hide a native one is innovative and made possible through these analyses. Many similar schema can be found at higher Layers in the stack but in general Layer 2 is under-resourced in terms of global security mechanisms.

DISCUSSION

The Layer 2 vulnerabilities have led to vender innovations that provide protection from many of the described attacks. Switches and integrated routers are wise to the weaknesses and provide optional functions that - when switched on – provide a first layer of defence. For example the CISCO bridge protocol data unit filter-guard, logs TNC traffic so that the source of an attack may be retraced to the point of attacker connection. However bigger steps can be taken to stop attacks getting inside or sniffing communication packets. Monitoring network traffic is termed sniffing and it provides the sniffer with a wealth of knowledge about the message contents. Layer 2 has tables of information that are checked to identify a host to which the information is to be forwarded. If a host is not found

then a message is broadcast to locate the destination host. The system is relatively secure but three main sniffing attacks are documented. First two concern manipulation of the two tables (CAM and ARP) and the third exploitation of the port data. The Address Resolution Protocol is vulnerable to address spoofing allowing the sniffer to position between the targets and forwarding hosts. The Content Addressable Memory is similarly vulnerable to flooding or overloading to the point of invoking a general broadcast and message disclosure. Port stealing also occurs as a consequence of flooding and allows the attacker to listen to information before forwarding. Traditional protection against these attacks is simple. In the first instance tie the physical ports to MAC addresses. In the second have static ARP entries, and third monitor ARP traffic. It is expected these security procedures are followed but the short-coming is that these procedures are well known and adversaries have developed countermeasures. Consequently we have made two suggestions based on the literature reviewed to further harden Layer 2 defences.

Many defence systems rely on formalised procedures and industry or International Standards to set the ground rules for engagement. However adversaries are wise to these positions and plan ahead to defeat the defences. Innovation, mobility and flexibility are also required in addition to the traditional defence positions, postures and standardised adoptions. Innovation can only be found in research that is prepared to look for better designs and processes that will out play adversaries. The innovations we suggest insist that forensic capability is a mandatory component of protection so that after an event the system can be better presented; and the perpetrator be traced for accountability. The strength the first innovation adds to a system is the disclosure of an adversary so the adversary (human or machine) may be known and secondly the security agency can learn from the adversary and harden their system from further similar vulnerability. The second innovation is to acknowledge adversaries exist but to trick them into taking low value options in fake environments. This can be achieve by inserting a suitable protocol for information management and cryptographic protection within the Layer 2 as a functionality (and with suitable physical resources) so an adversary will only ever see fake LAN/VLAN resources. This suggestion is over and above current functionality in the area and adds value by obfuscation capability. The objective is to hide the native resources at Layer 2 completely and to provide an adversary with multiple fake environments in which they experience satisfying learning and rewards that are of low or no value to the system. The limitations are found in the readiness of a system to take on the extra processing loads and the tendency for security managers to use exteriorities to the layer as the primary defence. Future research can involve the design, build and test of these theoretical innovation in practice. Also the theoretical scope of this work is not closed and further investigation can be made into the potential for innovation or changes in current protection practices.

CONCLUSION

The data link Layer 2 of the OSI communications model has many documented vulnerabilities that require redress. Most vendor supplied hardware and software has options to defend the attacks but the system weakness is often the security management preparation. Knowing a network and benchmarking the performance of the security mechanisms, services and protocols is the beginning of an assured system. The theoretical research reported in this paper suggests that more can be done to protect communications. The two innovations require the addition of retention and analysing capability at Layer 2 for forensic purposes; and the production of fake LAN/VLANs from within Layer 2 to mask and hide the often open workings of Layer 2 functionalities. The future proofing of Layer 2 security can be achieved by focusing on perfecting mechanisms within the Layer, by continuing to ask questions, and by continuous quality improvement.

REFERENCES

Altunbasak, S Krasser, H. (2005). Securing Layer 2 in Local Area Networks. *Network Security*, 26(1), 699-706.

Comer, D. (1995), Internetworking with TCP/IP Volume 1. Prentice Hall: New York.

Convey, (2014). Layer 2 Security Considerations (Ch 2). In General Design Considerations for Secure Networks. Cisco Press: CA.

Endicott, B. Frincke, D. Taylor, C. (2007). A Theoretical Framework for Organisational Network Forensic Readiness. *Journal of Computers*, 2(3), 1-11.

Kaushik, A. Joshi, R. (2010). Network Forensic System for ICMP Attacks. *International Journal of Computer Applications*, 2(3), 14-21.

ISO/IEC 7498-1 Information Processing Systems - Open System Interconnection - Basic Reference Mode: The Basic Model http://www.ecma-international.org/flat/activities/communications/TG11/s020269e.pdf

ISO/IEC 7498-2 Information Processing Systems - Open System Interconnection - Basic Reference Model - Part 2 - Security Architecture https://webstore.iec.ch/preview/info_iso7498-2%7Bed1.0%7Den.pdf

Nikkel, B. (2007). An Introduction to Investigating IPv6 Networks. *Digital Investigation*, 4(2) 56-67.

Nikkel, B (2005). Generalising Sources of Live Network Evidence. *Digital Investigation*, 2(3) 193-200.

NIST (2013). National Vulnerability Database, Common Vulnerabilities and Exposures. http://web.nnd.nist.govt
Reed, D. (2004). Applying the OSI 7 Layer Network Model to Information Security. SANS Reading Room Doc.
Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence*, 2(3) 1-28.
Senecal, L. (2006). Understanding and Preventing Attacks at Level 2 of the OSI Reference Model. IEEE CNSR Conference.
Shanmug, K. Memon, N. (2010). Network Monitoring for Security and Forensics. Lecture Notes in Security, Springer (4332) 56-70.
Singh, R. (2015). Attacks at the Data Link Layer of the OSI Model: An Overview. *International Journal of Advanced Technology in Engineering Science*, 3(2) 501-510.
Yeung, A. Wong, A. (2009). Network Infrastructure Security. Springer: New York.