TAP

The Hobbyist's Newsletter for the Communications Revolution

SPRING 1984 No. 91

Produced by TUC & BIOC Agent 003

Dunn and Bradstreet: Do they know something that we don't

by BIOC Agent 003 & Tuc

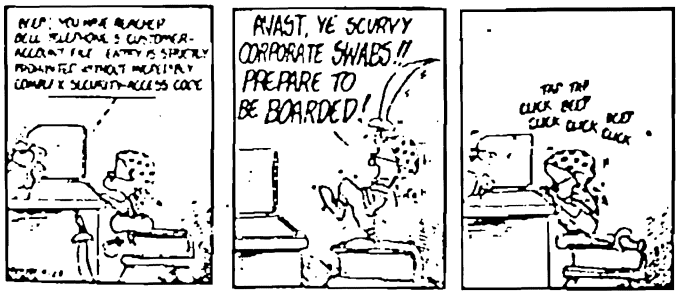
In issue #90, we explained how to use the Dunn and Bradstreet system (which is now known as DunSprint). A week after the issue was mailed a phellow phreak found out that a copy of the issue had fallen into the hands of our "friends" at D&B. To say the least, they weren't exactly thrilled about it. In fact, they did not even believe that they had a security problem! Well, that just goes to prove that if you are good (or they are incredibily stupid, whichever the case may be) no one will know that you are there!

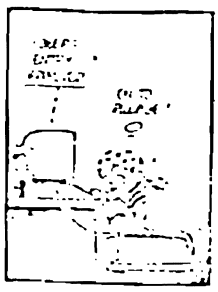
In a big effort to defeat hackers, they called in an outside service to spruce up their "security." Fortunately for us, we were able to find out about the new system! This was not really a problem, though. First, they had the new dial-ups posted when you logged on. Secondly, they have a nice little place on Telenet! (Where we do most of our "work" -- C 20188).

Recently they have set up a new system they like to call DunsNet. They are trying to pass it off as a big savings of time since the hassle of using a time shared public network does not exist. We are sure that Mr. J.W.P. of DUNSPRINT had more on his mind when he wrote the letter (on the system)! DunsNet is accessible from a regular dial-up. We have not been able to get a number yet for this system; once on it allegedly works just like Telenet! Two carriage returns and you will see "DunsNet" followed by the familiar "@" symbol. To use the system like we showed you, type "RPTS" at the prompt. To see Duns Financial profiles type "DFP". Finally, to use the Official Airlines Guide, type "OAG". One nice thing about the system, though, is when you type help from the "@", it gives you a variety of options to try.

Sorry D & B.... Good news travels fast!

This is not a mirage. Details in issue #92!





YET MORE PHUN WITH UNIX

by BIOC Agent 003

In previous issues of TAP, Fred Steinbeck (issues 78 & 79) & Simon Jester (issues 75 & 77) wrote about some interesting features of UNIX. In this article, I will hopefully expand on that theme.

Most UNIX systems are capable of communicating with other UNIX systems through a series of programs called uucp. Once on a UNIX system, type ls /usr/lib/uucp to list the support files stored in conjunction with the uucp programs.

The two most important files in this area (from a hackers point-of-view) are L.sys & L-dialcodes. It is in these files that the UNIX system stores the numbers AND passwords to other UNIX systems!

The first file (L.sys) contains: 1) the name of the remote system, 2) the time that the first UNIX system should call, 3) the hardwired device that should be used for the call (ie, modem port #), 4) the baud rate, 5) the phone #, & 6) the logon information. For example, the file might look like:

```
MaBell Mo,Tu tty99 300 dc2638 login: uucp ssword: it
```

In the example, the system called MaBell can be called on Mondays or Tuesday. You can probably call any time you want, though. The UNIX system is to dial it through device tty99 (not important to us). The number is dc2638. It will then wait for the string "login" and send uucp (the username), it will then wait for the string "ssword:" and send the password (it).

As you may have noticed, the phone # (dc2638) is non-standard. This is because the system can use abbreviations from the "L-dialcodes" file. A typical file might look like:

```
tc 9w18005215400w122-5e73w
dc 311555-
```

In this case dc2638 is really 311-555-2638. Also, some extenders may be thrown in the file! The "w" means to wait for dialtone.

To list these file you would type:

```
cat /usr/lib/uucp/L.sys
cat /usr/lib/uucp/L-dialcodes
```

(cont.)

In most cases, these files are protected but intelligence is not a prerequisite for UNIX administrators! Although, this should be no problem if you logon as (gasp!) the super-user (alias "root").

Unfortunately, the uucp password does not run under the normal UNIX shell. It uses a separate protocol.

If you are successful in obtaining these files you will have expanded your directory of UNIX systems, passwords, and possibly even SCC's & WATS extenders! If you master the uucp protocol you can copy ANY file! Once on other systems, this could work in a vicious cycle [vicious for THEM (that is)].

Hacking Western Union Revisited (Part II)

By Tuc

I've had a few questions from the people who have read my first article which I co-wrote with BIOC Agent 003 (TAP #90). They were asking what other things are possible with Easylink (1-800-325-4112). Well, to save time and space, the best command on the system is "/HELP". What I am going to explain, however, are two other services that Western Union provides with their Easylink.

The first of these is for whats known as "For Your Information" (FYI). This service is available to present Easylink subscribers for a "nominal" connect charge. FYI is very informative in what it contains. News that goes over the UPI wire is on-line with several other "neat" options. You are able to get up to the minute information on current events in the world. You can also access stocks, ski reports, entertainment news, and much more!

To connect to the service, you must dial 1-800-325-NEWS (1-800-325-6397). The familiar "ID?" prompt will once again appear. The logon format is in the same format as mentioned in part I (Eg : 01 USR999999 TEST.TEST). Once on, type CATALOG to see what reports are available.

Did you ever want to send a telex to a company you were almost sure had either Easylink or a Telex/TWX and didn't have the number? Or, have you had the telex number or answerback, but forgot who the heck it was for? Well, now Western Union makes it easy on you with thier version of Directory Assistance. To call, dial 1-800-325-1461 (300 baud only). When it answers, it is the same logon format as its associated services. Type DIRECTORY. Then, type NBR NNNNNNNNN if you need a telex number. (Eg: 62099999 (Easylink), 7105812236 (TWX), or 823410 (Telex I)). To find out by the answerback, type : ANS (answerback).

To find the number and information on a company when you know the company name and state, the sequence is: NAM SS CCCCCCCCCCC. SS is the two letter state abbreviation and the C's represent the company name.

There are two other commands for the system (besides DIRECTORY). They are FORMAT (a brief & useless help file) and WORLDWIDE FACTS (telex country code info, time zones, capitols, etc.).

Well, have fun, and if you find anything interesting, please tell me. Remember, you heard it first from Tuc at TAP.

A LESSON IN PHREAKING AND HACKING MORALITY:

By Big Brother

I find it truly discouraging when people, intelligent people seeking intellectual challenges, must revert to becoming common criminals. The fine arts of hacking and boxing have all but died out. Though you newcomers, you who have appeared on the scene in the last year or two, may not realize it, we had it much better. People didn't recognize our potential for destruction and damage because we never flaunted it, nor did we exercise it.

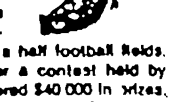
For hacking, it was the intellectual challenge which drove us to do it. The thrill of bypassing or breaking through someone's computer security was tremendous. It wasn't a case of getting a password from a friend, logging on, and destroying an entire database. We broke in for the challenge of getting in and snooping around WITHOUT detection. We loved the potential for destruction that we gave ourselves, but never used.

Today, after so much publicity, the fun has turned to true criminality. Publicity we have received is abhorring. From WarGames to the headlined October Raids, to the 414's, the Inner Circle, Fargo 4A, and the recent NASA breakins--not to mention all the local incidents that never made the big newspapers, like breakins at school computers or newspaper computers. TRW credit information services claims hackers used the three stolen accounts to aid them in abusing stolen credit cards. The thrill of entering and looking around has shifted to criminal practicality--how can I make my bank account fatter--how may I use this stolen credit card to its fullest--how could I take revenge upon my enemies.

And then there is the world of Phone Phreaking. The number of phreaks has grown from an elite few, perhaps ten or twenty, to well over a thousand. Still, there remain only about 10 or 20 good, longlasting phreaks. The rest receive information and abuse its uses until the information is no longer valid. Even worse, they seek publicity! They WANT to be caught! Many even use their real names on bulletin board systems to promote publicity. Meanwhile, the REAL phone phreaks have been resting in the shadow of the rest, waiting for phreaking to become so dangerous as to become a challenge once again. Once security tightens and only the strong survive (phreak Darwinism?), phreaking will be restored as a way to 'beat the system' without costing anyone anything.

Hacking may soon be dead, but may phone phreaking live on!

The charge: undefined
California, 1975
The take: Datsun 710 station wagon, a year's free supply of groceries, innumerable $5 gift certificates



Twenty-six students, used their university's IBM 370/158 computer to print out 1.2 million 3-by-5 forms with their names and addresses — enough paper to cover two and a half football fields. They used these forms to enter a contest held by McDonald's restaurants that offered $40,000 in prizes. Their entries made up over one third of the 3.4 million total entries. Though McDonald's protested the lack of ethics, the students met the contest qualifications and were allowed to keep their prizes. Since they had paid for their computer time, the school took no action against the students for using school computing resources. Burger King awarded $3000 to the school to set up a scholarship honoring the students.

PASSPORT CHECKSUMS

New passports are being issued throughout the world with a special laminated page that can be read by computers. These computers are linked to crime data banks such as INTERPOL. Of course they're nothing but a benefit to us, since they "speed up immigration queues."

When you pass through immigration, this page is inserted in a scanner. The scanner reads the last two lines on the page. In about two seconds, the computer returns all sorts of useful information about you (to speed up immigration queues, I'm sure). In a section of miscellaneous data (which the defendant is not allowed to see), appear any restrictions you have. Usually, the computer returns "NO TRACE". It can return other things, too, followed by the action the immigration officer should take. ACTIONS Q, A, AA, and J mean you're of interest to the police (in the UK). ACTION X means you'll be detained for inquisitioning.

This page is coated with a dye that will darken if exposed to oxygen (if the lamination seal is broken). Nitrogen or helium will not affect it, although it would be necessary to work in a fairly airtight environment, such as a clear plastic bag for microbe innoculations.

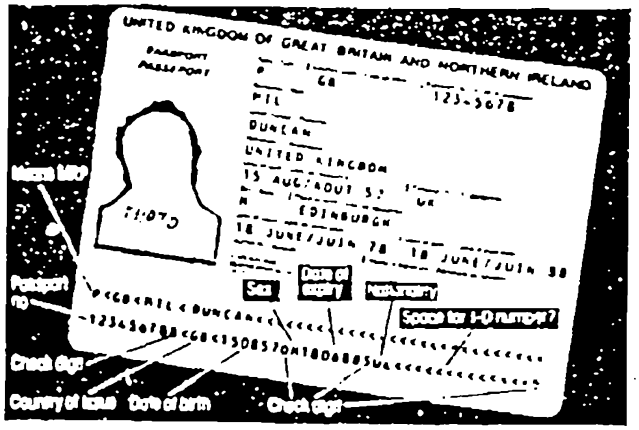
The first line contains a P (meaning the page is machine-readable), issuing country, and name. The second line contains an 8-digit passport number, a check digit right after this, issuing country, date of birth, a check digit right after this, sex (M/F), expiration date, nationality followed by several spaces (<'s), and a check digit in the last column. The check digits are calculated as follows:

1. Multiply each digit of a number (such as date of birth) by a number. For the first, fourth, and seventh digits, multiply the digit by 7. For the second, fifth, and eighth digits, multiply by 3. For the third, sixth, and ninth, multiply by 1.
2. Add the products.
3. Divide the sum by 10.
4. The remainder is the check digit.

A check digit is also calculated from passport number, expiration date, and possibly a national identification number. The final check digit is calculated from all other check digits.

More on this can be found in proceedings of the International Civil Aviation Organisation, and in the 5 January 1984 (vol. 101, no. 1391) of New Scientist. Since I'm not about to spend $42.00 on a new passport unless I have to, I don't know that the American format is the very same as this, but it should be.

--The New England Archivist--



The new passport page and at machine-readable numbers. The West Germans will use their page as an internal ID card. Space has been allowed for an ID number to be added

Risen from the ashes...

Europe - Not Half Bad.

by Cheshire Catalyst, Managing Editor

In issue 89, I put out the word. I was going to Europe. I was speaking to a seminar on Computer Crime. A few of the questins from the "Pack of Wolves" I found waiting for me (the press conference the seminar organizers set up for the first day of the seminar) asked things like "Why are you giving up your secrets to these Corporate types for?"

I mentioned that the people who had spent their money to be with us were here to learn how not to be stupid, but there were enough stupid companies out there for the crackers to have fun with. Besides, my newsletter is published for the kids who have fun with the systems they get into. The people attending our seminar should be grateful that the Electronic Graffitti artists awakened them to the fact that they have a data security problem. Just because IBM says you must be a member of the IBM priesthood to understand computers, doesn't mean that the statement is true. It's only how they want the public to relate to IBM mainframes.

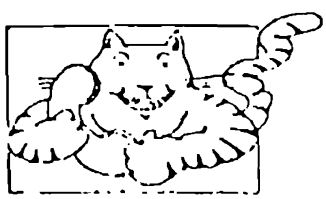
The corporate types should realize that if a teen-aged hacker is getting into their system, an industrial spy could have been logging in regularly for the past 3 years. While I may not particulary care for a TRW or Shitibank having "Confidential Information" about me, I especially don't like the idea of unauthorized people spreading the data around.

I got to Frankfurt for the Euro-Party, and no one showed up. Well, very few showed up. About 20 all together. Half of those people were journalists. I met Wau of the Chaos Computer Club of Hamburg, who I first met at Telecom '83 last September. He and his buddies are my hope for European computing. The type of 9-to-5 programmers that are of the "European Mentality" can't even program a videotex system made up of only menu trees. It takes "Hacker Mentality" to provide creative programs that do inspiring things.

In Munich, I spoke before an audience who didn't know, or care what the security problems were, they wanted quick answers. I was there to represent the threat that "hackers" supposedly posed. I explained that are no quick answers, because computer security is not just a matter of hardware, software, locks, and walls. Security is a people problem. When you put in locks, you watch the people you give the keys to (notice an analogy to encription here). If these people FEEL they're being watched, they may get "disgruntled". Needles to say, a disgruntled employee is worse than almost anything else you could be combating.

The beer was good (my favorite is Hacker-Pshorr) and I wish they'd import one or two of the beer halls. The beer halls sold bumper stickers, funny hats, and other party things, but I was appalled at how many women were blithly allowing their mates put cow bells around their necks. This is probebly some local custom, but I couldn't understand it. If those bells had the connotations I was thinking of, well, none of my girl friends would have appreciated it had I been crass enough to bring home a necklace like that.

Any of our corporate subscribers who would like to wake up their management to the vulnerabilities of computer systems should be made aware that I am available for lectures and consulting. Just drop me a line at the TAP maildrop, or via MCI Mail (Username: TAP), or telex number 650-119-5732.



BELL PIE
(To the tune of: "America Pie")

Long, long, time ago,
I can still remember,
When the local calls were "free."
And I knew if I paid my bill,
And never wished them any ill,
That the phone company would let me be...

But Uncle Sam said he knew better,
Split 'em up, for all and ever!
We'll foster competition:
It's good capitalism!

I can't remember if I cried,
When my phone bill first tripled in size,
But something touched me deep inside,
The day... Bell System... died.

And we were singing...
Bye, bye, Ma Bell, why did you die?
We get static from Sprint and echo from MCI,
"Our local calls have us in hock!" We all cry.
Ma Bell why did you have to die?

Is your office step by step,
Or have you gotten some Crossbar yet?
Everyone used to ask...
Oh, is TSPS coming soon?
IDDD will be a boon!
And, I hope to get a touch-tone fone, real soon...
The color phones are really neat,
And direct dialing can't be beat,
My area code is "low:"
The prestige way to go!

Oh, they just raised phone booths to a dime!
Well, I suppose it's about time.
I remember how the payphones chimed,
The day... Bell System... died.
And we were singing...
Bye, bye, Ma Bell, why did you die?
We get static from Sprint and echo from MCI,
"Our local calls have us in hock!" We all cry.
Oh, Ma Bell, why did you have to die?
Ma Bell why did you have to die?

Back when we were all at one rate,
Phone installs didn't cause debate,
About who'd put which wire where...
Installers came right out to you,
No "phone stores" with ballyhoo,
And 411 was free--seemed very fair!
But FCC wanted it seems,
To let others skim long-distance creams;
No matter 'bout the locals,
They're mostly all just yokels!

And so one day it came to pass,
That the great Bell System did colla'se,
In rubble now, we all do mass,
The day... Bell System... died.

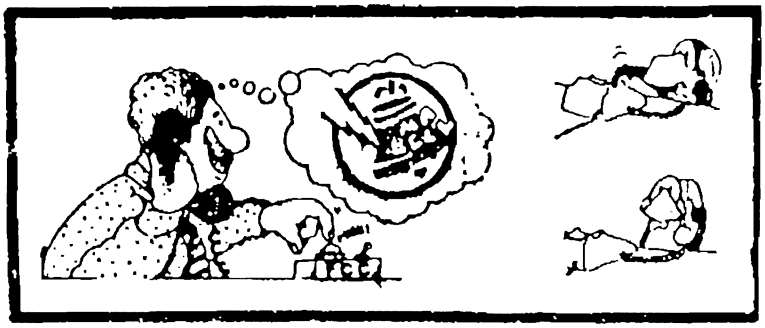
So bye, bye, Ma Bell, why did you die?
We get static from Sprint and echo from MCI,
"Our local calls have us in hock!" We all cry.
Oh Ma Bell why did you have to die?
Ma Bell why did you have to die?

I drove on out to Murray Hill,
To see Bell Labs, some time to kill,
But the sign there said the labs were gone.
I went back to my old CO,
Where I'd had my phone lines, years ago,
But it was empty, dark, and ever so re-cent...

No relays pulsed,
No data crooned,
No MF tones did play their tunes,
There wasn't a word spoken,
All carrier paths were broken...

And so that's how it all occured,
Microwave horns just nests for birds,
Everything became so absurd,
The day... Bell System... died.

So bye, bye, Ma Bell, why did you die,
We get static from Sprint and echo from MCI,
"Our local calls have us in hock!" We all cry.
Oh Ma Bell why did you have to die?
Why did you have to die?



T A P
TECHNOLOGICAL ASSISTANCE PROGRAM
Room 603, 147 West 42 St, New York City, 10036

Back Issues are $1 each. Issue #50 is $1.50.
Subscriptions - 10 issues per year - $10.
Foreign Air Mail - $13 in Money Order drawn on a US Bank. Sample - 3 International Reply Coupons
Corporate Subscriptions $30 in US, $35 Outside

The Underground Newsletter for the Communications Revolution.

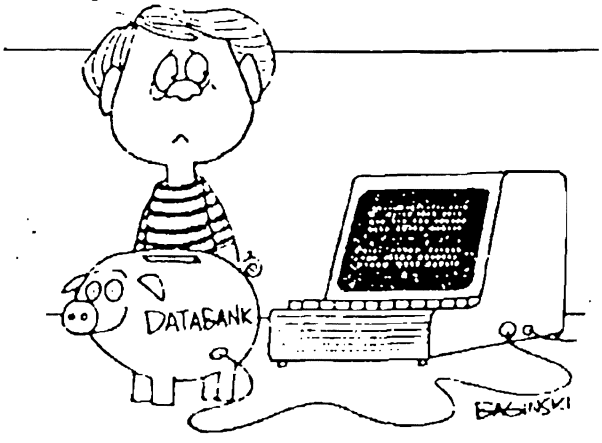
PUBLISHED FOR INFORMATIONAL PURPOSES ONLY SINCE 1971

TAP
Spring 1984 - #91

Managing Editor.....Cheshire Catalyst

Associate Editor.....Tuc
Associate Editor.....BIOC Agent 003

Printing.....Mr. Holmes



Thanks to Mr. Holmes of Baker Street for printing this issue