

桃園區網中心管理委員會
第三十六次會議
校園網路現況與經驗分享

(一) 技術篇

南亞技術學院電算中心

網路管理組組長 邱守男

email: snchiou@nanya.edu.tw

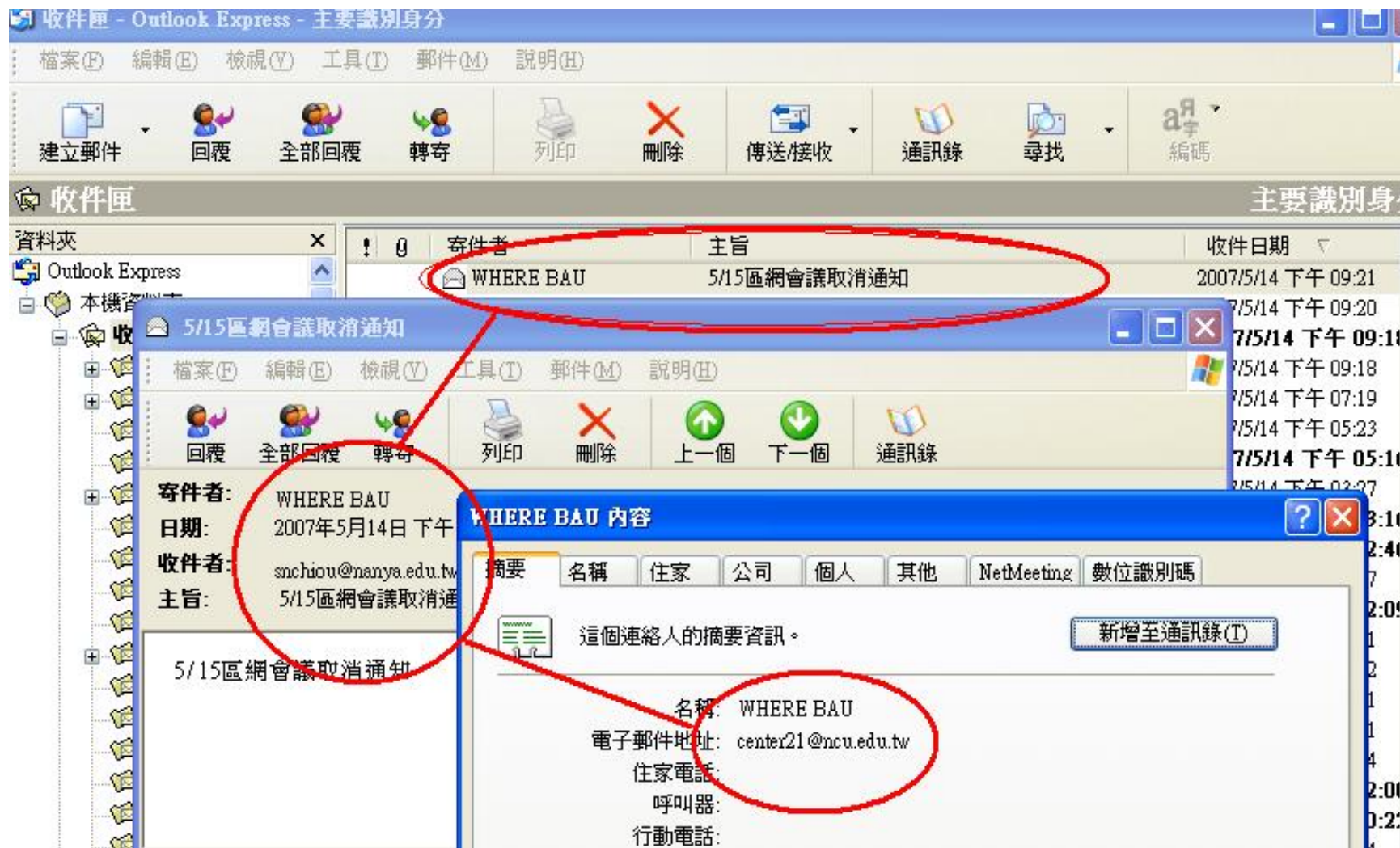
偽造電子郵件

SMTP 協定只負責”儘力”傳送

1. 不保證成功送達收件者手上
2. 不保證”MAIL FROM”是真的。所以 Outlook Express 看到的寄件者可能是假的。
3. 現有的 antiSpam 軟體沒有過濾偽造信能力

Solution=> 自己寫程式去追蹤判斷

追蹤偽造電郵 (一)



追蹤偽造電郵 (二)

```
[2007/05/14 15:00:08] [203.68.49.100:336-5] HELO 100.49.nanya.edu.tw
[2007/05/14 15:00:09] [203.68.49.100:336-5] MAIL FROM: <center21@ncu.edu.tw>
[2007/05/14 15:00:13] [203.68.49.100:336-5] RCPT TO: <snchiou@nanya.edu.tw>
[2007/05/14 15:00:30] [203.68.49.100:336-5] Connection closed. (33s.382030u)
```

自動過濾

```
[2007/05/14 15:01:53] [203.68.49.100:336-2] HELO 100.49.nanya.edu.tw
[2007/05/14 15:01:54] [203.68.49.100:336-2] MAIL FROM: <admin@moe.edu.tw>
[2007/05/14 15:01:59] [203.68.49.100:336-2] RCPT TO: <meiguo@nanya.edu.tw>
[2007/05/14 15:02:00] [203.68.49.100:336-2] RCPT TO: <qa93@nanya.edu.tw>
[2007/05/14 15:02:01] [203.68.49.100:336-2] RCPT TO: <khc@nanya.edu.tw>
[2007/05/14 15:02:02] [203.68.49.100:336-2] RCPT TO: <hty0223@nanya.edu.tw>
```

這是偽造信！

自動追蹤發信 ip 來源

For Help, press F1

Ln 4, Col. 76, C0

DOS

Mod: 2007/5/14 09:28:19下午 File Size: 27903

IP代理發放單位網段:203.68.0.0-203.68.255.255

Chinese Name	教育部
Netname	TANET-NET
Organization Name	Ministry of Education Computer Center
Street Address	12F, No 106, Sec.2,Hopi Rd.,
AdminHandle	YHC153-TW
TechHandle	TA8-TW
SpamHandle	YHC153-TW
用戶單位:203.68.48.0/23	
Netname	T-NANYA.EDU.TW-NET
Organization Name	NAN-YA JUNIOR COLLE
Registered Date	1997-09-01
Admin. Contact	TCAC@mailnanya.edu.t

命令提示字元

```
325 count:...
Found 0 lines
Done!
C:\Dev-Cpp\MyProjects\smtp>smtptracer2 center21@ncu.edu.tw
複製了 1 個檔案。
scan [smtpd.log]...
1 count:...match 1 found,ip= 203.68.49.100
scan [smtpd_temp.log]...ip hit:326
16 count:...match 2 found,ip= 203.68.49.100
scan [smtpd_temp.log]...ip hit:326
31 count:...match 3 found,ip= 203.68.49.100
scan [smtpd_temp.log]...ip hit:326
46 count:...match 4 found,ip= 203.68.49.100
scan [smtpd_temp.log]...ip hit:326
61 count:...match 5 found,ip= 203.68.49.100
```

2007-05-15

南亞技術學院

4

Conclusion

- Thanks for Listening ~