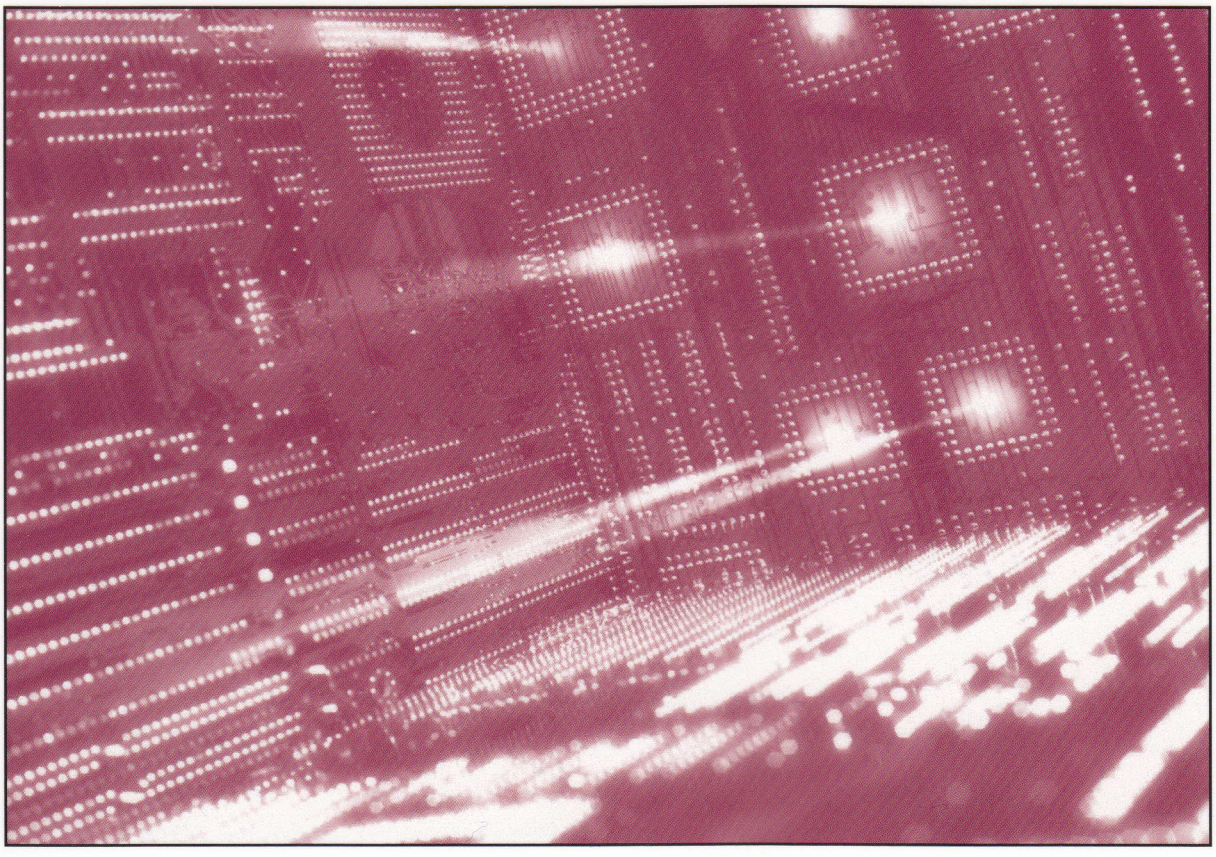
Vol. 5, No. 1
January-March, 2013
ISSN: 1937-9412

An official publication of the Information Resources Management Association

INTERNATIONAL JOURNAL OF

Mobile Computing and Multimedia Communications



IGI PUBLISHING

Publisher of IT books, journals and cases since 1988
www.igi-global.com

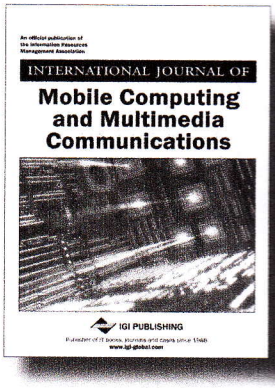
IGI PUBLISHING
WWW.IGI-GLOBAL.COM

CALL FOR ARTICLES

International Journal of Mobile Computing and Multimedia Communications

An official publication of the Information Resources Management Association

The Editors-in-Chief of the *International Journal of Mobile Computing and Multimedia Communications* (IJMCMC) would like to invite you to consider submitting a manuscript for inclusion in this scholarly journal.



MISSION:

The primary goal of the *International Journal of Mobile Computing and Multimedia Communications* (IJMCMC) is to provide researchers and academic communities around the world with the highest quality articles while reporting the state-of-the-art research results and scientific findings allowing students, developers, engineers, innovators, research strategists, and IT-managers in this field to gain greater insight into mobile multimedia as they relate to applications, management, and opportunities within any given construct. This journal publishes original research papers, state of the art reviews, technical notes, case studies, innovative projects, and books reviews on topics leveraging all aspects of mobile computing and multimedia communications: from underlying technologies to applications, from theory to practices, and from servers to networks to devices.

ISSN 1937-9412
eISSN 1937-9404
Published quarterly

COVERAGE/MAJOR TOPICS:

The coverage of this journal ranges from innovative topics to research findings to trends analysis on mobile multimedia and related theories, technologies, methods, applications, and services from all engineering, business and organizational perspectives.

- Active multimedia network
- Advances in MAN
- Augmented reality
- Billing and security for mobile multimedia services
- Coding, equalization, and modulation
- Consumer applications
- Content distribution architectures
- Content distribution internetworking
- Cooperation in mobile multimedia
- Database for mobile systems
- Digital rights managements
- Economics of mobile multimedia
- Effect of mobility on computing
- Emerging access networks
- Enabling infrastructures for mobile computing and multimedia
- Ergonomics and health issues
- Home networking
- Industrial applications
- IP video, streaming, and interactive video services
- Location- & context-aware dependent computing
- Low power networking
- Marketing strategies
- Measurement and modeling of network operation
- Medical applications
- Middleware support for mobile multimedia
- Military applications
- Mobile and multimedia markets and business models
- Mobile aware applications
- Mobile CSCW (computer-supported cooperative work)
- Mobile multimedia interfaces
- Mobile multimedia network traffic engineering
- Mobile multimedia platforms
- Mobile multimedia software architectures
- Mobile operating systems
- Multimedia and integrated services
- Multimedia traffic management
- Multi-point, multicast services
- Network models and architectures
- Network programming for mobile multimedia services
- New mobile and multimedia applications and services
- People with disabilities
- Personal area networks
- Personalization, privacy, and security issues
- Portable computers with wireless access
- Portable devices and smart sensors
- Provisioning of multimedia networks and services
- QoS management
- Regulatory and legal frameworks
- Regulatory and societal issues of mobile computing and multimedia
- Security and authentication
- Social implications
- Source coding/compression
- Spread spectrum communications
- Standardization
- Streaming media protocols
- Training
- Ubiquitous and pervasive computing
- Value added chains for mobile multimedia
- VoIP services
- Wearable computers and PDAs
- Wireless and mobile multimedia network management
- Wireless data services

All submissions should be emailed to:
Dr. Ismail Khalil, Co-Editor-in-Chief
E-mail: ismail.khalil@jku.at

Ideas for Special Theme Issues may be submitted to the Editors-in-Chief.

Please recommend this publication to your librarian. For a convenient easy-to-use library recommendation form, please visit: http://www.igi-global.com/ijmcmc

International Journal of Mobile Computing and Multimedia Communications

January-March 2013, Vol. 5, No. 1

Table of Contents

Research Articles

1 **Reconnaissance Attack on IPv6 to IPv4 Tunneling**
Nazrulazhar Bahama, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia
Anton Satria Prabuwono, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia
Teddy Mantoro, Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

10 **The Novel Method of Adaptive Multiplayer Games for Mobile Application using Neural Networks**
Widodo Budiharto, Bina Nusantara University, Jakarta, Indonesia
Michael Yoseph Ricky, Bina Nusantara University, Jakarta, Indonesia
Ro'fah Nur Rachmawati, Bina Nusantara University, Jakarta, Indonesia

25 **Exploration and Development of the JPEG Compression for Mobile Communications System**
Andik Setyono, Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia & Faculty of Computer Science, Dian Nuswantoro University, Semarang,, Indonesia
Md. Jahangir Alam, Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Sepang, Selangor, Malaysia
C. Eswaran, Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia

47 **Path Loss Model Tuning at GSM 900 for a Single Cell Base Station**
Allam Mousa, Department of Electrical Engineering, An-Najah National University, Nablus, Palestine
Mahmoud Najjar, Department of Electrical Engineering, An-Najah National University, Nablus, Palestine
Bashar Alsayeh, Department of Electrical Engineering, An-Najah National University, Nablus, Palestine

57 **Power Layer Energy Efficient Routing Protocol in Wireless Sensor Network (PLRP)**
Sardjoeni Moedjiono, Budi Luhur University, Jalan Raya Ciledug Petukangan Utara, Jakarta Selatan, Indonesia
Aries Kusdaryono, Budi Luhur University, Jalan Raya Ciledug Petukangan Utara, Jakarta Selatan, Indonesia

69 **Effects of Web Accessibility on Search Engines and Webometrics Ranking**
Media Anugerah Ayu, Department of Information Systems, International Islamic University Malaysia, Kuala Lumpur, Malaysia
Mohamed Ahmed Elgharabawy, Department of Information Systems, International Islamic University Malaysia, Kuala Lumpur, Malaysia

IJMCMC is currently listed or indexed in: ACM Digital Library; Bacon's Media Directory; Burrelle's Media Directory; Cabell's Directories; Compendex (Elsevier Engineering Index); DBLP; GetCited; Google Scholar; INSPEC; Journal-TOCs; Library & Information Science Abstracts (LISA); MediaFinder; Norwegian Social Science Data Services (NSD); SCOPUS; The Standard Periodical Directory; Ulrich's Periodicals Directory

Reconnaissance Attack on IPv6 to IPv4 Tunneling

Nazrulazhar Bahama, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

Anton Satria Prabuwono, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

Teddy Mantoro, Advanced Informatics School, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia

ABSTRACT

Internet Protocol version 6 (IPv6) is created to occupy the insufficient current Internet addresses. Consequently this significant contribution offers huge number of Internet addresses. Besides, the security also has been improved to challenge today threats in competent on IPv6 network. As alternative, an automatic tunneling was introduced along with other transition mechanisms to ensure smooth implementation on existing network. However, it's believed that the implementation of automatic tunneling has altered the form of the IPv4 threats. Then the gained information from this mechanism is exploited to attempt the target network. As a concern, this paper thoroughly describes on potential of reconnaissance attack reach through automatic tunneling named 6to4 Tunneling. The preference development tools and networking defense mechanism suite, is setup to conduct proposed attack method under 6to4 tunnel testbed environment. As a result, the attacking method is feasible to attempt and 6to4 tunnel showed their influence on the achievement of DoS attack in current internet.

Keywords: *6to4 Tunneling, Dual Stack, Internet Protocol Version 6 (IPv6), Protocol Version 4 (IPv4), Protocol-41*

INTRODUCTION

IPv6 is a new protocol of internet was developed by Internet Engineering Task Force (IETF) to replace the existing protocol (Raicu & Zeadally, 2003). Initially, the deployments of previous researches were to identify constraints that may occur in IPv6. Throughout years, Transition Mechanism (TM) has been inspired in order to ensure a successful integration of IPv6 into an existing network (AlJaafreh et al., 2008; Narayan & Tauch, 2010). As referred to (Waddington & Fangzhe, 2002), TMs are identified into three main categories based on their operation and the way of their implementation: dual stack mechanisms (Durand, 2001; Hirorai & Yoshifuji, 2006), tunneling mechanisms (Vazao et al., 2004; Waddington & Fangzhe, 2002), and translation mechanisms (Grosse & Lakshman, 2003; Kawarasaki et al., 2003). Among of these mechanism, tunneling is widest implemented nowadays.

DOI: 10.4018/jmcmc.2013010101

Since IPv6 in IPv4 tunnel is established between Node_A and Node_B, we may name it as *Tunnel (A,B)* and packet sent through this tunnel can be write as:

$$\textit{Tunnel}\ (A,B) = AB = A{:}[A_4 B_4\ payload_4] \blacktriangleright [A_4 B_4\ payload_4]{:}B \quad (3)$$

An IPv6 packet encapsulated in an IPv4 payload with source and destination IPv6 address Y_6 and X_6 is written as:

$$payload_4 = Y_6 X_6\ payload_6 \quad (4)$$

Then, if (2) is communicate through *Tunnel (A,B)*, we may write as:

$$\text{Tunnel}\ (A,B) = A{:}[A_4 B_4\ \text{payload}_4] \blacktriangleright [A_4 B_4\ \text{payload}_4]{:}B$$
$$\textit{Tunnel}\ (A,B) = A{:}[A_4 B_4\ [Y_6 X_6\ payload_6]] \blacktriangleright [A_4 B_4\ [Y_6 X_6\ payload_6] \quad (5)$$

Thus, this study is using the above interpretation on a real live tunneled network to observe its structure in general.

METHOD

This section describes the development of passive mode reconnaissance attack's model to address security issues of the 6to4 tunnel. As stated before, reconnaissance attack operates in Network layer which seeking active nodes in a same subnet. In this experiment, the implementation is conducted by looking into 6to4 tunneling traffic or specifically on IPv4 protocol type 41 traffic. The major goal is to identify the end nodes of each existing tunnels. The process involved capturing and peeling the network traffic that could obtain the useful information so that easy to commit the further attacks. The important information in this implementation is getting the source and destination of IPv4 addresses.

Refer to Figure 3, this kind of silent attack is through all protocol 41 traffics between node A and node B. Each node on the IPv6 network is communicated with other nodes on Dual Stack network. If each of the traffic flow is interpreted into the aforementioned equation, the structure of the traffics through 6to4 tunnels can be presented as follows.

By considering equation (5), we may write:

YW (Node_Y to Node_W)

$$\textit{Tunnel}(A,B) = A{:}[A_4 B_4\ [[Y_6 W_6\ payload_6]]] \blacktriangleright [A_4 B_4\ [Y_6 W_6\ [payload_6]]]{:}B \quad (6)$$

YX (Node_Y to Node_X)

$$\textit{Tunnel}(A,B) = A{:}[A_4 B_4\ [Y_6 X_6\ [payload_6]]] \blacktriangleright [A_4 B_4\ [Y_6 X_6\ [payload_6]]]{:}B \quad (7)$$

Then, to sight the addresses at ends of tunnel, it can be finding by $(6) \cap (7) = A_4 B_4$ and $payload_6$. Since the purpose of the attack is to find the end of the tunnel node addresses, so $payload_6$ is neglected.

This threat have been developed using free downloaded tool, Scapy because of the ability to permit building, sending, receiving and analyzing packets (Burns *et al.*, 2007). Then, a sequence of schematic flow has been designed as a process of Reconnaissance attack development as in Figure 2. Overall, this development selected only packet types 41 that carry the information about actives 6to4 tunnel end nodes and appear preferred information's into log file.

Here, the details explanation of the process involved is as follows.

Firstly, attacker filtered all traffics were on the IPv6 encapsulation protocol (IPv4 protocol-41):

```
if pkt[IP] and pkt[IP].proto==41
```

Then, the first byte of the payload is a '6' identified in hexadecimal (IPv6 packet):

Figure 2. Flow chart of reconnaissance attack development process

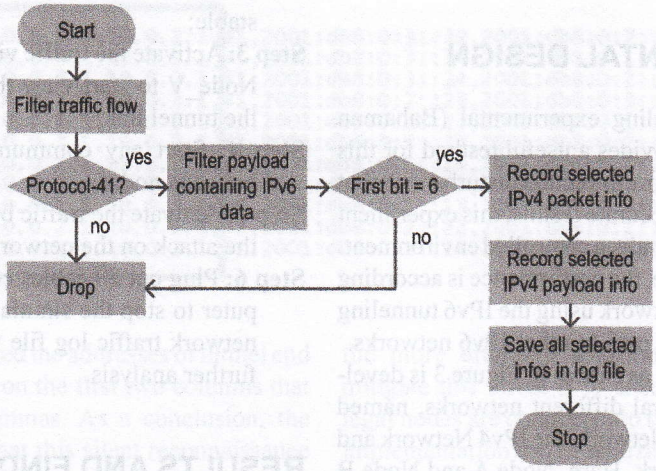
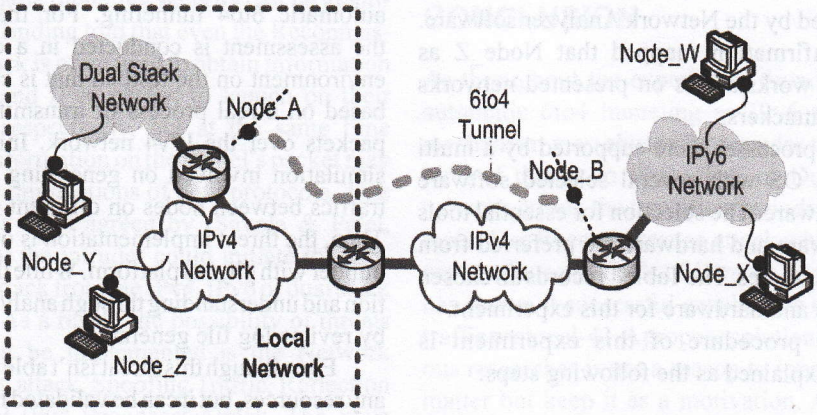


Figure 3. Testbed developed according to the desired environment



if pkt[IP].payload and hexlist(pkt[IP].payload)[0][0] == "6"

Next, record the ip protocol value and the outer source and destination IPv4 address:

```
v4src = str(pkt[IP].src)
v4dst = str(pkt[IP].dst)
v4p = str(pkt[IP].proto)
```

After that, the inner source and destination IPv6 address is taken:

```
v6src = v6tostr(hexlist(pkt[IP].payload)[8:24])
v6dst = v6tostr(hexlist(pkt[IP].payload)[24:40])
```

Lastly, the traffic flow in log file is save as below:

ISBN 978-1-4666-3085-7
90000
9 781466 630857