Home Users Vulnerabilities in Audio/Video Players

R.Jain and M.Papadaki

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Computer security researchers and professionals have a long history of computer vulnerabilities information. Days are gone when information security could be based on one firewall protecting a network from the dangers of external attacks. Today laptops and home computer systems have made information security a daunting task. In the recent years, there is a rapid increase in discovered computer vulnerabilities and home users have become the major target for vulnerability exploitation. Lack of human factor identification, analysis methods and user's unawareness in computer and information security has made the conditions worse. Previous researches have focused on usability aspects of security methods like passwords, smart cards and biometrics. The main purpose of this research is to develop a basic understanding of home user vulnerabilities, issues contributing to computer and information security vulnerabilities and suggest the possible ways of avoiding these vulnerabilities. This research examines how home user vulnerabilities have evolved over the past years, what are the main factors contributing these issues and how users can make their computer safe against those vulnerabilities. The information has been carried out in the form of surveying vulnerability databases and surveying existing research. After analysing the whole results conclusion and recommendations has been drawn.

Keywords

Media Players, Vulnerability, Trends of Vulnerability, Types of Home Users.

1 Introduction

When IBM introduced their first PC, in the beginning of eighties no one thought that 20 years later there would be a PC in every home and they all will be interconnected. During these 20 years several breakthroughs in computer technology has changed the opinion of ordinary people about computers. In the middle of nineties personal computers had become easy enough to use for ordinary people because of new Windows version. The huge amount of home computers and massive internet usage has improved the information flow in various ways. People now have access to the information they need and they can communicate with each other electronically. But there are some problems that need to be addressed. Home users have become administrators of their home computer without having basic knowledge of how to protect their system from increasing threats on the internet. Hackers and attackers launch various attacks on computer systems using internet. They use internet to steal important information, install programs that monitor pattern of surfing without user's knowledge. This makes computer security vulnerable and put information on high risk. (Ulf Frisk 2004)

Traditional sciences and engineering have a long history in the analysis of computer vulnerabilities. There are a few instances of researchers who have attempted to find some regularity in computer vulnerabilities. Same vulnerabilities occur again and again which should be a powerful incentive for the development of vulnerability database that can be used to learn from others' mistakes. The last years have seen a surge in interest for designing and maintaining vulnerability databases. These databases are not being widely published and analyzed because of the fear that it may trigger a great number of intrusions or intrusion attempts by hackers, students or employees. So it becomes essential to examines how home user vulnerabilities have evolved over the past years, what are the main factors contributing these issues and how users can make their computer safe against those vulnerabilities. (Krsul 1997), (Lieungh 2005)

2 Home User Vulnerabilities

As discussed in the previous section, home users have become the main target for the vulnerability exploitation in the recent years. The main reason behind this is users' unawareness and carelessness towards the security and the threats to the security of the computer. Before discussing home user vulnerabilities, this paper discusses the types of users. A users' knowledge is of two types: Syntactic and Semantic. Syntactic knowledge is device dependent and it can be easily forgotten by the users whereas semantic knowledge is well structured, device independent and stable. It is acquired by meaningful learning. Depending on the type of knowledge, users can be categorized as following:

- **Novice Users:** Novice users do not have syntactic knowledge of the system. They only have some semantic knowledge about the system or task they want to perform. They do not have much technical knowledge about the system.

- **Knowledgeable Intermittent Users:** These users have full semantic knowledge about the system and task they want to perform but it's hard for them to maintain the syntactic knowledge of the system. They can use simple menu functions or commands on the system.

- **Frequent Users:** Frequent users have thorough semantic and syntactic knowledge about the computer and its tasks. They can use shortcuts and abbreviations while performing any task on the system. (CERT)

Depending on the types of users following are the vulnerabilities caused by the users which results system or data compromise.

- Not installing antivirus on the system
- Not updating antivirus regularly.
- Not updating patches regularly.
- Use of weak passwords.
- Sharing passwords with friends and relatives.
- Not installing firewalls.

- Unawareness about certain vulnerabilities.
- Not configuring security policies on the system.
- Not taking backups.

Novice users who do not have much technical knowledge do not bother about the system security. It makes the system vulnerable and an open invitation for the attackers to attack. Usually novice users do not install antivirus on the system and do not know what type of password would be safe. They do not know much about the computer vulnerabilities putting the data security at high risk.

Intermittent users have some technical knowledge about the system but they also ignore some of the security rules while using the system. Some users' do not update their system time to time thinking that it can be done later putting the system security on risk. Most of the users do not take backups of their work done. This is also vulnerability in case of system crash or hard disk failure. Some of the users do not patch their system regularly which also makes the system vulnerable.

Frequent users also sometimes make the system vulnerable, as some of the frequent users do not enable firewall on their system. If a user is using a DSL connection for internet then it is very important to enable firewall at both ends: at the router and the system as well. (CERT)

3 Vulnerability Databases

There are many databases for reporting vulnerabilities and the databases chosen for this research are based on:

- Up to date information provided by the database.
- Relevancy and acceptability of the data provided by the database.
- Total number of vulnerabilities reported.
- Reference to the other sources used.

Based on the above facts, databases are chosen for the analysis of the vulnerabilities reported in specified audio/video players. In this chapter the research method used for this research and various vulnerabilities found in the audio/video players is discussed.

Source	URL
CERT	www.cert.org
SecurityFocus	www.securityfocus.com
Secunia	www.secunia.com

Table 1: Vulnerability Databases

Secunia is one of the most trusted vulnerability database and a computer security service provider also. So it is chosen as the major source for this research. Secunia collects vulnerability information from CERT, CVE (Common Vulnerabilities and Exposures), vendors, newsletters and bug reports. Secunia prioritised remediate techniques by considering the severity of the vulnerabilities, threat environment and

commercial use of the vulnerable assets. It gives the complete solution for fixing the vulnerabilities and finding the root cause of the vulnerabilities in order to eliminate its threat completely. Figure 4.1 shows the working procedure for vulnerability management by Secunia. (Secunia)

4 Research Method

The research method used for this research is comparative method of research. Data from the various databases is compared with each other and then the trends in vulnerabilities thus extracted are analysed. The following figure (Figure 1) shows the research method used. This approach is used to study trends of vulnerabilities in the given audio/video players. Data collected from databases like Secunia, SecurityFocus and CERT is compared with each other on the basis of total number of vulnerabilities, their impact on the end users, criticality and patch management. After analysing all the results, this information is used to define vulnerability management and suggestions for safeguards against those vulnerabilities.

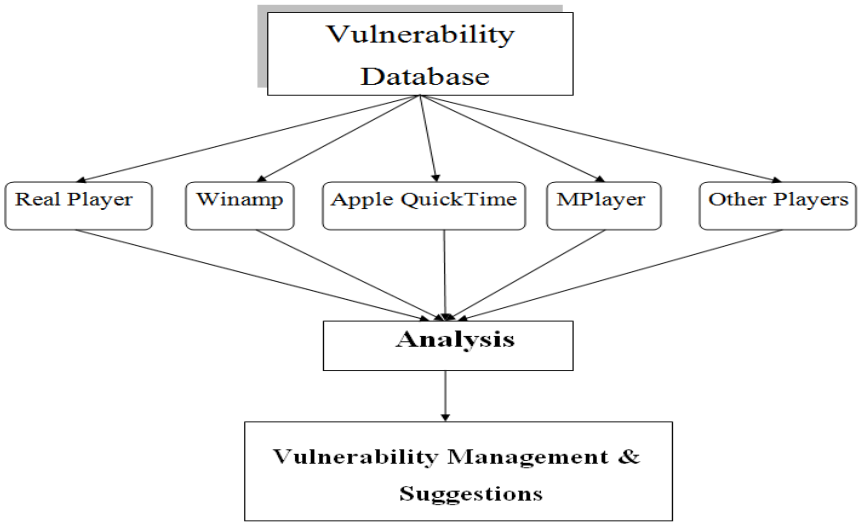

Figure 1: Comparative Research Method

5 RealPlayer

RealPlayer 10.x has been chosen for vulnerability analysis in this research. This has been chosen as it is one of the most widely used media player among home users. Secunia started reporting vulnerabilities in RealPlayer since 2003. Since then Secunia has released 15 advisories till 2007.

Year 2004: In year 2004, number of vulnerabilities reported in this version of RealPlayer is 4 by Secunia. SecurityFocus reported 3 vulnerabilities during this period which shows that the data from Secunia is correct. All of the vulnerabilities reported in that period of time were highly critical. Impact of these vulnerabilities at

the home users includes manipulation of data, cross site scripting and system access.(Secunia; SecurityFocus)

Year 2005: In this year Secunia reported 6 vulnerabilities for this version of RealPlayer. SecurityFocus reported only 7 vulnerabilities during this period of time. 4 of the 6 vulnerabilities reported by Secunia were highly critical. Impact created by these vulnerabilities was system access and manipulation of data on home users' computer by a remote attacker.(Secunia; SecurityFocus)

Year 2006-07: Secunia reported 4 vulnerabilities during this time period while 7 vulnerabilities were reported by SecurityFocus during these years. 1 out of 4 vulnerabilities reported by Secunia was extremely critical which RealPlayer Playlist Handling Buffer Overflow was and rest of the 3 were highly critical vulnerabilities. Impact of these vulnerabilities on home users included full system access from a remote location.(Secunia; SecurityFocus)

6 Winamp

Winamp is also used by a large group of users because of its features. Winamp 5.x has been chosen for vulnerability analysis in this research. Secunia has reported 12 advisories since it started reporting from the year 2003 till 2007 for this version of Winamp.

Year 2004: Secunia reported 3 vulnerabilities during 2003 year for this version of Winamp as there were no vulnerabilities reported in 2003. Two out of three vulnerabilities were extremely critical including Winamp Skin File Arbitrary Code Execution Vulnerability and Winamp "IN CDDA.dll" Buffer Overflow Vulnerability. Remaining vulnerability was highly critical based on its' criticality which was Winamp "in mod.dll" Heap Overflow Vulnerability. Impact of these vulnerabilities was full system access by the remote attacker.(Secunia; SecurityFocus)

Year 2005-06: Secunia reported 6 vulnerabilities during the years 2005-06 for this version of Winamp. One out of six vulnerabilities was extremely critical which Winamp Three Playlist Parsing Buffer Overflow Vulnerability was. Rest of the five vulnerabilities were highly critical. Impact of these vulnerabilities included System Access and DoS (Denial of Service) after exploitation by remote attacker.(Secunia; SecurityFocus)

Year 2007: In 2007 Secunia reported 3 vulnerabilities so far for this version of Winamp. Two out of three vulnerabilities are highly critical and one is moderately critical.. Impact of these vulnerabilities on home users was system access by the remote attacker after the exploitation of these vulnerabilities.(Secunia; SecurityFocus)

7 Apple QuickTime

Apple Quicktime player is the top most used media player among home users. Apple QuickTime 7.x has been analysed in this research to find vulnerability trends. Secunia started reporting vulnerabilities in Apple QuickTime 7.x since 2003. 15 advisories have been reported by Secunia since 2003 till 2007 whereas 18 reported by SecurityFocus.

Year 2004-05: Secunia reported 4 vulnerabilities during the year 2004-05 in this version of Apple QuickTime where as SecurityFocus reported 5 vulnerabilities proving the data from Secunia to be correct. Two out of four vulnerabilities were highly critical including Apple QuickTime "QuickTime.qts" Heap Overflow Vulnerability and Apple QuickTime Multiple Vulnerability. Impact of these vulnerabilities on home users was system access by a remote attacker after exploiting these vulnerabilities.(Secunia; SecurityFocus)

Year 2006: In 2006, Secunia reported 3 vulnerabilities in Apple QuickTime 7.x and SecurityFocus also reported the same number of vulnerabilities. 2 out of 3 vulnerabilities were highly critical including Apple QuickTime Multiple Vulnerability and Apple QuickTime "qtnext" Input Validation Vulnerability. Other was less critical vulnerability. Impact of these vulnerabilities on users was System Access and DoS.(Secunia; SecurityFocus)

Year 2007: Secunia reported 8 vulnerabilities so far for this version of Apple QuickTime during the year 2007. SecurityFocus reported 10 vulnerabilities during the same period for this version of Apple QuickTime proving the data from Secunia to be true. 1 out of 8 vulnerabilities was extremely critical including Apple QuickTime RTSP "Content-Type" Header Buffer Overflow. Remaining 7 vulnerabilities were highly critical. Impact of these vulnerabilities on home users and all other end users could have been System Access and DoS if being exploited by the remote attackers.(Secunia; SecurityFocus)

8 MPlayer

MPlayer 1.x has been analysed for vulnerability trends in this research. Secunia reported 13 advisories for this version of MPlayer since 2003 to 2007.

Year 2003-04: Secunia reported 5 vulnerabilities during the time period between 2003 and 2004 whereas SecurityFocus reported 6 vulnerabilities during the same time period for MPlayer 1.x proving the data from Secunia to be correct. Two out of five vulnerabilities reported by Secunia were highly critical including MPlayer GUI Filename Handling Buffer Overflow Vulnerability and MPlayer Multiple Vulnerability. Impact of these vulnerabilities after its exploitation by a remote attacker includes System Access.(Secunia; SecurityFocus)

Year 2005-06: In these years Secunia reported 5 vulnerabilities for this version of MPlayer. 2 out of 5 vulnerabilities were highly critical and the rest 3 were moderately critical. Highly critical vulnerabilities include MPlayer RTSP and MMST

Streams Buffer Overflow Vulnerability and MPlayer FFmpeg Multiple Buffer Overflow Vulnerability. Impact of these vulnerabilities if being exploited could have been System Access and DoS by the remote attackers.(Secunia; SecurityFocus)

Year 2007: Secunia reported 3 vulnerabilities so far in year 2007 for MPlayer 1.x and SecurityFocus also reported the same number of vulnerabilities proving the data from Secunia to be correct. Two out of three vulnerabilities are highly critical and one is moderately critical. Impact of these vulnerabilities after being exploited by remote attackers could have been System Access and DoS putting the home users' data on high risk.(Secunia; SecurityFocus)

9 Trend Analysis

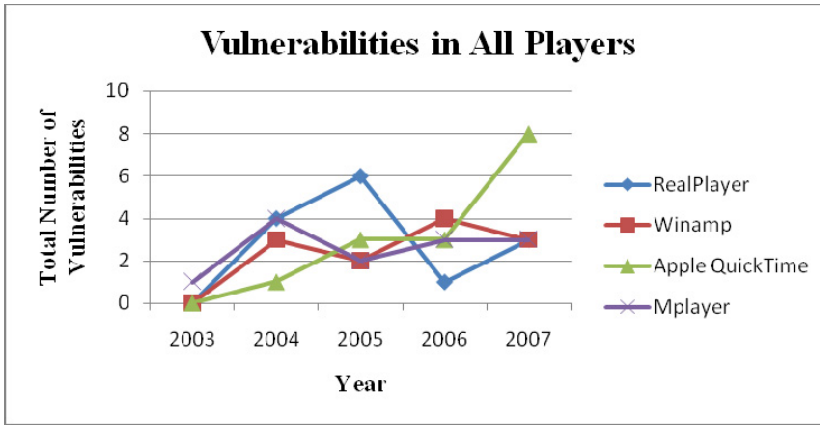

Figure 2: Trends of Vulnerability in All players. (Secunia)

Figure 2 analyses the trends of vulnerability in all the media players discussed and it is clear that the number of vulnerabilities is increasing year per year. With increase of window of exposure and patch release time, the threat to home users is also increasing. As can be seen, vulnerabilities are rapidly increasing in case of Apple QuickTime as compared to other players. This issue should be considered more seriously as it is the most commonly used media player among the home users across the globe. Number of vulnerabilities is increasing at an inconsistent rate in case of RealPlayer. Winamp and MPlayer are under minimal threat of vulnerability exploitation as compared to other two media players. (Secunia)

Figure 3 illustrates the trends of vulnerability in all the players based on the criticality of the vulnerabilities. This graph is generated on the basis of data collected from Secunia for every audio/video player during the time period between 2003 and 2007. The graph indicates the inconsistent increase of extremely and highly critical vulnerabilities in all the media players per year. This shows the huge impact of these vulnerabilities after exploitation. Number of extreme and highly critical vulnerabilities in Apple QuickTime has been increased consistently per year. Apple QuickTime is the most common and popular product used across the globe and increase of seer vulnerabilities has put home users under the threat of malicious

attacks. It is clear that the rate of vulnerabilities has increased with the increase of its popularity. RealPlayer is at second place in case of severing vulnerabilities. RealPlayer is also most common product among home users and the graph shows that the rate of sever vulnerabilities is inconsistent per year. There are not much significant vulnerabilities in Winamp and MPlayer though these are also commonly used by the home users. So it is clear that Apple QuickTime is the most vulnerable media player under the threat of malicious attacks.

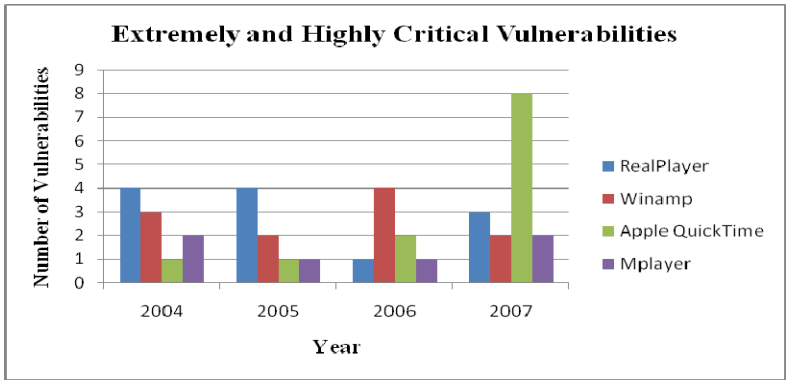

Figure 3: Trends of Vulnerability based on Criticality. (Secunia)

10 Conclusion and Recommendations

The main objective of this research was to obtain the understanding of home user vulnerabilities and its evolution. According to the results media players are becoming more popular among attackers for vulnerability exploitations. Though there is not much vulnerability founded in the recent years in media players as compared to other applications like web browsers yet it is clear that the trends in media players are increasing. With the increase of these trends, window of exposure is also increasing giving the malicious attackers more time for attacks and exploitations. It's becoming difficult for the vendors to release the patch as soon as the vulnerability is publically exposed. It is of no doubt that home users have become the primary target for the attackers to exploit vulnerabilities. Due to lack of exact information from various vulnerability databases this research did not meet up to its standards and this area still needs to be carried on. Following are the recommendations for the home users to safeguard against the vulnerabilities analysed in this research:

- Always apply current patches to the media players and be updated.
- Always review default installation settings while installing the media players.
- Do not install any add on from untrusted sites and other sources.

- All the media players provide features for browsing music online, so configure the media player in order to prevent unintentional installations from internet.

- Install the media player which you need, do not just install every media player.

- Windows Media Player is analysed to be the most secure media player, so it is strongly recommended to use Windows media Player rather than any other if you are using Microsoft Windows operating system.

- Always use Antivirus and Spywares to block unwanted malicious media files.

- Always install and configure firewall in order to prevent remote attacks.

- Do not use unsecure wireless connections as it makes things easier for an attacker to attack on your system remotely.

- Always deploy security policies on your system in order to avoid unauthorized system access.

- Despite of these vulnerabilities, it is also recommended to use large and complex passwords for the systems.

- Always review security bulletins from various organizations and be updated about the vulnerability information.

- If you are a non technical user then it is recommended to use your operating systems default help option as much as you can in order to gain knowledge about the security of your system.

- Do not give your details to any untrusted site as it can be a spoof page.

- Always check the padlock in the bottom of the web browser before shopping online.

11 References

CERT "Home Computer Security". http://www.cert.org/homeusers/HomeComputerSecurity/. Accessed on May 16, 2007

CERT "Home Network Security". http://www.cert.org/tech_tips/home_networks.html#III. Accessed on May 25, 2007.

Krsul, I. (1997). "Computer Vulnerability Analysis Thesis Proposal". http://ftp.cerias.purdue.edu/pub/papers/ivan-krsul/krsul-thesis-proposal.pdf. Accessed on May 13, 2007.

Lieungh, S. (2005). "Rate Vulnerability Reducing Measures for Home Offices Based on a Cost Effectiveness Analysis". http://hig100.hig.no/imt/file.php?id=623. Accessed on May 13, 2007.

Secunia. "MPlayer". http://secunia.com/search/?search=Mplayer&w=0. Accessed on November 10, 2007.

Secunia. "QuickTime". http://secunia.com/search/?search=quicktime&w=0. Accessed on November 13, 2007.

Secunia. "Real Player". http://secunia.com/search/?search=Real+Player. Accessed on November 20, 2007.

Secunia. "Winamp". http://secunia.com/search/?search=winamp. Accessed on November 18, 2007.

SecurityFocus. "SecurityFocus Introduction". http://www.securityfocus.com/about. Accessed on May October 23, 2007.

SecurityFocus "Vulnerabilities". http://www.securityfocus.com/bid. Accessed on November 21, 2007.

Ulf Frisk, S. D. (2004). "The State of Home Computer Security". www.diva-portal.org/diva/getDocument?urn_nbn_se_liu_diva-2584-1_fulltext.pdf. Accessed May 11, 2007.