



UNIVERSITI SAINS MALAYSIA

PEJABAT PENGURUSAN DAN KREATIVITI PENYELIDIKAN
RESEARCH CREATIVITY AND MANAGEMENT OFFICE

MEMORANDUM

Kepada :

Prof. Madya Sureswaran Ramadass
Pengarah
Pusat Kecemerlangan IPv6

Daripada:

Penolong Pegawai Tadbir Kanan

Ruj. Kami : FPP 2005/379 [P2430]

Tarikh : 18 Disember 2007

Laporan Akhir Projek Penyelidikan USM Jangka Pendek

Tajuk Projek : "Big Picture Codec for Multimedia Conferencing System"

No. Akaun : 304/PKOMP/636075

Dengan segala hormatnya perkara di atas dirujuk.

Terlebih dahulu saya ucapkan terima kasih di atas laporan akhir untuk projek penyelidikan USM jangka pendek seperti tajuk di atas. Bersama-sama ini disampaikan komen penilaian daripada Pemangku Dekan Penyelidikan Pelantar Teknologi Maklumat & Komunikasi untuk perhatian tuan.

Seterusnya walaupun projek ini telah selesai, Jabatan Bendahari telah dinasihatkan untuk menangguhkan penutupan akaun projek kepada **31 Disember 2007**. Tempoh ini diberi untuk membolehkan penjelasan semua urusan tuntutan dan bayaran yang telah dikomitkan di dalam tempoh projek. Walaubagaimanapun, tuan dinasihatkan supaya tidak mengeluarkan borang-borang pesanan baru di dalam tempoh ini.

Selanjutnya sila ambil perhatian terhadap perkara-perkara berikut sekiranya berkaitan :

- (i) semua penerbitan harus merakamkan penghargaan kepada geran penyelidikan jangka pendek dan tuan dipohon mengemukakan satu salinan ke pejabat RCMO; dan
- (ii) pihak kami akan mengagihkan semula peralatan yang telah dibeli menggunakan peruntukan geran ini seandainya terdapat penyelidik lain yang memerlukan peralatan tersebut.

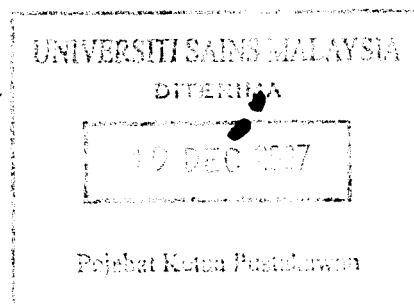
Harap maklum, projek ini dianggap telah selesai dengan jayanya.

Sekian, terima kasih.

"BERKHIDMAT UNTUK NEGARA"

"Bersaing Di Peringkat Dunia: Komitmen Kita"

CHE MERAH ISMAIL



Bhg. Rujukan/MIHA/
SRMS

s.k. Y. Bhg Dato' Profesor Muhammad Idris Saleh
Timbalan Naib Canselor
[Penyelidikan & Inovasi]

Prof. Madya Bahari Belaton
Pemangku Dekan Penyelidikan
Pelantar Teknologi Maklumat & Komunikasi
Pejabat Pelantar Penyelidikan

Rohani Bakar
Pegawai Sains
Pelantar Teknologi Maklumat & Komunikasi
Pejabat Pelantar Penyelidikan

Puan Sofiah Hashim
Ketua Pustakawan
Perpustakaan Hamzah Sendut 1

Puan Ansuya a/p Narhari
Penolong Bendahari
Unit Kumpulan Wang Penyelidikan
Jabatan Bendahari

Disampaikan satu salinan
laporan akhir projek untuk
simpanan Perpustakaan

Sila ambil tindakan menutup
akaun projek pada **31 Disember 2007**
dan sila kemukakan satu salinan
keuangan terakhir ke pejabat
(RCMO)

LAPORAN AKHIR PROJEK PENYELIDIKAN JANGKA PENDEK

FINAL REPORT OF SHORT TERM RESEARCH PROJECT

Sila kemukakan laporan akhir ini melalui Jawatankuasa Penyelidikan di Pusat Pengajian dan Dekan/Pengarah/Ketua Jabatan kepada Pejabat Pelantar Penyelidikan

1. Nama Ketua Penyelidik: Dr. Sureswaran Ramadass <i>Name of Research Leader</i>				
<input checked="" type="checkbox"/> Profesor Madya/ Assoc. Prof. <input type="checkbox"/> Dr./ Dr. <input type="checkbox"/> Encik/Puan/Cik Mr/Mrs/Ms				
2. Pusat Tanggungjawab (PTJ): National Advanced IPv6 Centre (NAv6) <i>School/Department</i>				
3. Nama Penyelidik Bersama: <i>Name of Co-Researcher</i>				
4. Tajuk Projek: <i>Title of Project</i> <u>Big Picture Codec For Multimedia Conferencing System</u>				
5. Ringkasan Penilaian/Summary of Assessment:				
	Tidak Mencukupi Inadequate		Boleh Diterima Acceptable	Sangat Baik Very Good
	1	2	3	4 5
i) Pencapaian objektif projek: <i>Achievement of project objectives</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> X
ii) Kualiti output: <i>Quality of outputs</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> X
iii) Kualiti impak: <i>Quality of impacts</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> X
iv) Pemindahan teknologi/potensi pengkomersialan: <i>Technology transfer/commercialization potential</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> X
v) Kualiti dan usahasama : <i>Quality and intensity of collaboration</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> X
vi) Penilaian kepentingan secara keseluruhan: <i>Overall assessment of benefits</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> X

6. Abstrak Penyelidikan

(Perlu disediakan di antara 100 - 200 perkataan di dalam **Bahasa Malaysia dan juga Bahasa Inggeris**. Abstrak ini akan dimuatkan dalam Laporan Tahunan Bahagian Penyelidikan & Inovasi sebagai satu cara untuk menyampaikan dapatan projek tuan/puan kepada pihak Universiti & masyarakat luar).

Abstract of Research

(An abstract of between 100 and 200 words must be prepared in Bahasa Malaysia and in English).

This abstract will be included in the Annual Report of the Research and Innovation Section at a later date as a means of presenting the project findings of the researcher/s to the University and the community at large)

A video codec is a device or software module that enables the use of compression for digital video.

Historically, video was stored as an analog signal on magnetic tape. Around the time when the compact disc entered the market as a digital-format replacement for analog audio, it became feasible to also begin storing and using video in digital format, transmitting compressed video and a variety of such technologies began to emerge. In this research, we worked on higher quality and high resolution video at low bit rate for video conferencing.

Sebuah *video codec* adalah sebuah alat atau modul perisian yang membolehkan penggunaan mampatan untuk video digital. Dari segi sejarah, rakaman yang telah disimpan dalam video adalah sebagai satu isyarat analog atas pita bermagnet. Dalam waktu yang sama, apabila cakera padat memasuki pasaran sebagai satu bentuk digital bagi menggantikan audio analog. Ianya menjadi munasabah untuk membekalkan dan menggunakan video bentuk angka, memancarkan mampatan video serta satu kepelbagaian teknologi seumpamanya dimulakan. Dalam penyelidikan ini, kami menggunakan video persidangan yang berkualiti tinggi dan video beresolusi tinggi pada kadar yang agak rendah.

7. Sila sediakan laporan teknikal lengkap yang menerangkan keseluruhan projek ini.

[Sila gunakan kertas berasingan]

Applicant are required to prepare a Comprehensive Technical Report explaining the project.

(This report must be appended separately) **Rujuk Lampiran**

Senaraikan kata kunci yang mencerminkan penyelidikan anda:

List the key words that reflects your research:

<u>Bahasa Malaysia</u>	<u>Bahasa Inggeris</u>
Transmisi video berkualiti tinggi	High quality video transmission
Sidang video	Video conferencing
Video yang besar berkualiti tinggi pada kadar agak rendah	High quality big video at low bit rate

8. Output dan Faedah Projek

Output and Benefits of Project

(a) * **Penerbitan Jurnal**

Publication of Journals

(Sila nyatakan jenis, tajuk, pengarang/editor, tahun terbitan dan di mana telah diterbit/diserahkan)

(State type, title, author/editor, publication year and where it has been published/submitted)

"A Framework For Detecting Bluetooth Mobile Worms" Proceedings 2007 14th IEEE International Conference on Telecommunications, Penang, Malaysia May 15-17, 2007. Usman Sarwar, Sureswaran Ramadass and Rahmat Budiarto, USM.

- (b) **Faedah-faedah lain seperti perkembangan produk, pengkomersialan produk/pendaftaran paten atau impak kepada dasar dan masyarakat.**
State other benefits such as product development, product commercialisation/patent registration or impact on source and society.

Research product is integrated with commercialized multimedia conferencing system version 6. Potential filling of patents will be possible as well in the future.

* Sila berikan salinan/Kindly provide copies

- (c) **Latihan Sumber Manusia**
Training in Human Resources

Graduates Students

2

(Perincikan nama, ijazah dan status)

(Provide names, degrees and status)

i) Pelajar Falsafah : Manjour (PHD) in progress

ii) Pelajar Sarjana: Usman Sarwar (Masters Degree) in progress

ii) Lain-lain: Final year undergraduate students (2)

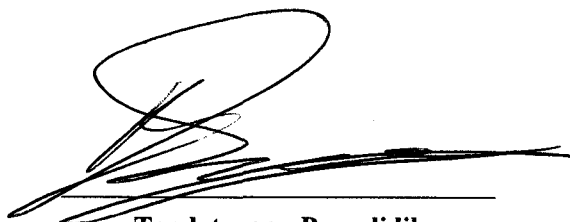
Others

Industrial trainees (2)

9. Peralatan yang Telah Dibeli:

Equipment that has been purchased

None



Tandatangan Penyelidik
Signature of Researcher

7/9/2007

Tarikh
Date

Komen Jawatankuasa Penyelidikan Pusat Pengajian/Pusat
Comments by the Research Committees of Schools/Centres

The project was concluded with a new version
of codec for the use of digital video compression.
Four students were trained with the codec technology
under this grant.

Assoc. Prof. Dr. Azman Samsudin
Deputy Dean
Postgraduate Studies and Research
School of Computer Sciences
Universiti Sains Malaysia
11800 USM Penang


TANDATANGAN PENERUSI
JAWATANKUASA PENYELIDIKAN
PUSAT PENGAJIAN/PUSAT
Signature of Chairman
[Research Committee of School/Centre]

Oct 1, 2007.
Tarikh
Date

A Framework For Detecting Bluetooth Mobile Worms

Usman Sarwar, Sureswaran Ramadass and Rahmat Budiarto, *Universiti Sains Malaysia*

Abstract — Bluetooth is an industrial standard for wireless specification for wireless personal area network (PAN). In recent years, Bluetooth technology has become a standard in mobile devices such as cell phones, smart phones and personal digital assistant (PDA) for short range communication. There is a new era of worm attack on these mobile devices through Bluetooth. Few years back worms on cell phones and mobile devices were more like science fiction but these days it is more than a reality. In this paper, our main concern is to detect and prevent malicious propagated code over the Bluetooth network to reduce the chances of epidemic. We propose a framework for detecting Bluetooth worms on public locations such as airports and sports arenas.

Index Terms— Worms, Bluetooth worms, Bluetooth worm detection system, Cabir

I. INTRODUCTION

A worm is a self replicating program which does not need to be part of other programs to propagate and is designed to exploit the vulnerabilities of the computers and policy flaws. In addition to replicating itself, worms may be designed to do various tasks such as deleting files on the host system, send documents or itself for spreading by emails and more recently worms have multi-headed and carry other executables as their payloads. Worms can slow down the network traffic because of its reproduction.

A Bluetooth is radio frequency (RF) technology utilizing the unlicensed 2.4 Ghz industrial, scientific and medical (ISM) band. Bluetooth uses short range radio links, intended to replace the cables connecting portable and/or fixed electronic devices [2]. Its key features are robustness, low complexity, low power and low cost. It is designed to work in noisy frequency environments and it has fast acknowledgement and frequency hopping schemes to make a link robust. There are various applications for Bluetooth which includes PC and peripheral networking, hidden computing and data synchronization such as for address book, synchronization.

Recently mobile devices like cell phones and PDA are the new targeted platform for worms; using Bluetooth and multimedia messaging service (MMS) as their medium of propagation and distribution although few years back, worms and viruses for these types of devices seemed more like science fiction now it is a hard fact. People are not aware that viruses and worms do exist on mobile devices and they use multiple ways like Bluetooth and MMS as a medium of

proliferation. Mobile users may use Bluetooth for multiple purposes like transferring of data (for example, Pictures) and network gaming; in doing so the worms from the infected device can infect the non-infected device with worms like cabir.

Malicious code or Worms on the mobile device has somehow the same characteristics of the other worms but with the exception of limited processing power and resources of mobile devices and specifically utilize the features and functionality of these devices like MMS. Although with limited resources these malicious codes are still destructive and will be communal sooner or later. Until now these worms show different behavior and give deficit to the device user for instance crashing the phone, high phone bills, stealing personal information etc.

As the evolution from current generation of cell phones to next generation phones with more capabilities is currently undergoing there is a good possibility of getting higher epidemics in the future. A study released by McAfee Avert labs declares "The number of malicious software programs created for mobile devices is expected to reach 726 by the end of 2006, up from an estimated 226 at the end of 2005"[16]. Another survey conducted by Finnish company F-Secure stated in 2005 "Symbian malware is the vast majority in all mobile malware, but in our opinion this is not because Symbian would be any more insecure compared to other mobile platforms. The large number just shows how popular Symbian devices are, and thus they are the most interesting target for malware authors" [5].

II-AN OVERVIEW OF BLUETOOTH WORMS

Worms using mobile devices have the same characteristics of the other network worms but with the limitation of mobile device processing power and utilization of special features. To advocate our proposed framework, we need to discuss prevalent Bluetooth worms hence we talk about two pioneers of worms on mobile devices SymbOS/Cabir and Commwarrior

A. Symbian Cabir worm

Cabir worm signaled the dawn of a new era of malicious code on the limited computation power devices like phones and PDA. Cabir is considered to be the first worm infection on

mobile devices and targeted the Symbian OS. The worm was first discovered by Symantec on 14 June 2004.

"The worm's code is compatible with mobile phones using ARM series processors with Symbian operating system such as Nokia 60 series. Normally the Bluetooth connection is off on these devices but as the users exchange data such as images and some little programs between their devices, and in doing so they open up the Bluetooth communication channel to Cabir-like worms as well" [10].

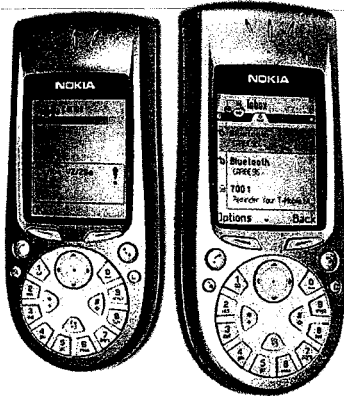


Figure 1: Infection of Cabir worm

Cabir replicates over bluetooth connections and arrives in phone messaging inbox as caribe.sis file which contains the worm. When the user clicks the caribe.sis and chooses to install the Caribe.sis file the worm activates and starts looking for new devices to infect over Bluetooth. As the infected device finds another Bluetooth device it will start sending infected SIS files to the target device. Cabir worm can infect only Symbian mobile devices that support bluetooth, and are in discoverable mode. Setting your phone into non-discoverable (hidden) Bluetooth mode will protect your phone from Cabir worm. But once the phone is infected it will try to infect other systems even as the user tries to disable bluetooth from system settings. [10].

Cabir worm uses three phases to spread. In the first phase it searches for Bluetooth enabled devices and connects to the first device found, even if it is a printer or mouse. In the second phase it sends the caribe.sis file to the device. And third stage disconnects from the device. The worm will restart the first stage again and repeat all the phases on the same device while it is allowed. Phase one dramatically reduces the battery power of the device but if Bluetooth is disabled, the worm will not turn it on and hence will not be spread.

There are various variants of this worm which may exploit the devices differently.

B. Symbian Commwarrior

Commwarrior is another mobile worm which propagates using Bluetooth and MMS. It was first discovered in March 2005. It shows the capabilities of mass mailing itself by using MMS. It targets the Symbian Series 60 smart phones and it propagates randomly named .sis files.

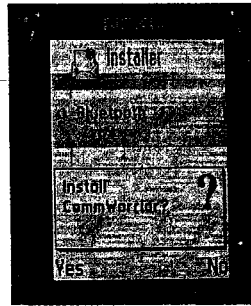


Figure 2: Arrival of worm by Bluetooth

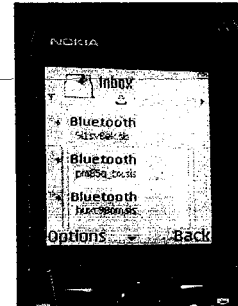


Figure 3: After infection

The replication approach of this worm is very interesting as it uses different time frames for infection. During the normal user waking hours i.e. 8am to 11:59pm it uses Bluetooth to spread itself as there will be good possibility of other Bluetooth devices within its range. During the normal users sleeping hours which are normally 12:00am to 6:59 am; it uses the phonebook and sends itself by attaching with MMS. It sends MMS after every 10 seconds. The selection of phone number is done by enumerating every contact and looking for mobile numbers which means that land numbers are ignored. The purpose of this procedure is to maximize the propagation of infection to compatible mobile devices. Then from 7:00am to 7:59am it cleans up all the sent MMSes carefully as well as message log afterwards. On the 14th day of every month, worm's payloads activate and reboot the phone in silent mode.

III - RELATED WORK

F-Secure a security company, are the pioneers who did research on mobile-based Bluetooth worms. F-Secure mobile anti virus is a host based worm detection system. Their software application must be installed on the smart phone or PDA to secure the device. As there are different software and hardware platforms available for mobile devices, so they have different versions of applications which ranges from Symbian-based operating system to windows mobile operating system.[13]

Symantec mobile security is another product for symbian series 60 and 80 platforms, including selected models from nokia and Panasonic. This is also a host based detection application. It has a built in firewall for inbound and outbound LAN/WAN communication. It scans for malicious code in SMS, EMS, MMS, HTTP files and email files. [18]

IV- PROBLEM STATEMENT

As we have seen to prevent the device from getting infected it must have host based application software like anti virus which can detect or prevent infection of malware on these mobile devices. Until now most of the work has been done to secure these devices by applications like anti virus software [12] [13] which uses lesser resources because of the limited computation power and capabilities of these devices. They also have the limitation of developed for different platforms.

There is a problem with the current approach, the software must be installed on the device else it will be infected. Moreover the antivirus heuristics must be updated to protect the device.

As technology advances, there will be a possibility of more advanced worms which may create havoc in the usage of mobile devices. Till now, Cabir and Commwarrior worms give us the initial perception of the situation.

If any of the devices does not have the antivirus software, and if it had gotten infected; it will infect many devices within its range. Furthermore there is no means of informing the device owner about the infection. As there is illiteracy among common mobile users about the malicious code, the infection may become severe. Especially when we consider public locations for instance airports, sports arenas, shopping malls. Hence, it can create local and global epidemic as most of the people are not aware of this hazard especially when the device owner travels.

Our proposed system is platform independent as we are developing a Bluetooth network based worm detection system. We will explain the framework in section V.

V. THE PROPOSED FRAMEWORK

We propose a framework for detecting worms on Bluetooth network which we call Bluetooth Network Worm Detection System (BNWDS). It is a defensive system to detect worms or worm attack on the Bluetooth network.

The framework has the following objectives:

1. To detect the worms from the Bluetooth enabled infected mobile devices on PAN level.
2. To stop local epidemic of Bluetooth worms by deploying the system at public locations like sports arenas, hospitals.
3. To stop global epidemic by deploying our framework at airports.

The purpose of the proposed system is to detect worms in Bluetooth networks at public places where there is a good possibility of worms spreading. The system will be flexible enough to be deployed at smaller or larger location.

There are five major entities in our system sensors or sensor nodes, core system, worm heuristics, alarming units and remote heuristics services system as illustrated in figure 4.

The sensors or sensor nodes are used for sniffing Bluetooth packets from piconets or PAN. There can be more than one sensor in our system depending on the required secure coverage area. Each sensor node will cover range depending on Bluetooth power class. Here we are using power class 2 which covers 10 meters or 30 feet range. Class 1 which covers 100 meters can also be used. The sensor nodes will be connected with the core system. All the sensors will have their own unique addresses which will be used by the core system to distinguish the location of the attack. Sensor nodes will sniff the packet and send it to the core system for processing.

The core system is basically an x86 based workstation which has our BNWDS engine running. Sniffed packets are sent by sensor(s) to the core system for analysis and processing. The analysis part will analyze the Bluetooth packet and will authenticate if the packet is from devices like cell phones and PDAs not from devices like printers. After authentication, the packets are moved to detection engines. The core software system consists of a smart engine that utilizes both misuse detection and anomaly detection respectively for better detection and lower false alarm. The sub-core smart engine that handles the matching of the packets data will match the data using a fast algorithm and if any malicious data is detected on the network. An alarm will be activated on the alarming display unit. The second sub-core engine will monitor the ambiguous activities on the network. We state different levels and rules of anomalies into the system. If the ambiguity level found on the network is high; the system will raise an alarm and a message will be sent to the alarming display unit.

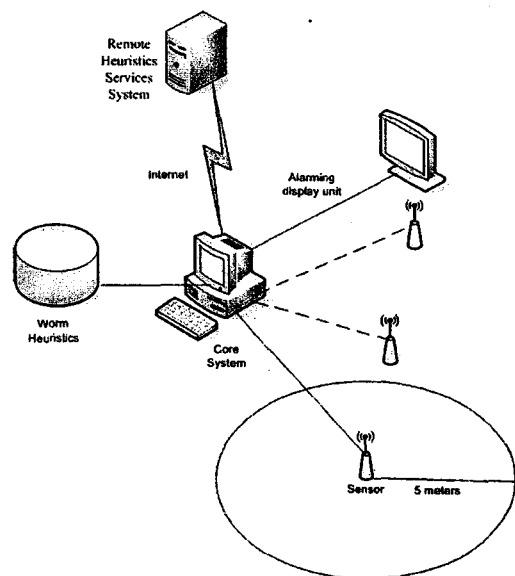


Figure 4: Bluetooth Network Worm Detection System [BNWDS]

The alarming display unit is the vital entity to alert Bluetooth device users about worm propagation in their surrounding area. A message will be displayed and there will be also a vocal announcement to alert users. Alerted display message will advice the Bluetooth device users to turn off their Bluetooth or check their device for worm infection.

Remote heuristics services system use RHS is a web service running on a remote server. RHS will maintain the latest Bluetooth worm signatures in its heuristics. These signatures will be updated by the Bluetooth worm analyst. All core systems will connect with remote heuristics services system periodically through HTTPS to get the latest worm information. RHS will also be responsible to update rules and levels of the BNWDP anomalies engine. Sub-core anomaly engine can also send information about the high ambiguities found on the network to the remote heuristics services. This vital information can provide data to the analysts to investigate those anomalies on the networks.

In short, the proposed system works as follows, whenever a user with an infected device comes within the range of BNWDS sensors, the packets will be captured and sent to the core system for analysis. After the authentication of packet type; the matching sub-core system of the smart engine will analyze the packet and if any malicious data found, it will call the alarm to notify the users. Subsequently, anomaly sub-core will also analyze the network in parallel to detect unknown malicious attacks.

As the objective of our propose framework is to detect the propagation and epidemic of Bluetooth malware from mobile devices. We will discuss two models to deploy our system and effectively stop the Bluetooth worm propagation.

Our framework is designed to stop the epidemic at the public places to control the havoc done by the Bluetooth worms.

Simple Modeling of global propagation as an example

The first solution is to deploy the sensors at the entrances of public areas like entrances and lounges of airports as there is a high probability of worm propagation by infected device. Deploying our system at these locations will allow us to control the epidemic at the global level.

Hence for detection of global epidemic we model it at the airport. At the entrances of airport we arranged sensor S1 and sensor S2 i.e S(S1, S2). Each Sensor has the range of 10 meters. Any passengers with the device D1 or D2 entering into the inspection area of S1 or S2, it will be scrutinized. As passenger with the infected device ID1 will come into the inspection zone of S1. The BNWDS will detect the infectious device and will send the alert. Figure 5 illustrates the simple model. Afterwards the Infected device will be put in a quarantine area where it will be disinfected. If the infection is

new and detected by the sub-core anomaly engine; the information will be sent to the RHS.

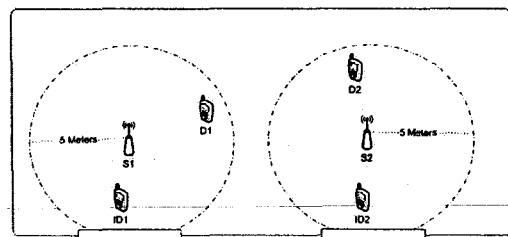


Figure 5 Entrance of airport.

Simple modeling of local epidemic as an example

To control local epidemics, we propose the framework to be deployed at public locations such as sports arenas and shopping malls. The reason behind deploying at these sites is due to detection at early local epidemic and stop at that location.

We did a simple model of detecting worms in sports arenas. We arranged multiple sensors S (S1, S2, ..., S8) in the area. Each Sensor has the range of 10 meters. All the devices D (D1, D2,..., D10) will be within the range of inspection zone. Whenever any infected device ID (ID1, ID2) will be detected; the users will be notified to secure their device which will make the epidemic slower or totally controlled. Figure 6 illustrates the above solution.

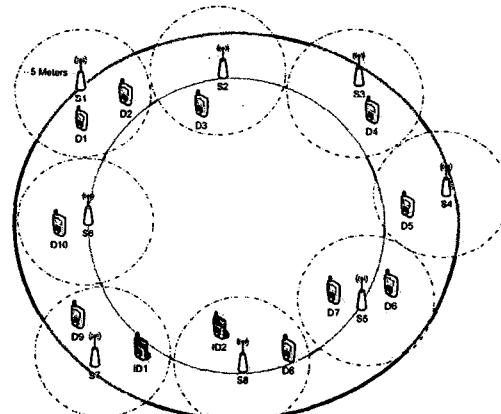


Figure 6, System deployment for Sports arenas.

VI. CONCLUSION

Hence we have presented a framework and also discussed different scenarios where it can detect and solve the worm spreading epidemic. In the future, there will be higher probability of smarter Bluetooth worms; and their propagation and infection. Our Framework will be effective to stop and control the epidemic of Bluetooth worms

VII. FUTURE WORK

In the future, we want to implement the proposed framework and also want to include worm prevention system.

VIII. ACKNOWLEDGEMENT

We would like to express our gratitude to 'Big picture grant for multimedia conferencing system' to support us.

REFERENCES

- [1] Zaruba, G.V., Chlamtac, I. Accelerating Bluetooth inquiry for personal area networks.
- [2] Specification of Bluetooth system version 1.2, 05 NOVEMBER 2003
- [3] Bluetooth 2000: To enable the star generation, Cahners In-Stat group, MM00-09BW, June 2000
- [4] S. Krco, "Bluetooth based wireless sensor networks implementation issues and solutions," 10th Telecommunications forum (TELEFOR2002) NOV.2002
- [5] Nicholas Weaver (UC Berkeley), Vern Paxson (ICSI), Stuart Staniford (Silicon defense), Robert Cunningham (MIT Lincoln Laboratory). *A taxonomy of computer worms*.
- [6] F-secure <http://www.f-secure.com>
- [7] Symantec Corp. <http://www.symantec.com>
- [8] Peter Szor. The Art of Computer Virus Research and Defense. Published by Addison Wesley Professional.
- [9] Number of mobile malware close to 100 now by F-Secure http://www.f-secure.com/wireless/news/items/news_2005092800.shtml
- [10] F-Secure Virus Descriptions : Cabir. <http://www.f-secure.com/v-descs/cabir.shtml>
- [11] Pravin Bhagwat, Reefedge Inc. Bluetooth: Technology for short range wireless apps.
- [12] Symantec anti virus for hand held, http://www.symantec.com/home_homeoffice/products/virus_protection/savhh/index.html
- [13] F-Secure Mobile Anti-Virus, <http://www.f-secure.com/wireless/>
- [14] Mobile malware to triple in 2006, <http://news.zdnet.co.uk/internet/0,39020369,39242892,00.htm>
- [15] Virus analysis of Commwarrior by Symantec
- [16] Dawn Kawamoto. 2006: Year of the mobile malware. http://news.com.com/2006+Year+of+the+mobile+malware/2100-7349_3-6001651.html
- [17] Guanhua Yan and Stephan Eidenbenz. Bluetooth Worms Models, Dynamics, and Defense Implications
- [18] Symantec mobile security. http://www.symantec.com/en/ca/small_business/products/overview.jsp?pcid=is&pvid=sms40symb
- [19] Jarno Niemela F-secure. F-Secure Virus Descriptions : Cabir. <http://www.f-secure.com/v-descs/cabir.shtml>
- [20] Frederic Perriot, Peter Ferrie and Eric Chien. Symantec security response. Symbian OS Commwarrior,

Technical Report for Big Picture Codec for Multimedia Conferencing System

1.0 Synopsis:

A video codec is a device or software module that enables the use of compression for digital video. Historically, video was stored as an analog signal on magnetic tape. Around the time when the compact disc entered the market as a digital-format replacement for analog audio, it became feasible to also begin storing and using video in digital format, transmitting compressed video and a variety of such technologies began to emerge. In this research, we worked on higher quality and high resolution video for video conferencing.

1.1 Objective:

The objective of this research is to achieve high quality and high resolution video transmission (big picture) at a lower bit rates with software compression and decompression to use it with video conferencing system. Normally video conferencing uses 320x240 or 352x288 pixels video resolution. In our research, we are using 640x480 pixels frame size for high resolution video transmission which gives us advantages of high quality visuals as well as compatibility with TVs. Mostly televisions doesn't support resolution higher than this.

*not really
clear at all.*

1.2 Discussion

The objective of this research was to do extensive study on suitable video codec for higher resolution video transmission for video conferencing.

1.2.1 Video Codecs Evaluation

Video compression refers to reducing the quantity of data used to represent video content without excessively reducing the quality of the picture. It also reduces the size of storage and transmission of multimedia content. Compressed video can effectively reduce the bandwidth required to transmit digital video via terrestrial broadcast, via cable, or via satellite services.

For current research, we evaluated different video codecs to be used for our objective. Following are the video codecs.

- 1- VP6
- 2- VP7
- 3- H.264
- 4- X.264
- 5- Divx 5
- 6- Xvid
- 7- Theora
- 8- Mpeg 4 v3

The above used video codecs performed well in initial tests but later on we found out that most of the codecs were not suitable for our requirements. For instance, H.264 is a high quality video codec but requires high CPU. In the end we preferred to use Mpeg 4 v3 which has high quality with utilization of low CPU.

1.2.1.1 Mpeg 4 v3

MPEG-4 is a standard developed for the delivery of interactive multimedia across networks. The underlying intention of the MPEG-4 (ISO 14496) standard is to provide an audio and video compression scheme suitable for video conferencing at data rates less than 64 kbps. It is an open standard. Another important MPEG-4 feature is flexible, highly interactive access to and manipulation of audio-visual data by the end-users. The video component of MPEG-4 is very similar to H.263. It is optimized for delivery of video at Internet data rates. Microsoft uses a MPEG-4 based codec called Microsoft MPEG-4 Video codec v3 in its Windows Media streaming solution [16] and the Internet Streaming Media Alliance has created a more standard approach. It has good image quality at low data rates. It uses Discrete Cosine Transform (DCT) with Motion Prediction algorithms.

1.2.2 Video codecs evaluation test results

We evaluated the video codecs and benchmark using system resources as the parameters for testing. We used Pentium 4 2.8 Ghz with 512 MB ram as a test setup machine. Following Table I illustrate the test results:

Table I: Benchmarking of video codecs		
No	Video Codec	CPU Utilization
1	VP6	98%
2	VP7	100%
3	H.264	99%
4	x.264	97%
5	Divx 5	90%
6	Xvid	90%
7	Theora	97%
8	Mpeg 4 v3	50%

1.2.3 System Overview

Our framework consists of two components, Video capture or video sender component and the video playback or video receiver component. Following are the system overview of two components:

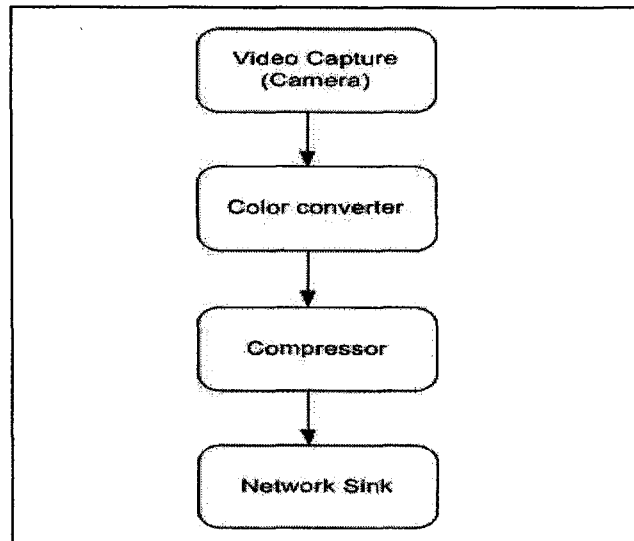


Figure 1: Video capture overview

Video capture part of our framework is responsible for capturing video from the camera and forwards the uncompressed data to the Color converter. Color converter converts the color depth of video from 24 bit to 16 bit. Then the data is moved to compressor which will compress the data with a high quality video codec like H.264. After compression, data send to network. We use our own packet format which is based on RTP (real-time transfer protocol). [14][15]

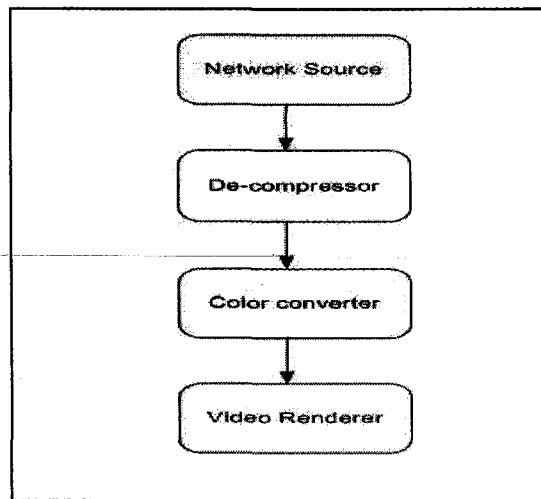


Figure 2: Video capture overview

Video playback component captures the packets from the network and sends the data to the de-compressor. After Decompressing, data send to color converter which transform the color depth from 16 bit to 24bit. Video renderer renders the data on screen.

1.2.4 Implementation

Our framework is implemented using Microsoft Visual C++ as a baseline programming language, component architecture using Microsoft Component object modeling (COM) and media framework with Microsoft Directshow architecture.

Microsoft DirectShow is a media-streaming architecture for the Microsoft Windows platform that enables the high-quality capture, compression, decompression and playback of multimedia content. The content can contain video and audio data compressed in a wide variety of formats, including MPEG, audio-video interleaved (AVI), MPEG-1 Layer 3 (MP3), and WAV files. Capture can be based on either Windows Driver Model (WDM) or legacy Video for Windows (VFW) devices. DirectShow also utilizes the DirectX technologies to take advantage of any audio and video acceleration hardware to deliver the highest possible performance. [11][12][13]

1.2.5 Multimedia Conferencing System (MCS)

MCS Version 6.0 presents a revolutionary MULTIPOINT-TO-MULTIPOINT video conferencing system that is ahead of current video conferencing technology. It allows conferencing with as many people as needed from anywhere around the world.

1.2.5 Final Results

After final implementation and we integrate the module with MCS v6. Following is the sample picture capture showing wide variety of colors at high quality and resolution.

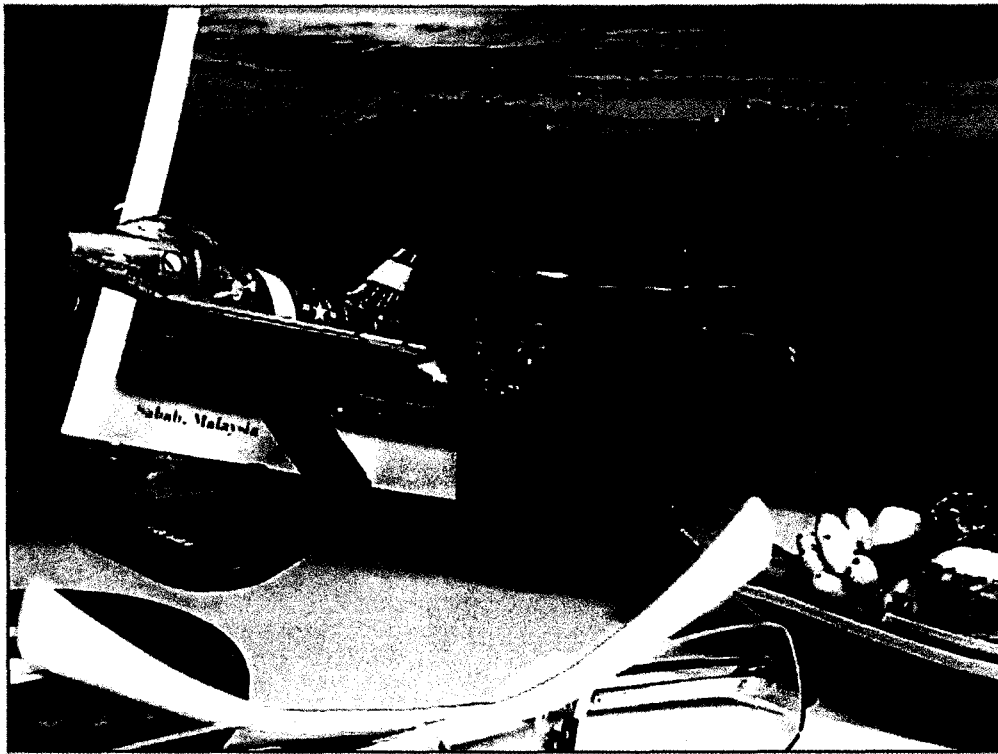


Figure III: High quality big picture

REFERENCES

1. White papers: Advantages of TrueMotion VP6 technology.
<http://www.on2.com/technology/vp6>
2. White papers: TrueMotion VP7 technology. <http://www.on2.com/technology/vp7>
3. H.264 / MPEG-4 Part 10 White Paper. www.vcodex.com
4. White Paper: MPEG-4 AVC/H.264 Video Codecs Comparison
5. RFC 3984: RTP Payload Format for H.264 Video
6. x264 - a free h264/avc encoder. <http://developers.videolan.org/x264.html>
7. Divx. <http://www.divx.com/>
8. Xvid. <http://www.xvid.org/>
9. Theora. <http://theora.org/>
10. VP3. <http://vp3.com/>
11. Microsoft Directshow
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/directshow/htm/directshow.asp>
12. Book: Programming microsoft directshow for digital video & tv.
13. Book: Programming microsoft directshow by Micheal Linetsky.
14. RFC 3550, RTP: A Transport Protocol for Real-Time Applications
15. RFC 3551, Standard 65, RTP Profile for Audio and Video Conferences with Minimal Control
16. Windows Media <http://people.csail.mit.edu/tbuehler/video/codecs/wm.html>
17. Multimedia Conferencing System - MCS: Technical White Paper.
<http://www.mlabs.com>