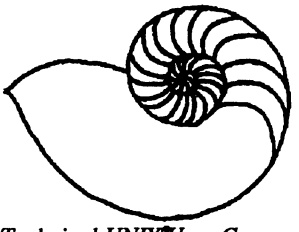


Technical UNIX User Group

May 1989 $2.50
Volume 1, Number 8

newsletter of the

Technical UNIX® User Group

This month ...

Late Breaking News...
Next Meeting to be held at Prime Computer
See inside for details

Your article could go here!

Become an active member of the Technical UNIX User group and submit your newsletter article today.

Group Information

The Technical Unix User Group meets at 7:30 pm the second Tuesday of every month, except July and August. The newsletter is mailed to all paid up members 1 week prior to the meeting. Membership dues are $20 annually and are due at the October meeting. Membership dues are accepted by mail and dues for new members will be pro-r[illegible]ly.

The Executive

President:	Gilbert Detillieux	261-9146
Vice President:	Vacant	
Treasurer:	Gilles Detillieux	261-9146
Secretary:	Susan Zuk	(W) 786-8483
Newsletter Editor:	Darren Besler	(W) 934-5475
Membership Sec.:	Pat Macdonald	(W) 474-9870
Information:	Gilbert Detillieux	261-9146
	(or) Susan Zuk	(W) 786-8483

Technical UNIX User Group
P.O. Box 130
Saint-Boniface, Manitoba
R2H 3B4

Copyright Policy and Disclaimer

ANNOUNCEMENT...

Meeting Location Change:
The May meeting location will be hosted by Matt Binnie at Prime Computer of Canada Ltd., Suite 808-240 Graham Ave (Cargill Building). In order to get into the building you will have to buzz the security guard. Upon entering the building you will then be required to sign-in.

President's Corner

by Gilbert Detillieux, President

Ah spring! The sun shines. The air warms. The streets get (cough!) cleaned at last! I always wait with great anticipation as the temperature climbs past another boundary: 10 degrees, then 15, then 20 (hopefully by the time you read this); and I think "This is what I've been waiting for!"

That is also the sort of excitement I feel as our membership count climbs past another "boundary." At our last meeting, we finally reached 30 paid up members. Maybe by the fall we'll reach 50! Who knows? We'll see.

Our last meeting featured a workshop-style presentation on UUCP, where we actually got a connection working between a system at Unisys and one of the Masscomps at the Health Sciences Centre. We were able to transfer mail messages and files back and forth. We still have this all set up and continue to use it to send messages between some members of the executive. One of our goals for the fall is to open this up to all members of the group, and use it for sending news updates about meetings, submitting material for the newsletter, and so on. We will likely be discussing this further at the next executive meeting and at the May users' meeting.

As I write this, I am busy preparing for the Business Show. Our company is one of three companies at the show this year who deal primarily or exclusively in UNIX related products and services. This may be a first for the business show, and is hopefully an indication that UNIX is catching on in Winnipeg. Also encouraging for the group is the fact that all three of these companies are members of TUUG.

This has been another one of those months where a lot of last minute rushing was done to get the newsletter out on time and plan for the next meeting. It seems that everyone in the executive gets busy at more or less the same time. Ah, if only we had a couple more bodies to help out at times like this! Maybe some of you newer members would consider helping out. It's not that much work, it's usually great fun, and it's a good way to get to know more about the group and its members. Remember that elections for the executive are coming up this fall, and that all nominations are welcome. But, more about this at the next meeting.

Speaking of the next meeting, as I write this, we still aren't sure where it will be held. You'll have to check the front cover of the newsletter to find out. Anyway, the presented topic will likely be a system administration workshop focussing on printer spoolers. We will also open it up to other topics if time permits.

It now looks quite definite that the June meeting (the last one before we take a two month break for the summer) will be a barbecue and outdoor party, and the best part: no business meeting! We still have to work out the details (including confirming the location), but you'd better get those lawn chairs ready! I hope we'll have a good turn- out. It should be a lot of fun.

Hope to see you at the next meeting (May 9). A happy springtime to all!

The fortune file

This month's fortune comes care of Darren Besler.

```
... Now you're ready for the actual shopping.  Your goal should be to get it over with as
quickly as possible, because the longer you stay in the mall, the longer your children will
have to listen to holiday songs on the mall public-address system, and many of these songs
can damage children emotionally.  For example: ''Frosty the Snowman'' is about a snowman who
befriends some children, plays with them until they learn to love him, then melts.  And
''Rudolph the Red-Nosed Reindeer'' is about a young reindeer who, because of a physical
deformity, is treated as an outcast by the other reindeer.  Then along comes good, old Santa.
Does he ignore the deformity?  Does he look past Rudolph's nose and respect Rudolph for
the sensitive reindeer he is underneath?  No.  Santa asks Rudolph to guide his sleigh, as
if Rudolph were nothing more than some kind of headlight with legs and a tail.  So unless
you want your children exposed to this kind of insensitivity, you should shop quickly.

                -- Dave Barry, ''Christmas Shopping: A Survivor's Guide''
```

Comments on Password Aging

By David Ferrier

[Ed. - The following was retreived from the Unix-Wizards electronic mailing list. The message was addressed from <security%pyrite.rutgers.edu%pica.army.mil@BRL.MIL> but appears to be authored by David Ferrier <ncc!myrias!dbf@pyramid.com>.]

>Resent-Date: Wed, 18 Jan 89 8:46:36 EST
>Password aging minimizes the amount of time that your
> password is open to attack. You may have a well-chosen
> password, but the longer it is >used, the more likely it is that
> someone has [obtained it]...

This sounds good, but no matter how they try to justify or explain it, password aging is one of those things that system administrators do that look really good to system administrators, auditors, and security consultants, but in practice does not give enough benefit to justify the tremendous inconvenience and loss of time caused to users and the organization.

Security measures are put in place to prevent losses. If the cost over time of a security measure exceeds the probability of loss over time times the value of the assets, use of the security measure is bad management. Password aging is an example of a security measure, which, except for the CIA or other exceptional organizations, usually costs more to implement than the value of the assets protected.

What does password aging buy you?

- It helps reduce risk by preventing access to the system and data by unauthorized users.

Examination of past security incidents invariably shows that almost all damage done to systems or data was done by authorized users with passwords, not by the spooks that password aging is supposed to defend against.

What are the risks of access by unauthorized users?

- Theft of machine cycles, unauthorized access to data, unauthorized modification or destruction of data.

In most systems, the wastage of machine cycles by authorized users who are inexperienced or inefficient, or read dozens of USENET articles every day, far exceeds the possible cost of system use arising out of unauthorized access.

As for data: signon passwords are only the first line of defense.

Depending on the system, a user often has limited access to data. Unless unprotected data are not backed up, contain vital trade secrets, or there is no audit trail log generated of modifications to critical data, access by an unauthorized user is not much of a problem--not enough, anyway, to justify the cost of password aging.

What is the objective improvement to security given by password aging?

- Who knows? How can you measure the likelyhood of a password being compromised when it is not changed regularly? A similar study might be done on people with wall safes who do not change the combination on a regular basis.

What is the cost of password aging?

- Administrative: staffing a responsive corporate security department who can give out new passwords to users who tend to forget theirs when they have to change them regularly.

- User: need to build into project schedules enough slack to allow for loss of productivity due to being unable to access the system because a password has expired.

- Organizational: replacing people who get fed up with the security run-around and leave.

Anything constructive to say about password aging?

The following concepts came from working with a password aging system used by a Toronto computer utility that prevented reuse of any password for 20 cycles. Worse, it even prohibited use of near matches--"moon" and "fool" for example. Users had to keep a list of old passwords, because as a final diabolical twist, the system only gave you five tries to assign a valid new password when the old one expired, at which point use of your id was suspended.

- If you must have password aging, keep it within reasonable bounds. As with any other corporate program, force the people proposing it to do a cost justification, and make a business case if they can for forcing people all over the company do regular password changes.

- Make sure it is an option that you can control on an individual or departmental basis, so that only people with high risk data or extensive access rights are put to the inconvenience of changing passwords frequently, or at all. This control should extend to the number of generations of old passwords that are kept on file to ensure the new password does not replicate a previous password.

-- David Ferrier
alberta!myrias!dbf

Edmonton, Alberta
(403) 428 1616

[Moderator note: It looks like the upshot of this discussion is that aging isn't really much help... _H*]

Securing Your Network

By Derek Hay

A few year ago, the only people who were concerned about computer security were the managers and administrator of large mainframe centers. However with today's fast growing pace of micro- computers, there is now a need to implement a security plan.

HARDWARE

The network system should be located in a secure area away from windows or outside walls. Care should be taken into where the main data storage unit is kept, as to assure that it is under an extensive physical security system.

Try not to use workstations that allows data to be stored on a storage device and/or save on a removable media. Terminal cables should be shielded as well as run inside conduit and should not leave the confines of the owners office. Such as running along the suspended ceiling of a common access hallway or shaft. Where ever possible, the use of fibre optic cable should be used, as this is harder to try and tap or splice into. Position workstations so that passer's-by can not see the screens.

Printers should be centrally located and set up so that confidential documents do not print until an authorized person actually goes to the print room and redirects the print job to the printer. This person would then be able to oversee the printing to assure that no unauthorized personael see the data. Printers also should be turned off and/or disabled at night time to assure that no reports are printed unauthorized or left sitting on the printer for people to read.

The use of modems should be restricted only to business hours, and only to personnel who actually need to use the device. If possible, modems should be configured to accept a call, verify the caller, then disconnect and call them back at a telephone number assign to the caller.

PASSWORDS

Every user on the network should be assigned a user log-in ID as well as a starting password. The users should then set their own new password the first time they log-on the system. Passwords should not be told to anyone, and if they are compromised they should be changed immediately. Passwords should also not be seen as they are typed in. Care should be taken in the choice of your password. Do not use common names such as your wife's or childs name, or the name of the family pet. A combination of 6 to 8 upper and lower case characters as well as numeric symbols should be used. If at all possible, the password can be randomly generated by the computer.

Once a password is set, it should not be written down or kept in a non-encrypted form on the computer system. Please do not tape it to the bottom of your terminal. No one, including the system administrator, should be able to decern your password, or have the ability to change it. The administrator should only be able to start a procedure for a new password where by the user enters their own new unique password. A procedure should be set up so that the system request that passwords be changed after a ninety day or so period has passed by.

ACCESS TO THE SYSTEM

Now that each user has a log-in ID and password, how do we control what they do once they are logged on. Firstly each user should only be allowed to log-in from one particular device. They should not be allowed to log-in from any terminal. If some one needs to use a different terminal periodically the system administrator can set up a temporary ID on the requested terminal.

Once a user is logged onto the system, they should be restricted only to system resources & files according to their user ID, security access level and group rating or name. (eg. a user can only access their own files privately, system utilities and files according to their access level, and other user files according to their group associated name. All common architect files would have a group rating of arch. Thus the file can shared among the group.

Read, write, and execute status should also be set for each file on the system by owner, group, and access level.

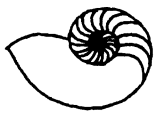
The ability for a user to change groups and to which group they can change to should be closely monitored and periodically reviewed to see if they still need to have access to a particular group's files.

All users should enter the system at the same point and then follow paths which increase in security the farther they proceed from the log-in area. Users should not be able to jump from one path to another without first returning to the starting log-in point.

JOB ACCOUNTING

A job accounting log should be keep for every task that is started or attempted to be started. The job should consist of who started which procedure, at what time, and from which device it was initiated. The log should also be protected so that only the system administrator can start, stop, or modify it.

All though not all current micro-computer networks have the ability to provide all of the mentioned security features, they do provide most of these options. As technology advances, and we are able to port main-frame operating systems down to the micro world, the need for a well maintained system will be a top priority and should be carefully thought out before the system is brought up to operational control.



Minutes From the Business Meeting
April 11, 1989

1. Minutes:

MOTION : (Susan Zuk) The minutes from the March 14th, 1989 meeting be approved.

SECONDED : (Paul Hope)

In Favour : 16 Opoosed : 0 Carried

2. Membership Report:

We now have a total of 30 paid members. The membership list is being included in May's newsletter.

3. Newsletter Report:

Note that the April newsletter included shell program listings. Please submit articles and thank you Derek for your submission.

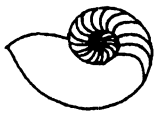
4. Treasurers Report:

Financially we are in doing well and shouldn't have to increase membership fees for next year.

5. Miscellaneous:

A discussion was held on forming a special interest group (SIG) next year. This special interest group would be for people interested in the marketing side of UNIX. Such things as standards, who's doing what and what UNIX projects are going on in Winnipeg would be topics discussed. The idea will be discussed, by the executive, over the summer break and then brought to the general membership in the fall. Anyone interested in either forming the SIG or becoming involved should let someone on the executive know.

Note: The SIG meetings should be separate from those of the technical group but each SIG would have their own report in the newsletter.



Agenda

for

Tuesday, May 9, 1989
7:30pm
Prime Computer
Cargill Building
808-240 Graham Avenue

1. Round Table 7:30

2. Business Meeting 8:00
   a) Minutes of April's Meeting
   b) Membership Secretary's Report
   c) Newsletter Report
   d) Treasurer's Report
   e) Nominations
   f) BBQ June 13 g) modem

3. Break 8:30

4. Presented Topic 8:40
   System Administration Workshop
   a) Backup/Restore Procedures
   Uqueue - UNITECH Software

5. Adjourn 9:30

- Arrive at 6-30 PM
- RSVP by Friday June 9
- Lawn chair
- 3 BBQ's
- BYO Meat, BYOB
- Spouses, friends, kids welcome (RSVP)