IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB12712

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

The Architecture of Presence Investigation for Remote Control

Hsieh-Hong Huang & Cheng-Yuan Ku
Dept of Information Management, National Chung Cheng University,, 168, University Road, Min-Hsiung, Chia-Yi 62102, Taiwan, R.O.C., {chorist, cooperku}@mis.ccu.edu.tw

ABSTRACT

With the rapid development of software and communication technologies, the availability of remote control of computers has become increasingly popular. Unlike the traditional remote applications, which are working under text mode, the new remote desktop technologies provide graphic user interface (GUI) for users to control their faraway computers via Internet now. There are numerous commercial products of remote control software that enables users to take control of the distant desktop with their own keyboard and mouse from other place, even abroad. This characteristic makes the usage of remote access and control of computers easier; and thus improves productivities. However, most remote control or remote administration software packages are not well-documented. This situation causes that it is difficult to monitor, record, and detect the online illegal action. Because of the lack of well-organized transaction log, it is really hard to trace and audit illegal activities if the suspect uses remote control software. It has increased the difficulties of cyber forensics and the distress of the law enforcers due to the national or jurisdictional boundary. In this paper, five countermeasures for cyber-crime regarding remote control software are proposed. This result could be viewed as a pilot study of remote presence and provides the guidance for further research.

INTRODUCTION

With the advance of information and networking technologies, the number of criminal cases on Internet has largely increased. Even though many experts and researchers had been working on various problems of the network, there are still a lot of works that need to be done. As observed from reports on all kinds of medias, cyber-crime happens anytime and anywhere. As shown in research results, computing facilities from the world now can be networked together that transcends jurisdictional boundaries and increase in computer use has been accompanied by a rise in cyber-crime (Brungs and Jamieson, 2005).

Moreover, computer remote control and administration is a previously undocumented tradition that evolved from scientific and technical network environments and is now becoming applicable to an increasing range of business networks (Reed, 2005). Due to the popularity of remote access software, like Terminal Services with Remote Desktop Connection (RDC), cyber-suspects and their computers may locate at different places. So, a new pattern of cyber-crime, which is related to remote access control, is going to be prevalent. In fact, it is not easy to monitor, trace, record, and search for the illegal activities on the Internet due to the national or jurisdictional boundary. Some studies focusing on log-tracing of remote login were done, but a more efficient way to record and prove the abuse of remote control software is still in need.

Remote access or administration is defined as that a specific host runs a service that enables a remote person or process to connect to remote computers and allows access according to their specific access privileges (Venter and Eloff, 2003). Traditionally, users could access and manage the remote host by sending text-mode commends. With the help of new technology GUI, remote access control packages become more popular and provide various features that allow users to interact with computers through direct manipulation of graphical images. It is especially useful for screen control and to monitor separated computers when computer support staffs are located across campus, or even farther away (Jones, 2004). Some research results also indicated that although remote administration would allow a user to remotely monitor and control a target system and perform some operations in the distance, for instance, to execute any applications on the target machine, to view the contents of any file on the target machine, and to transfer files to and from the target machine, but it might take security risks if placed in the wrong hands (Furnell et al., 2001).

BACKGROUND

Remote access technology is not a new thing. It has been more than thirty years since telnet was proposed in RFC 318. Telnet has become more efficient and convenient with the widespread diffusion of the Internet. As described in RFC 318, telnet protocol is intended to eliminate the need for using and serving sites to keep information about the characteristics of other terminals, which can handle conventions among users, the using site, and the serving site (ITEF, 2005).

After the GUI technology is introduced, remote access software became more and more popular and convenient. Using GUI, remote access software can control a distant desktop with drag-and-click interface. Most packages communicate with targeted computing facility by redirected keyboard or mouse inputs. The user can view the displayed output on his/her screen.

Microsoft proposed a specific protocol for remote control and access on Windows 2000, XP and 2003. It was named as Remote Desktop Protocol (RDP). This protocol is functionally equivalent to X Window System for UNIX and XDMCP for Linux. Due to the usage of GUI, there is no well-documented log file for transaction about remote control software. Therefore, in this paper, we used the widely used GUI-based remote control software as subject to study the related security problems. Microsoft's RDP, a built-in feature of Microsoft Windows 2000, Microsoft XP, and Microsoft Windows 2003, is the most popular remote control software. In the following, we show how the remote control process works step by step (Cai et al., 2004).

Step 1: Client sends a nonce to Server (Hello).
Step 2: Server responses with a random number, public key of Server, and selected cipher suite, which contains the encryption algorithms supported by the client, and requires that subsequent message received from Client contains the correct value.
Step 3: Client encrypts the random number with the public key of Server and then returns to Server.
Step 4: Client starts transmitting RC4-encrypted commands and message authentication code (MAC) to Server.
Step 5: Server responses with the data encrypted in RC4 and MAC back to Client.
Step 6: Disconnect.

As observed, some bad things, such as deception, threaten and terrorist communication, could happen and not caught if there is no good mechanism to detect the traffic while necessary.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

PROPOSED COUNTERMEASURES

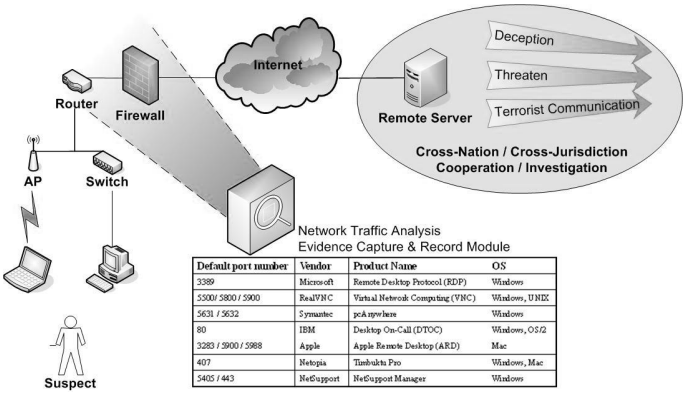
Traffic Analysis

In software market, there are many network analysis tools, such as A-PacketMan, SecuServer, Ethereal, TCPDump, NetMonitor, SnifferPro, and Snort. These tools can help cyber investigators to collect important evidences and may have been used. After a suspect is identified, the investigator can monitor unusual traffic coming from the suspect's computer to particular target by analyzing network traffic. The well-known service ports and ports used by remote control transactions are the first choice to be watched. If the investigator can not recognize the content of captured packets, at least he/she can collect the communicating target of suspect and then draw the overview picture of the corresponding criminal event.

Capture and Record

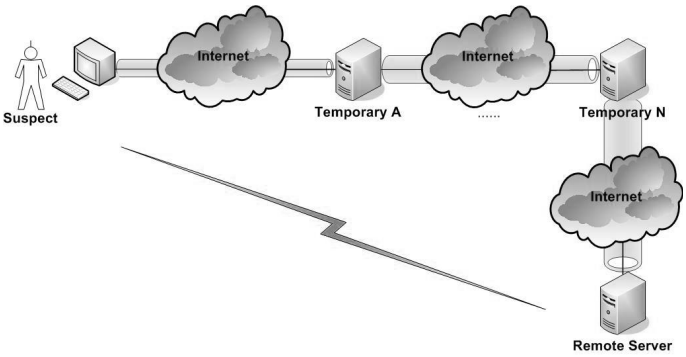
Berghel stated that Internet forensics deals with the ephemeral and transient events (Berghel, 2003). That is the reason why Internet forensics is thus essential. As mentioned earlier, the communication protocol of remote control software is well-known, so investigators can focus on this point. First, use the specific monitor software to monitor and detect port 3389. Only when the communication using port 3389 is identified, the related software module is automatically activated to keep an eye open on the source and destination IP. Then the monitor analyzes network traffic flow, even the contents of network packets. The monitoring and recording software module is able to capture these packets and resolve them to understand what the suspects are doing in the distance. The earlier-mentioned countermeasures can be integrated and implemented as shown in Figure 1.

Figure 1. The Architecture of Presence Investigation for Remote Control



Default port number	Vendor	Product Name	OS
3389	Microsoft	Remote Desktop Protocol (RDP)	Windows
5500/ 5800 / 5900	RealVNC	Virtual Network Computing (VNC)	Windows, UNIX
5631 / 5632	Symantec	pcAnywhere	Windows
80	IBM	Desktop On-Call (DTOC)	Windows, OS/2
3283 / 5900 / 5988	Apple	Apple Remote Desktop (ARD)	Mac
407	Netopia	Timbuktu Pro	Windows, Mac
3405 / 443	NetSupport	NetSupport Manager	Windows

Figure 2. Multiple Levels of Remote Control Activities



Regulations and Legislation

The source code of some remote access packages, such as VNC, is publicly available. Hence, it is not difficult for the investigators to watch over what a suspect is doing and record it. Although some software packages, for example Desktop On-Call, do not release the source code, the investigators still can try to capture and view the screen shot of remote computer by sniffing the network packets. Of course, there is no good way to deal with the remote control packages if they use specific coding and decoding protocol, such as RDP. No official document of RDP is publicly available. Therefore, the decoding work without help from vendor is almost impossible. The government should consider to actively getting involved. Use the corresponding laws to enforce remote control software vendors to disclose more detailed information or provide specific monitoring methods for crime investigation as the precedent cases of the regulation on cryptography. The U.S. Cyber Security Enhancement Act (US-CSEA) had permitted that when there is an ongoing attack on any computing facility, surveillance is allowed to collect a suspect's personal information. However we still need more powerful regulations to prevent the misuse of remote control software.

Cross-Nation and Cross-Jurisdiction Cooperation

In the most cases of remote control presence, suspects and their remote servers were separated geographically and temporally. Investigators should collect the remote server as evidence for a local computer crime. Unfortunately the remote server might be located in other jurisdiction, region or country. The problem of multiple-level remote control, which crosses the national and/or jurisdictional boundary, has raised the complexity of remote control crime. Therefore, the cross-jurisdiction and cross-nation investigation and cooperation is especially in need. Now, U.S. and British agents are trying hard to get other countries to cooperate in sharing criminal information and some European and Asian governments are beginning to work with U.S. and British to fight back against remote control and Internet crime (Germain, 2005).

Variations

A network suspect may use different combination of remote control software packages to hide his/her action and trace. Furthermore, he/she may use multiple levels of remote activities to avoid tracking as shown in Figure 2. Until now, there is still no efficient way to deal with these variations. We think that it is the obligation of the software vendors to build up the complete log mechanism in order to prevent the cyber crime, especially for the hard problem of remote access.

DISCUSSION

To be honest, there are always pros and cons in using computer and communication technologies. In fact, performance of the information technology relies on how the corresponding participants use it. They can use it in a good way or bad way. Since the cyberspace is like the real world, any criminal behavior should be caught and punished. Therefore, there should be some scientific methods to collect, record and identify the criminal activities.

As Berghel said, where computer forensics deals with physical things, Internet forensics deals with the ephemeral (Berghel, 2003). That is why Internet forensics is so important to form a discipline from computer forensics. In addition, the authorities of different countries should work together to build up the inter-jurisdictional laws to prevent cyber crimes and train professional technicians to fight for crimes using remote technology.

REFERENCES

Berghel, H. (2003). The discipline of Internet forensics. *Communications of the ACM*, 46 (8), pp. 15-20.

Brungs, A. and Jamieson, R. (2005). Identification of legal issues for computer forensics. *Information Systems Management*, 22 (2), pp. 57-66.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

Cai, L., Yu S. and Zhou J. (2004). Research and implementation of remote desktop protocol service over SSL VPN. *Proceedings of 2004 IEEE International Conference on Services Computing*, pp. 502-505.

Furnell, S. M., Chiliarchaki, P., and Dowland, P. S. (2001). Security analyzers: administrator assistants or hacker helpers? *Information Management & Computer Security*, 9 (2), pp. 93-101.

Germain, J. M. (2005). The Real-Life Internet Sopranos. NewsFactor Network, available at http://www.newsfactor.com/story.xhtml?story_id=39574

ITEF (2005), Request for Comments. http://www.ietf.org/rfc.html

Jones, C. (2004). How long can we keep doing more with less? *Proceedings of the 32nd annual ACM SIGUCCS conference on User services*, pp. 125-128.

Reed, A. (2005). Information technology and systems – II: server administration networks. *Communications of the Association for Information Systems*, 15, pp. 642-660

Sipior, J. C., Ward, B. T., and Roselli, G. R. (2005). A United States perspective on the ethical and legal issues of spyware. *Proceedings of the 7th international conference on Electronic commerce*, pp. 738-743.

Skoudis, E. (2002). Infosec's worst nightmares. *Information Security*, November 2002, pp. 38-49.

Venter, H. S. and Eloff, J. H. P. (2003). A taxonomy for information security technologies. *Computers and Security*, 22 (4), pp. 299-307.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.

0 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/proceeding-paper/architecture-presence-investigation-remote-control/32967

Related Content

Mutation Testing Applied to Object-Oriented Languages
Pedro Delgado-Pérez, Inmaculada Medina-Buloand Juan José Domínguez-Jiménez (2018). *Encyclopedia of Information Science and Technology, Fourth Edition (pp. 7459-7469).*
www.irma-international.org/chapter/mutation-testing-applied-to-object-oriented-languages/184443

Material Flow Management in Industrial Engineering
Costel Emil Cotetand Diana Popescu (2015). *Encyclopedia of Information Science and Technology, Third Edition (pp. 3786-3794).*
www.irma-international.org/chapter/material-flow-management-in-industrial-engineering/112817

An Adaptive CU Split Method for VVC Intra Encoding
Lulu Liuand Jing Yang (2023). *International Journal of Information Technologies and Systems Approach (pp. 1-17).*
www.irma-international.org/article/an-adaptive-cu-split-method-for-vvc-intra-encoding/322433

Fog Caching and a Trace-Based Analysis of its Offload Effect
Marat Zhanikeev (2017). *International Journal of Information Technologies and Systems Approach (pp. 50-68).*
www.irma-international.org/article/fog-caching-and-a-trace-based-analysis-of-its-offload-effect/178223

Re-Engaging the Public through E-Consultation in the Government 2.0 Landscape
Shefali Virkar (2015). *Encyclopedia of Information Science and Technology, Third Edition (pp. 2774-2782).*
www.irma-international.org/chapter/re-engaging-the-public-through-e-consultation-in-the-government-20-landscape/112696