April 1994

FOCUS

The Magazine of the North American Data General Users Group

Good locks make good neighbors

User-access management with DG/UX

In Focus

Protecting data with cryptography
Network disaster planning

Plus

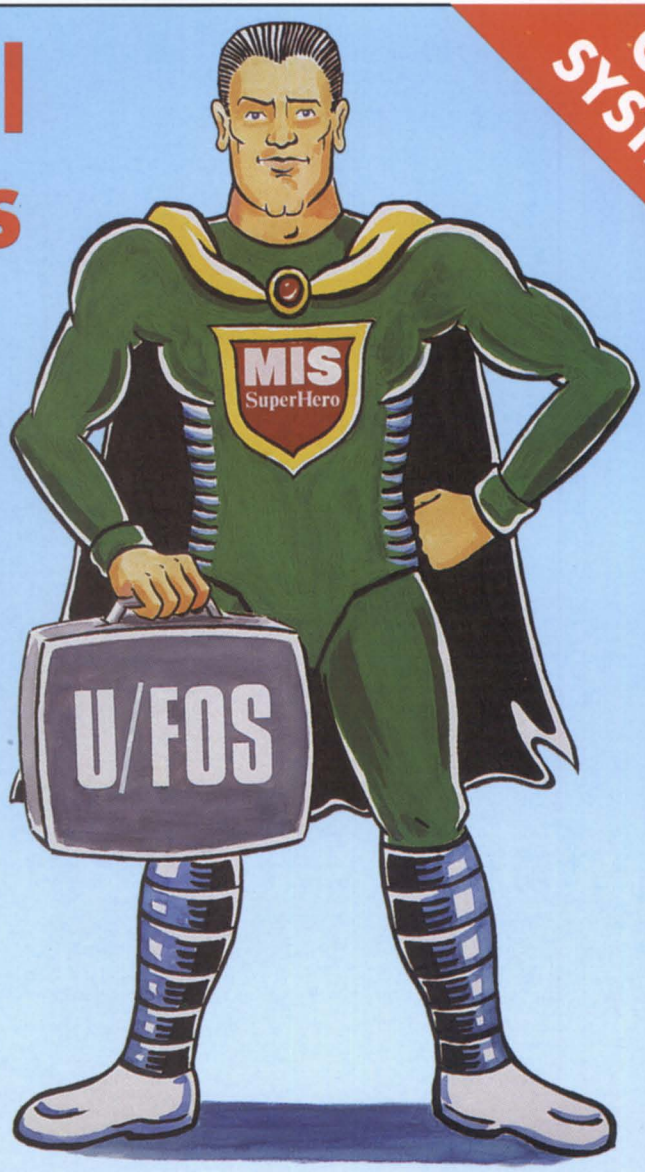
More about the Internet
Managing your (data) relationships

Bulk Rate
U.S. Postage
Paid
Permit No. 38
Fulton, MO

Attention all INFOS® users

OPEN SYSTEMS

Become an MIS SuperHero with AIM™ Automated INFOS Migration



Based on U/FOS™, the first UNIX implementation of INFOS, the Transoft AIM products and supporting consultancy give you – for the first time ever – a smooth, rapid and cost-effective migration route to a choice of major Open Systems platforms.

The AIM product set

U/FOS: INFOS on UNIX:
- full INFOS functionality
- automatic data migration
- added functionality and better utilities.

UAC: U/FOS Access Converter:
- converts INFOS I/O statements to U/FOS I/O calls.

UCC: Universal COBOL Converter:
- converts other AOS/VS COBOL code
- to ANSI-standard ACUCOBOL or Micro Focus COBOL.

APIs for Fortran and C

The same – only much better

Better database management, better reporting, better COBOL development environment... U/FOS gives you powerful additional features, including improved data compression and checkpointing. We are also adding RDBMS-level data integrity and recovery, plus SQL reporting using our proven U/SQL technology. COBOL users also benefit from the modern, more powerful development environments of ACUCOBOL and Micro Focus COBOL.

Transoft – the low risk option

Ours is the low risk solution, in terms of both the company and the technology. Transoft is an established, profitable, growth company. It commenced trading in 1987 and revenue and profits have increased every year since. With seven years' experience, Transoft has unrivalled migration expertise and is a leading international supplier of Open Systems tools to the Data General community. With our products and methodology you eleminate the enormous risks, as well as the costs, of re-engineering.

Largest team

Transoft has the largest team in the world dedicated full time to migrating *your* INFOS applications to *a choice* of Open Systems.

Benefits and savings – now

Why wait? Get the financial and operational benefits of this Open Systems solution now.

Don't delay, contact us today:
TRANSOFT INC, 1899 Powers Ferry Road, Suite 420, Marietta, GA 30067, USA.
Tel: (404) 933 1965 Fax: (404) 933 3464
TRANSOFT LTD, Nash House, Datchet Road, Slough, SL3 7LR, England.
Tel: 0753 692332 (Int + 44 753 692332)
Fax: 0753 694251 (Int + 44 753 694251)

TRANSOFT™

Portability & Productivity

MV TO UNIX MIGRATION

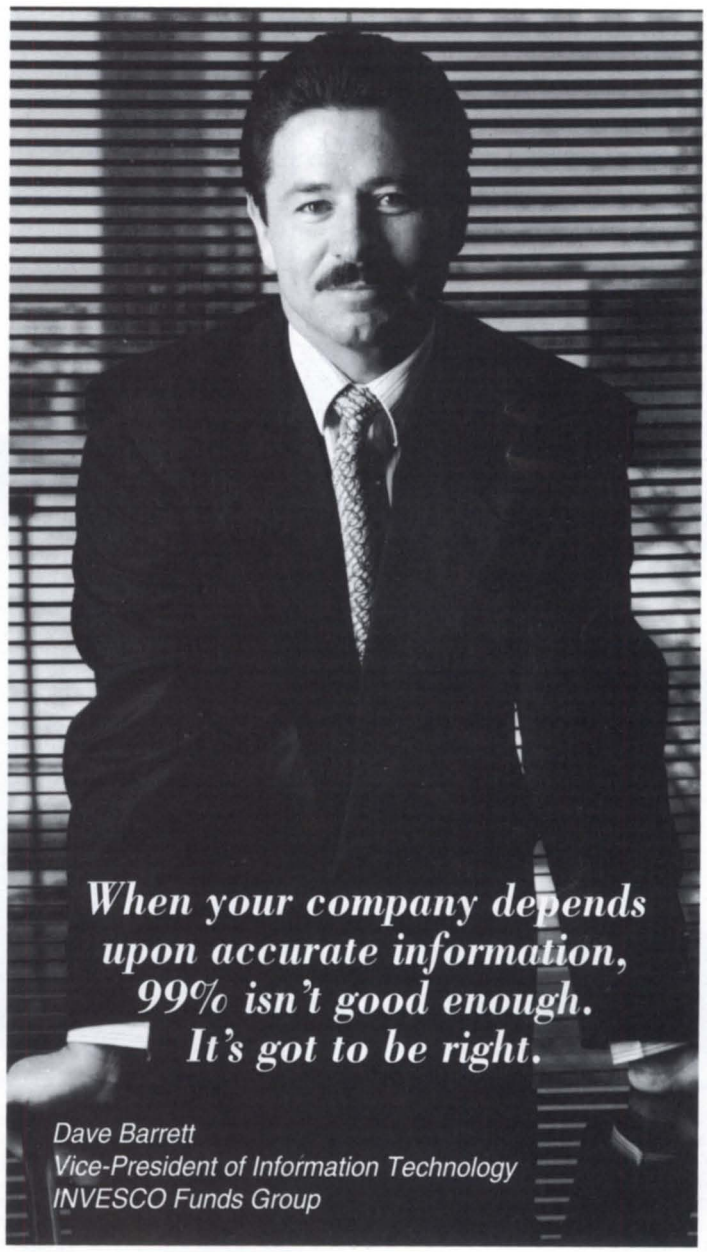
Real People, Real Applications, No Cartoons.

As one of America's highest rated and fastest growing mutual fund groups, INVESCO Funds Group manages more than $10 billion in assets for its customers. The company processes thousands of customer transactions every hour. With strict regulatory oversight, it's got to be right.

"Our proprietary MV system couldn't keep pace with our growth. We needed a scalable UNIX system," said Dave Barrett, Vice President of Information Technology. To provide the quickest, most cost-effective migration, INVESCO chose Wild Hare Computer Systems. "Wild Hare's software allowed us to run existing applications as-is under UNIX on a six-processor symmetric multiprocessor. Our system performance improved dramatically. Our night processing, which previously took eight to twelve hours, now takes only two to three."

A Total Project Approach

"Wild Hare's project approach gave us confidence that the migration would be successful. The company's staff worked closely with ours every step of the way – in the planning, migration, and testing. When you're dealing with other people's money and stringent regulatory rules, testing must be rigorous. I would characterize the project as very successful, and I think the whole INVESCO organization would agree."



wild hare
COMPUTER SYSTEMS INC.

P.O. Box 3581
6595 O'Dell Place, Suite M
Boulder, CO 80301
303/530-2221
Fax: 303/530-9637

To find out how Wild Hare can help you get DG COBOL migrations right, call us at (303)530-2221.

Circle 16 on reader service card.

FOCUS

The Magazine of the North American Data General Users Group

Cover design by John Houser

FOCUS, the Magazine of the North American Data General Users Group (ISSN 0883-8194) is the official publication of the North American Data General Users Group (NADGUG) in cooperation with Turnkey Publishing.

Editorial and business offices are at P.O. Box 200549, Austin, TX 78720, phone 512/335-2286. NADGUG headquarters are located at NADGUG, c/o Danieli & O'Keefe Associates, Inc., Chiswick Park, 490 Boston Post Rd., Sudbury, MA 01776, phone 508/443-3330.

FOCUS, the Magazine of the North American Data General Users Group is distributed to members of the North American Data General Users Group. Membership fees are $60 per person ($110 outside North America). A one-year (12 issues) subscription to *FOCUS, the Magazine of the North American Data General Users Group*, costs $48. For memberships and subscriptions outside the U.S., add $50 to defray the cost of mailing.

The cost of single copies is $4. Requests to replace missing issues free of charge are honored only up to six months after date of issue. Send request to *FOCUS, the Magazine of the North American Data General Users Group*, c/o Turnkey Publishing.

NADGUG is an independent association of computer users; it is not affiliated with Data General Corporation, nor does it represent the policies or opinions of Data General Corporation. The views expressed herein are the opinions of the authors, and do not necessarily represent the policies or opinions of NADGUG or of Turnkey Publishing, Inc.

Advertisements in *FOCUS, the Magazine of the North American Data General Users Group* do not constitute an endorsement of the advertised products by NADGUG or Turnkey Publishing, Inc.

Volume 10, Issue 4.

NORTH AMERICAN DATA GENERAL USERS GROUP

AViiON and Data General

A five year open systems success story!

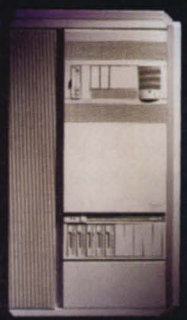
The AViiON® success story began five years ago with an open systems vision. Today, AViiON servers, storage products and services are a global best seller with a more than $1 billion installed customer base.

And our customers keep giving AViiON rave reviews. For two years running, AViiON has been voted the No.1 RISC server for customer satisfaction by Computerworld readers,[1] beating IBM, SUN, Hewlett-Packard and Digital in everything from reliability to value.

The AViiON success story also includes a dramatically expanding customer base. A recent IDC report found AViiON to be the leading platform in the U.S. medium-scale UNIX systems market in 1992.[2] And our CLARiiON™ open storage system has won praise as the fastest, and most flexible, hardware-based RAID system.[3] To make this a real page-turner, we've added over 3,000 software applications and a full suite of services for a complete open enterprise solution.

What's the next chapter in the AViiON success story?
To see for yourself,
call 1-800-DATA GEN

Data General
The Open Systems Experts



COMPUTERWORLD
BUYERS' SATISFACTION SCORECARD
HIGHEST RANKING PRODUCT
1993, 1994

1. "The CW Guide to Servers," Computerworld, March 22, 1993 and "The CW Guide to Servers and Superservers," Computerworld, January 31, 1994.
2. International Data Corporation, "Data General's Ascent in the UNIX Market," October, 1993
3. "Clash of the Drive Arrays," PC Week, October 11, 1993

Circle 2 on reader service card.

Frank Perry

Confessions of a user group 'junkie'

I would like to thank all of you for your many expressions of concern about my health since the NADGUG 93 conference in Atlanta. This was the first conference I missed in quite a few years, and I really wanted to join you. But the "Old Ticker" said NO! The many items from conference exhibits that were forwarded to me have been very interesting and useful. Thank you to Jan Grossman and the rest of the NADGUG board for your efforts in collecting them. To bring you up to speed, I'm feeling better and currently undergoing rehabilitation. And I plan to see you all in Nashville for NADGUG 94.

I've been quite deeply involved in user groups of various kinds since college. My first career involvement with computers was when the State of Rhode Island got an IBM 1620 in 1962 for supporting the public works engineering function. We belonged then to the Highway Engineering Exchange Program (HEEP), which consisted of state highway departments that wanted to exchange programs and ideas.

In those days, 48 out of the 50 state highway departments had IBM 1620 computers, so we were able to exchange programs directly. Without this type of association, it would have taken months for us to become productive. As it worked out, I drove to the MIT Civil Engineering Systems Lab one afternoon and returned with COGO and DTM, two programs that enabled us to be fully productive within just five days after the computer was installed.

Those were the days of bundled software. For you newer people: the machine came completely equipped with operating systems and software at no additional cost, and the manufacturer developed and supplied (free) many types of system applications. There were ease-of-use questions and so forth, but it was free and . . . Next we joined the IBM 1620 Users Group (later COMMON), which maintained an IBM-supported library of user-contributed programs.

All three of these groups figured prominently in providing us with information and assistance to continue growing our applications and determining our future directions. So after my career came full circle and I was back in data processing with Data General equipment, I was open to my salesman's suggestion that we begin a regional user group. I'd been receiving this little pamphlet that indicated there was a DG user group, but that was all I knew.

We were successful in forming what became the Southeastern New England Data General Users Group. Then, as president of the local group, I received an invitation to the spring board meeting of NADGUG in Boston, and the rest is history: audit committee chair, treasurer, vice president, president, planning committee chair, membership committee chair, and into the future.

The real purpose of my story is to try to convince many of you of the real value of belonging to a user group. None of us are capable of doing everything ourselves, and I have never believed in "re-inventing the wheel." Participation in a user group such as NADGUG gives us the opportunity to network with our peers, to meet people who have traveled the same road we are starting down. And it's not always the case of the big helping the small (although there's some level of moral responsibility there); small installations often do some significant, trendsetting developments.

We should never cease learning, and we must always be open to all sources of information. So join NADGUG! Call 800/253-3902. Δ

__Frank Perry__ is chairman of NADGUG's Membership Committee.

FOCUS
The Magazine of the North American Data General Users Group

If you are serious about moving to Open Systems, you should know

Zortec has Been Moving AOS Users to AViiONs for Five Years!

You've seen the articles and the ads about AOS to AViiON migration. The February issue of FOCUS Magazine contained several of them. They talk about "pains and gains" of migration. They focus on "simple, safe options".

Well, at Zortec, we're flattered that so many of the ideas that we've been stressing for years are being recognized by others. We've been in the migration business over five years, and we learned many of these lessons long ago. Many different organizations have migrated to Open Systems with technologies from Zortec over the years.

"In 1990, we migrated our first application, for durable goods management, from AOS to AViiON. It took only three months, including training."
- Greg Shaw, Alpha Omega, DG VAR

Why did these organizations choose Zortec? With our solution, they preserved their investment in existing software and avoided retraining their users. Their migration was accomplished in a short, predictable time frame.

But there's much more to the story. COBOL-to-COBOL and BASIC-to-BASIC translators and emulators (like those you've read about) offer many of these same benefits. The Zortec solution offers much more.

There are two major problems with standard translators and emulators: (1) They do nothing to reduce your code maintenance costs. That means 80% or more of your programming costs are not affected or reduced during your move to Open Systems. (2) COBOL and BASIC are simply not the most effective tools for taking advantage of new technologies in Open Systems - things like relational databases, client-server computing, and advanced user interfaces. **Your company may need these technologies to stay competitive.**

The Zortec migration solution addresses all of these problems. We migrate your existing code to System Z, our advanced 4GL and Rapid Application Developer. With System Z, your software is far easier to maintain and enhance, and new systems can be produced in a fraction of the time needed with COBOL or BASIC. Yet the resulting software runs as fast as COBOL or BASIC equivalents, and System Z's ability to accept COBOL syntax in-line means you can code the most complicated procedural logic without resorting to any other language. And System Z's advanced features offer you transparent access to the latest Open Systems technologies such as client-server and relational databases.

Most importantly, we've been doing this for years. We have experienced migration specialists and highly automated tools. We have a stack of success stories from companies who have made the transition from DG AOS to Open Systems, and more coming through each month. We've been featured in articles in DG-oriented publications (see the list at bottom left).

FOCUS Magazine, September 1991
"The 4GL Philosophy"

DG Review, April 1992
"4GL Express"

FOCUS Magazine, May 1992
"Downsizing with a 4GL"

(If you would like reprints of the above articles, please call us. We would be pleased to send them to you.)

Now and Later

Not ready to migrate yet? There's another option you should know about. You probably will need to migrate eventually, and you can position yourself to make the migration almost painless - and pick up tremendous benefits in the bargain.

"After converting our software from BASIC to Z on the MV, we changed over to the AViiON in a weekend. There was minimal impact on our day-to-day operations." - Scott Goldman, Eltman, Eltman, & Cooper, DG user

We call it our **Now and Later** program. Since System Z is available for AOS as well as the AViiON, you can start using 4GL technology on your MV system right now. That means quicker production of new software and dramatically lower costs in software maintenance. And since the code produced in System Z will run **unchanged** on both AOS and the AViiON, when the time comes you can move to Open Systems in as little as a weekend. (If you doubt that, call us for case studies.)

The Bottom Line

The solution you choose for migration to Open Systems is one of the most important decisions you will ever make for your company. Choose one with the technologies you want and the track record you need. We've got both. Call us for more information.

Zortec, Inc.
1321 Murfreesboro Road
Nashville, TN 37217
(615) 361-7000
FAX - (615) 361-3800

ZORTEC

The latest products for Data General systems

Automated CEO conversion

MV AV PC

Salina, KS—Eagle Software's CABINET_CONVERTER utility program now supports file transfers from CEO to Apple's System 7 for Macintosh and Wordperfect 6.0.

CABINET_CONVERTER automates conversion of CEO drawers, folders, and documents to other platforms, converting CEO files to MS-DOS, Macintosh, and Unix.

Minimum program hardware requirements: Any Data General Eclipse MV computer running the AOS/VS or AOS/VS II operating systems, revision 2.00 CEO or later, with 700 free disk blocks for installation and 1 MB of main memory. The number of documents a company needs to convert determine pricing.

Eagle Software, Inc., *123 Indiana Avenue, P.O. Box 16, Salina, KS 67402-0016; 913/823-7257.*

E-mail made easier

MV AV

Pittsburgh, PA—Universal Data Corporation's new version 1.60 of EZ/Mail offers several productivity enhancements, including:

- Group scheduling with calendar memo updating
- Enhanced e-mail processing
- Extended productivity toolset
- Calendar and inbox resource sharing
- Inbox wastebasket with janitor.

EZ/Mail uses CQCS, the popular fourth-generation language (4GL) from Cyberscience Corporation, and is available for a variety of hardware platforms, including Data General's Eclipse MV family, Aviion series of workstations and servers, and MS-DOS machines.

Universal Data Corporation, *P.O. Box 5826, Pittsburgh, PA 15209; 412/364-9909.*

Port plethora

AV

Nashville, TN—Chase Research announced IORACK, a rack-mount terminal/communications server for Unix and TCP/IP-based systems.

IORACK provides 8 or 16 RJ45 asynchronous ports for connecting modems, terminals, printers, or data-acquisition

Continued on page 33

BUY ★ SELL ★ TRADE

CHECK OUT

OUR MILLION DOLLAR INVENTORY

- MV SERIES UPGRADES
- UNIX & PC BASED SOLUTIONS
- NOVA/ECLIPSE SPARES
- COMPATIBLE PERIPHERALS
- ADD-ON COMMUNICATION GEAR
- DISKS, TAPES, MEMORY, PROCESSORS

MONITOR & PRINTER REPAIR

WE STOCK ODD PIECES
THAT OTHERS DON'T CARRY!

CALL 800 462 CEII (2344)

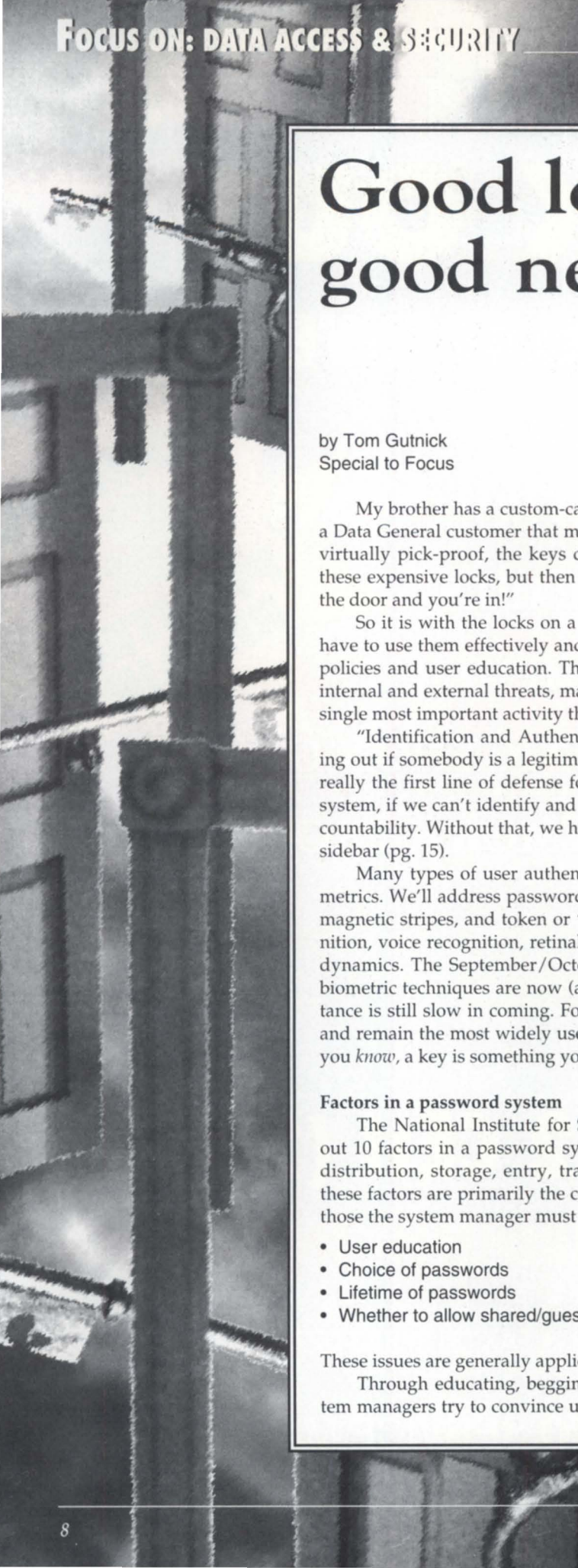
COMPUTER ENGINEERING INT'L. INC.

2231 STAR COURT • P.O. BOX 81755
ROCHESTER, MI 48308 • FAX (313) 853-0775
IN MICHIGAN (313) 853-0770

OUR COMMITMENT TO SERVICE MAKES IT
SEEM LIKE WE ARE RIGHT NEXT DOOR

MasterCard VISA

Circle 8 on reader service card.



Good locks make good neighbors

SYNOPSIS

Improve your user-access management with features available under DG/UX.

by Tom Gutnick
Special to Focus

My brother has a custom-carpentry business. Recently I was telling him about my visit to a Data General customer that manufactures some of the best locks in the world. The locks are virtually pick-proof, the keys difficult to duplicate. But he was unimpressed. "People buy these expensive locks, but then they put the door into a flimsy doorframe. One good kick to the door and you're in!"

So it is with the locks on a computer system. You need good software controls, but you have to use them effectively and in the context of a secure overall environment, with security policies and user education. The security-conscious system manager faces many challenges: internal and external threats, malicious *and* unintentional. But controlling system access is the single most important activity the manager can take to minimize risks.

"Identification and Authentication" is the security practitioner's big mouthful for figuring out if somebody is a legitimate user—in other words, username/password validation. It's really the first line of defense for any multi-user system. If we can't control who's using the system, if we can't identify and authenticate users effectively, then we have no individual accountability. Without that, we have no effective security. For references on this subject, see the sidebar (pg. 15).

Many types of user authentication exist, including passwords, physical "keys" and biometrics. We'll address passwords later in this article. *Physical keys* include badges, cards with magnetic stripes, and token or "smart" cards. *Biometric* techniques include fingerprint recognition, voice recognition, retinal-pattern scanning, signature dynamics, and password typing dynamics. The September/October 1993 issue of *InfoSecurity News* took the position that biometric techniques are now (after years of hype) technically viable. But marketplace acceptance is still slow in coming. For the time being, passwords are still the easiest to implement and remain the most widely used. (To keep straight the differences: a password is something you *know*, a key is something you *have*, and a biometric is something you *are*.)

Factors in a password system

The National Institute for Standards and Technology publication *Password Usage* spells out 10 factors in a password system: composition, length range, lifetime, source, ownership, distribution, storage, entry, transmission, and authentication period. Fortunately, most of these factors are primarily the concern of computer system designers. This article will stick to those the system manager must consider. Log-in issues facing the system manager include:

- User education
- Choice of passwords
- Lifetime of passwords
- Whether to allow shared/guest accounts
- Changing default passwords
- Minimizing concurrent log-ins
- Console line controls.

These issues are generally applicable to both the Generic and Trusted versions of DG/UX.

Through educating, begging, pleading, cajoling, threatening, and thumbscrews, we system managers try to convince users to log off when leaving their terminals; to use good pass-

words; to *not* share their passwords with others. What's often lacking is a specific security policy to remind users of their responsibility to protect the organization's assets—including intangible information assets. *Password Usage* states, "Users should understand their responsibility to keep passwords private and to report changes in their user status, security violations, etc. To assure security awareness among the user population, it is recommended that each user be required to sign a statement to acknowledge understanding these responsibilities." What kind of security policies do ***you*** enforce?

What makes a good password? One that's easy to remember and hard to guess. And why are unguessable passwords so important? Partly to make it more difficult for a "shoulder surfer" to watch you log in. But also keep in mind that some of the most spectacular hacking incidents, including the infamous Internet Worm as well as many little-publicized incidents, have succeeded at least partly because of successful password cracking. When Unix was originally designed, such "dictionary attacks" were difficult because of the large amount of computing resources needed. But today's computers are many orders of magnitude faster; dictionary attacks are a real threat.

So avoid the obvious. Don't use your middle name. Or your spouse's name, your cat's name, or your car's tag number. Longer passwords tend to be better than shorter ones. Although NIST requires passwords to be at least four characters long, DG/UX requires a minimum of six. A rich character set—mixing alphabetic, numeric, and punctuation characters—is also desirable. DG/UX allows all printable characters to be used, and requires that a password contain at least two alphabetic characters and at least one non-alphabetic character. Remember also that DG/UX passwords are case-sensitive. Mix the case and improve your password!

How often should users be forced to change their passwords? The longer you keep a password, the greater the

Figure 1: Minimizing concurrent log-ins

```
# shell code to inhibit concurrent
log-ins
# add to /etc/profile or $HOME/.profile
TRAP "" 2 3    # Disable ^C interrupts
MAX_LOGINS=1   # Set as appropriate
WHO=`who am i | cut -f1 -d" "`
HOW_MANY=`who | grep "^$WHO " | wc -l`
if [ "$HOW_MANY" -gt "$MAX_LOGINS" ]
then
      echo "Too many sessions ...
sorry"
      exit 0
fi
```

D470C D463 D430C D413 W460 VT320 VT100 TEK4010

SVGA XGA VGA MCGA EGA CGA MDA COMPATIBLES PS/2 AT PC

TEXT BINARY XMODEM YMODEM KERMIT DOS OS/2 WINDOWS DESQVIEW

Check out EMU/470 Version 5.0!

Rhintek now provides complete emulation for all current DG Dasher Terminals.

NEW! ❑ Complete D463 Emulation, including: Double high / double wide characters; Selectable 25th line; Downloadable function keys; Tektronix emulation; UNIX mode.

NEW! ❑ D430C Emulation

❑ VT Emulation for DEC, UNIX, and AViiON

❑ PC/TCP Kernel Interface

❑ Scroll back buffer

❑ Network Support

❑ 190+ Macro Keys

❑ Compressed Mode

❑ Built-In Diagnostics

❑ Command Language

❑ Script Files

❑ International Keyboards

❑ Code Pages 850, 437

❑ File Transfers

❑ Complete Printer Support

❑ Auto Dial, Logon & Logoff

Very, Very fast!

EMU/470

DG Color Graphics Terminal Emulation for IBM Micros

Then call 1-800-234-4546 to get your own copy of Rhintek's EMU/470, Version 5.0.

Rhintek offers products spanning the entire Dasher Terminal Line, priced from $95 to $249. We offer volume discounts and unlimited free technical support. Call us and we'll FAX the Facts! Your complete satisfaction is always guaranteed.

Rhintek, Inc.
Computer Engineering
P.O. Box 220, Columbia, Maryland 21045

Visit us on CompuServe (GO PCVENC); Tech Support 410-730-2575; VISA and MC Accepted

PC/TCP INT14 NACS NASI BAPI NETBIOS TCP/IP NOVELL

Circle 37 on reader service card.

chance of it being compromised. On the other hand, if users are forced to change passwords too often, they're more likely to forget them or be tempted to write them down. It usually makes sense to require privileged users to change passwords more frequently than other users. And the NIST Guideline specifically states that no password should be good for more than one year. I recommend that you establish appropriate password lifetimes for each class of user. Later in this article we'll discuss how you can rely on DG/UX features to manage them.

Figure 2: Modem cable for VDA/VDC connections

1	—>	1
2	—>	3
3	—>	2
4	—>	5
5	—>	4
6	—>	20
7	—>	7
8	—>	8
20	—>	6

Guest/shared accounts

Do you allow shared user accounts on your system? Do you think you should? I generally recommend against this practice because it makes user accountability more difficult. Each user ID should be assigned to one person only. When a user leaves, the ID is *not* re-used. It should be considered a security violation when two or more people know a user ID's password.

Under normal circumstances, a user shouldn't be logged on simultaneously at two or more terminals. Unless the terminals are at the same desk, it means that the password has been shared or a logged-in terminal has been left unattended—either situation should be considered a security policy violation.

It's easy enough for you to prevent this. Figure 1(page 9) is a fragment of a shell script (Bourne or Korn shell), which limits a user's concurrent log-ins. Add this code to the beginning of */etc/profile* (to control all users) or an individual user's *$HOME/.profile*. I won't guarantee that it's bulletproof, but I've tested it on my system. A more robust version would be a daemon written in a high-level language to track log-ins and log-outs for each user.

Console line controls

Proper modem control is essential! Consider what happens without it: Let's say I dial into my system, I log in, and start doing some work. In the absence of proper modem control, if my connection is broken for any reason (I hang up the phone without logging out, or noise on the line causes the modem to disconnect), the system doesn't know I'm no longer there. The next person to dial into the same modem doesn't get prompted for username and password, but ends up in the middle of my session! When proper modem control *is* in place, the system is aware of the disconnect and terminates my process tree, ensuring that the next user goes through proper user authentication.

Proper modem control entails correct setup of hardware *and* software. For connection to an Aviion via a VAC, a standard modem cable is needed—pins 1-8 and 20, all running straight through. For connections through a VDA or a VDC, pins 1-8 and 20 are still needed, but pins 2 and 3 cross over, pins 4 and 5 cross over, and pins 6 and 20 cross over (see Figure 2).

The software setup is just a wee bit more involved. The easiest way is through ***sysadm***, with ***Devices -> Port -> Port Services***. For "TTY Definition Label", specify M9600 for a 9600-baud modem, M1200 for a 1200-baud modem, etc. If you use a label that doesn't start with "M", then you must explicitly use ***stty*** to specify ***-clocal*** and ***hupcl***. In addition, set "Hangup?" to yes, "Connect on carrier?" to no, and "Timeout" to the number of seconds you want to allow the user to respond to the log-in prompt before it disconnects.

Password aging is the process of limiting the lifetime of a password and requiring a user to change it. Under Generic DG/UX, password aging is controlled by part of the user's entry in */etc/passwd*. You can specify that a password expires after some number of weeks, and that it's frozen after it's been changed (that is, it can't be changed) for some other number of weeks. The rationale behind password freezing: When I'm forced to change my

password, I might be tempted to change it right back to its previous value. But when it's frozen I can't do that; by the time I *can* change it, presumably I will have gotten used to my new password and I'll no longer want to change it back. See Figure 3 for a description of the password aging entry in */etc/passwd.*

You can deal with password aging for individual users through ***sysadm, user -> login account -> add/modify.*** But if you want to enable aging for a large number of existing accounts, it's probably easier to use ***vi*** or ***sed*** to make mass changes to */etc/passwd.*

Stronger locks with Trusted DG/UX

Trusted DG/UX is upwardly compatible with Generic DG/UX, but adds features to satisfy requirements for commercial security. (Trusted DG/UX also meets the federal government's criteria for evaluating trusted computer systems, at the C2 and B1 levels.) In fact, my recommendation is that if you are running any kind of production operation on an Aviion, you should consider running Trusted DG/UX so that you'll have the extra security features.

With the C2 option, Trusted DG/UX has three main areas of difference compared to Generic DG/UX: 1) Identification ad Authentication; 2) Discretionary Access Control; and 3) Audit. The latter two areas are beyond the scope of this article.

The idea behind the Trusted I&A is really the same as with Generic DG/UX: "Who are you? Prove it!" But the Trusted version provides even more control and flexibility than Generic DG/UX. Using a service-based model, DG/UX allows us to identify each of the different ways a user can gain access to the system as a separate service (such as ***login, ftp,*** etc.). We can control the different locations from which a user can access the system, and different times during which the user can access the system with a particular device. The password can depend on the particular service, and we can specify different audit masks depending on the service.

At the heart of this is something called a "session monitor," which is a part of Trusted DG/UX and mediates

Figure 3 notes:

2) If M and m equal zero (i.e., "."), the user is forced to change the password at next login. No additional aging is done.

3) If m > M, only the superuser can change the password.

4) The week of last change is encoded as a two-digit number in base 64, using the codes shown in note 1 above; this number is a scalar, which represents the number of weeks since the beginning of 1970. In the example shown above, FH = 17 * 64 + 19 = 1,107 weeks, or the 35th week of 1993. (In fact, I changed my password on 24 August 1993.)

Figure 3: Aging data stored in /etc/passwd

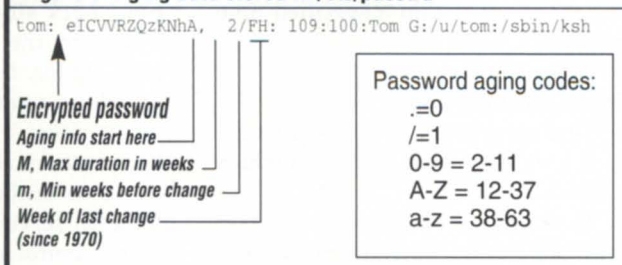


Figure 4: Service-based access model

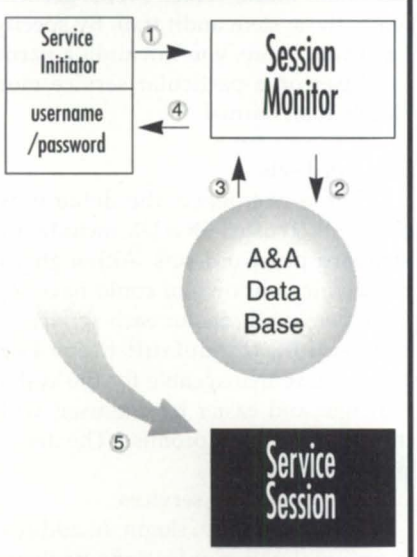


Figure 4 notes:

1) User requests a service (such as login). The service initiator gets the username and password, and passes this information, along with the service, location, and time to the Session Monitor.

2) The Session Monitor checks against A&A data base.

3) Assuming a match, the Session Monitor gets the attributes assigned for the requested service session.

4) The Session Monitor passes these attributes, plus permission to access the service, to the service initiator.

5) The login service session is started for the user.

all requests to create a session (see Figure 4).

Under Trusted DG/UX, there are several components to the information used to control log-ins, including the user account itself, the user authorizations, and the user's password sets. We'll look at each of these.

Identity

User account: The account defines the overall identify and runtime characteristics of a user. ***Authentication ID:*** A number, usually greater than 100, which should be unique to each user. Used by the system for audit trails. It's easiest to just let sysadm provide default values. ***Group memberships:*** Primary and supplementary group memberships, which are used in checking file permissions.

Runtime characteristics

Home directory: The user's initial working directory, from which files such as *.profile* and *.mwmrc* are executed. ***Root directory:*** The highest file-system directory the user can access. ***Execution priority.***

Shell: The user's initial shell—usually Bourne, C, or Korn shell. ***Service authorizations:*** Which services (login, xdm, telnet, fop, rlogin, etc.) the user is authorized to use.

Account aging

Lifetime: The maximum lifetime of the account, after which the account is automatically disabled. This is especially handy when creating accounts for temporary personnel—instead of having to remember to lock them out at the end of their terms, you can set up the

accounts to automatically expire at the appropriate time. As with all the time fields associated with user accounts, you can specify this field in days, hours, minutes, and seconds. (I learned the hard way that the default account lifetime is 366 days; exactly one year after I had set up my workstation, I couldn't log in! Now I specify a longer lifetime.) ***Idle time allowed:*** The account would be disabled automatically if the user does not use it within a specified time period.

History information

Last used: When was the last time this account was used, and from which location?

Last denied: When was the last time that a failed log-in attempt occured with this account, and from which location? ***Lock status:*** The account can be locked by the system manager, to inhibit log-ins. Handy when you need to disable an account temporarily.

User authorizations

User authorizations are specified for each service, and allow additional access control and auditing.

Time and location restrictions: A particular user may not be allowed to access the system between midnight and 5 a.m., nor on weekends, for example. Similarly, a user may be restricted to coming in from specified workstations or console lines only.

Audit mask: Which events get written to the system audit trail. By specifying a value here, you can audit a particular user on a particular service more closely than normal.

Password sets

For convenience, the defaults we ship with Trusted DG/UX include four standard password sets. Although you can define your own or could have separate password sets for each service authorization, the default helps keep things more manageable for the system manager and easier for the user, without significant compromise. The default password sets are:

Local: login, xdm services

Remote: telnet, ftp, rlogin. In addition, if optional communications packages have been licensed, ftam, pad, dni, vtp.

su: for the su ("switch username") service only.

Public: This duplicates what's in ***/etc/password***. It exists in case you choose to boot a non-trusted kernel, and also for ill-behaved applications that access ***/etc/password*** directly instead of doing the proper authentication system calls. The public password set is not considered part of the Trusted Computing Base.

Within each password set, the following information is maintained:

- ***Password value:*** The actual password for using this group of services.
- ***Lock status:*** Whether this password set has been locked.
- ***Aging information:*** (see next section)
- ***Change allowed:*** Is the user allowed

to change the password, or is only the system manager able to do so?

- ***Password failures:*** Lock on how many? How many consecutive log-in failures will cause this password set to be locked?
- ***Password failures, history:*** Current number of consecutive failed log-in attempts.

A user's password goes through many stages. You can change the time intervals for each stage, although the default values are good for many users.

Frozen: The password cannot be changed. Default is 7 days.

Normal: The password can be changed as desired, and no warnings are given. Default 90 days.

Warning: Each time this password is used, the user will receive a warning of when the password will expire. Default 30 days.

Expired: The user must change the password in order to use the service. Refusing to change the password means you won't be granted access to the service. Default is 53 days.

Extinct: It's too late to change the password. You will be denied service!

User authentication references

DEPARTMENT OF DEFENSE PASSWORD MANAGEMENT GUIDELINE ("The Green Book"), National Computer Security Center publication CSC-STD-002-85. Spells out many guidelines for managing systems effectively. Although oriented toward defense and intelligence agencies, the guidelines are useful for commercial sites as well.

PASSWORD USAGE, National Institute for Standards and Technology Federal Information Processing Standards Publication 112, provides guidelines which are binding for federal systems, but also are good recommendations for non-federal sites. You may find this a good source of verbiage in developing your own security policies. Includes the *GREEN BOOK* as an appendix.

UNIX PASSWORD SECURITY—TEN YEAR'S LATER, David C. Feldmeier and Philip R. Karn. The "ten years" is an allusion to a paper by Robert Morris and Ken Thompson in Communications of the ACM.

"FOILING THE CRACKER": A SURVEY OF, AND IMPROVEMENTS TO, PASSWORD SECURITY, Daniel V. Klein. Available via anonymous ftp from ***ftp.sei.cmu.edu*** under ***~/pub/dvk/passwd.****.

Δ

"Why can't I get in?"

As with liberty, the price of a secure system is eternal vigilance. Trusted DG/UX provides a lot of control in how the system is accessed; a corollary is that DG/UX provides many reasons why a user may be unable to log-in. Reasons include:

- Incorrect username
- Account locked
- Account lifetime exceeded
- Account idle time exceeded
- Not authorized for this service
- Not authorized for this time/location
- Nobody authorized for this time/location
- Incorrect password for this service
- Password extinct
- Password locked
- Too many failures

In addition, system administrator actions can cause problems. If some attribute has been altered, it may invalidate the account. For example, if a user's primary group has been removed, log-in will fail.

In all of these cases, the user receives the message, "Login incorrect." We certainly don't want to give a potential malefactor clues that might help him break in. Some of the things a system administrator can do to determine the reasons for a lock-out are:

1) Run ***authck*** to get overall account status.
2) Run ***passwd -q <username>*** to get the aging status of all password sets.
3) Run ***sysadm*** to check for locked password sets.

By now you should appreciate that the system manager has a lot of control over who accesses the system. Generic DG/UX has a strong set of basic security features, and Trusted DG/UX gives you the tools to enforce a security policy effectively on your system. Remind your users that they should treat a password like a toothbrush: Change it frequently. Never share it. Δ

Tom Gutnick is a systems engineering consultant for Data General, specializing in operating system issues. He can be reached at 7927 Jones Branch Drive, Suite 200, McLean, VA 22102; 703/827-9669; Internet: Tom_Gutnick-@dgc.ceo.dg.com.

Protecting data with cryptography

SYNOPSIS

The heart and soul of message security is called "public key encryption." It has been built into products from Lotus, Novell, and Wordperfect. Jim Bidzos, president of RSA Cryptosystems, cites more than 1 million public key user licenses today. The January 31, 1994, issue of *Information Week* claims 3 million. This article explains what a public key cryptosystem is. Part 1 of 2.

by Michael E. Marotta
Special to Focus

Back when the typical Data General environment was a single Eclipse or standalone MV, computer security was mostly a matter of internal controls. The main idea was to keep authorized users from stumbling into unauthorized places. Now that we're running Unix and are connected to the Internet, all that has changed. The first challenge is to keep *unauthorized* users from entering the system. The second (and tougher) challenge is to secure our messages as they travel to and from our sites along the "information superhighway."

Codes and ciphers

A *code* is a pre-arranged set of arbitrary symbols. We could set up a table of meanings like this:

10:21 am	yellow	restaurant	handkerchief
2:00 pm	green	theater	scarf
3:15 pm	red	library	gloves
3:21 pm	blue	zoo	sweater

Then a message that reads: "Thank you for the green gloves." would carry a hidden meaning. Instead of colors and places, of course, we could use numbers, letters, astrological symbols, and so on. Without the *key* or *codebook*, unraveling the message is usually hopeless.

A *cipher* is an orderly transposition or substitution of characters. We could use the ASCII chart as a cipher. With "A=65, B=66,..., Z=91", the word *Focus* becomes "71 79 67 85 83". This kind of secret message is relatively easy to break. Since *E* is the most common letter in English, any message that is simply enciphered will show more symbols for E than any other. There are ways to make a cipher more complex. We could have a table or an array of several columns, and use each cipher in turn. Then, a message like "LEE SEEMS COMPETENT" would have several symbols for the many *E* characters. Ciphers can also be created on the basis of transposition. We can take a message like, "THE GOTHS ARE CHARGING AT MIDNIGHT," and write down every other letter (with the space as a "letter"):

TEGTSAECAGN T MDIG H OH R HRIGA INGT.

Again, the transposition can be more complex.

For computing, ciphers have an inherent advantage over codes. A cipher can be expressed as an algorithm. You can write a program to execute and unravel a cipher. On other hand, a code requires a look-up table. Ciphers, therefore, are the preferred solution in computerized communications.

In 1974 the Department of Commerce announced its desire to implement a Data Encryption Standard (DES). The DES would be used for all nonmilitary government communications, typically bank transfers and other commercial transactions. The Data Encryption Algorithm (DEA), created by IBM, was accepted for this purpose. However, it was accepted only after it was downgraded for simplicity by the National Security Agency (NSA). By 1982 some cracks appeared, at least at the theoretical level. Today, even though it has never been (publicly) broken, the DEA is considered obsolete. The search is on for a newer, better method for safeguarding data in transit.

Public keys

Historically, codes and ciphers have shared a common weakness: the *key*. You can substitute and transpose to any level of complexity, but if the algorithm gets out, your messages will be deciphered in short order. This problem has been attacked by several researchers over the past 20 years. The solutions are called "public key cryptosystems." (***Cryptology*** is the science of secret writing. ***Cryptography*** is the creation of methods of secret writing. ***Cryptanalysis*** is the breaking of codes and ciphers.)

Ralph Merkle was a graduate student at The University of California at Berkeley when he suggested placing the key *in* the message. A long message, such as a bank's daily transactions, consists of a stream of millions of ones and zeros. No subset of this stream is any more meaningful than another. All that's required is to define where the encryption key begins and ends. It could start at bit number 38,493 or bit number 912,745, or wherever. The key could be 87 bits long, or 3,962,521 bits long, or whatever.

At MIT, professor Ronald Rivest and two doctoral candidates (Leonard Adleman and Adi Shamir) took a different approach. Based on the "totient function" discovered by Leonhard Euler (1707-1783), the RSA cryptosystem relies on two

different keys. Both keys are based on long integers of 100 digits or more. One key is published, the other held secret. Anyone who wants to send you a secret message looks up your published key. When you get the message, you use your secret key to decipher it. A 100-digit number can be stored in 100 bytes or less. This is a small chunk of data for a modern computer. Yet the most powerful computer running the most efficient program would require several years to crack this number. The time can be increased to several centuries just by making the cipher key a few digits longer. There isn't enough time in the universe to break a cipher based on a number that can fit into a 1-kilobyte file.

Prime numbers

Not just any number will do, of course. The most secure ciphers rely on prime numbers. A prime number has only itself and 1 as factors. Prime numbers include 17, 23, 57, and 93. However, 12, 51, and 60 are not prime. You can factor 12 down to 6 x 2 or to 4 x 3. And 51 = 17 x 3. The factors of 60 are 2, 3, 4, 5, 6, 10, 12, 15, 20, and 30. In order to find out if a number is prime, just divide it by every number in turn, starting with 3. (We can rule out even numbers: any number that ends in 0, 2, 4, 6, or 8 cannot be prime.) If a number has no remainder after a divide, it is rejected.

The ones that remain are prime. This method is called "The Sieve of Eratosthenes" after the Greek mathematician who discovered it about 250 B.C. Is the number 5,301 prime? You would have to reach 57 times 93 until you found its factors. Of course, 57 and 93 are primes, so they are the lowest possible factors. Note also that 57 and 93 are 2-digit numbers. Their product is a four-digit number. If you multiply two 100-digit prime numbers, you get a number 200 digits long. Prime numbers are important to the RSA system because the Euler totient function rests on "modulo" or "residue" arithmetic. For instance, we say that 1700 hours is 5:00 pm. The formal mathematical statement is "17 mod 12 = 5", or, as we learned in grade school, 17 divided by 12 equals 1, remainder 5.

All of this 100-digit prime number modulo arithmetic takes place at the code level. The users never see it. The system manager seldom needs to be concerned with it. Once the hardware or software is installed, it is as seamless as disk I/O.

The RSA cryptosystem was announced more than 15 years ago. It has been described and defined in papers and at conferences. The algorithm is known and understood. While some theoretically weak keys can be generated for it, it has stood the test of time. The RSA cryptosystem has been selected by Wordperfect, Lotus, Novell, and many other companies for securing data in transit. It is not the only option, however. The federal government has announced two products, Clipper and Tessera, that also provide data security for network communication. In addition, there is an unlicensed version of the RSA algorithm, called PGP, which is extremely popular with Internet users. Since PGP intrudes on the RSA patents, its use is controversial. ***(Next month: issues, threats, and opportunities in data security.)*** Δ

Michael Marotta *is a freelance writer in Fowlerville, Michigan.*

Network disaster planning

SYNOPSIS

Contingency plans will help keep your business running.

by Katherine Jones, Ph.D.
Special to Focus

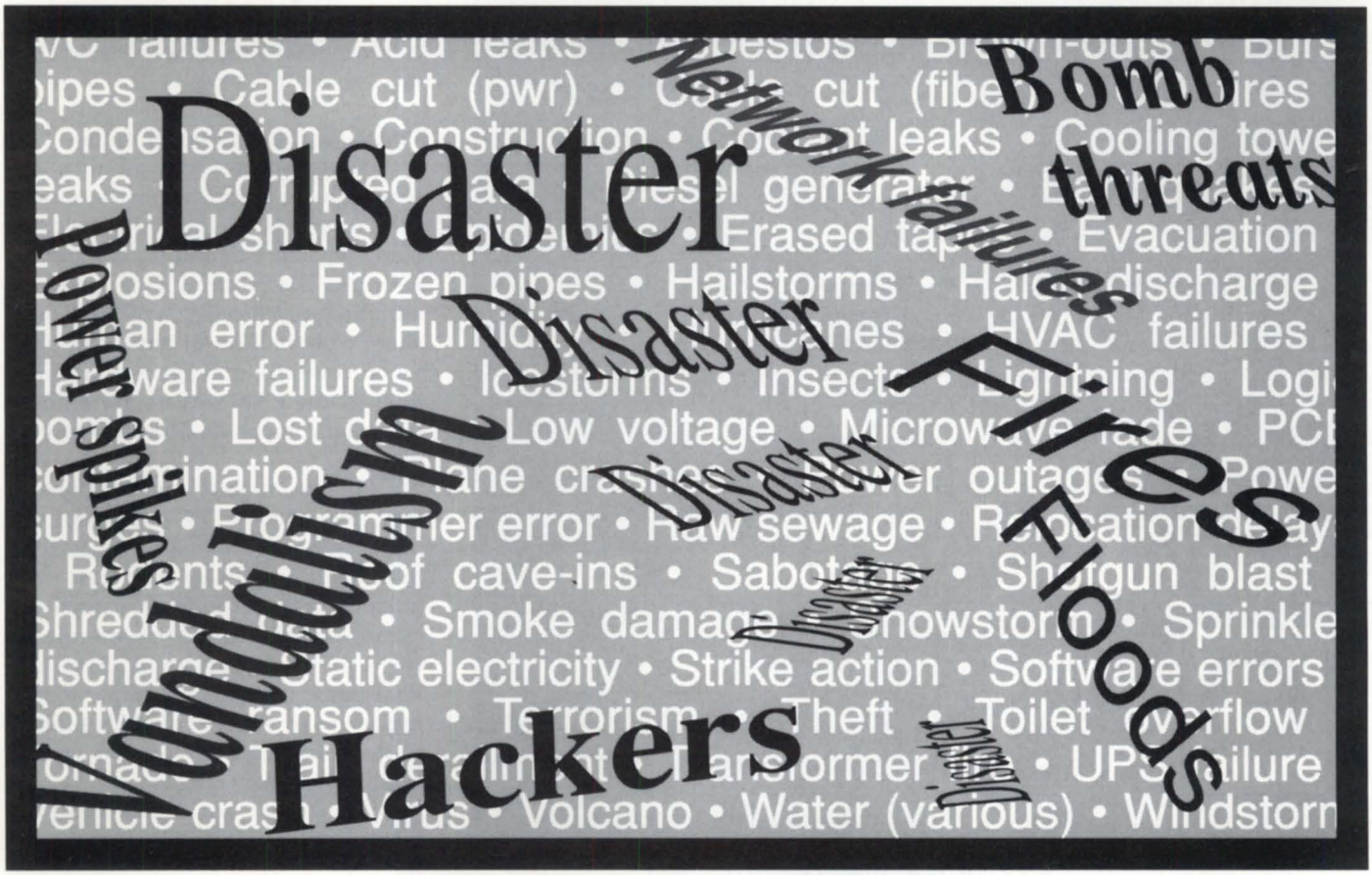
Is your network disaster-ready? In the aftermath of recent hurricanes in the South, fires and earthquakes in California, and floods in the Midwest, it may be time to view the vulnerability of your network sites and create a plan to address "what if?".

Too many network administrators avoid disaster (or more aptly, "contingency") planning, saying it's unnecessary, unfeasible, or undesirable. Most frequently, however, network administrators who lack a network contingency plan cite lack of time to think about developing such a plan as the only reason they do not have one. And when a disaster-recovery plan *is* in place in a company, it is often solely for the mainframe. Too often, no attention is paid to the distributed departmental servers. Self-analysis is necessary in such instances—can you afford the risk of network disruption?

Have you explored your exposure in case of network loss? Analyzing the risk of network "disasters" has to include business input—it is not the probability of network failure you prepare for, it is the eventuality. Think about the small sign on airline seats: "**Fasten Your Seatbelt. Seat cushion may be used as a flotation device.**" The last sentence is part of a disaster-recovery plan! Knowing the effects on your business of network unavailability is important, and helps set priorities in which LANs to restore first or which people to get online most immediately.

Assessing your risk

While some may not think of a network failure as catastrophic, recent events such as the bombing of the World Trade Center in New York City and the California earthquakes certainly gave network and telecommunications administrators reason to pause.



Companies who most successfully avoided negative business impact were those who had a plan for dealing with voice and data communications in the event of total network inaccessibility. These companies had plans that included alternate telephone lines, access to critical data at a remote site, or in some cases a plan that included relocating staff to a temporary site from which to conduct business as usual.

A 1988 survey of mainframe systems managers demonstrated that 80 percent of MIS directors had *no* disaster-recovery plan. And of the 20 percent that had plans, 80 percent of those plans were untested. By June 1993, The Gartner Group reports, some 60 to 70 percent of MIS directors had a disaster-recovery plan (DRP) in place for the mainframe, but fewer than 50 percent test their plans regularly.

While the tangible cost of downtime may be determined by a business (for example, the average cost of downtime in voice communications for 450 members of the *FORTUNE 1000* is $78,000 per hour—adding up to $2.97 million per year per business), the intangible costs may not be considered. Respondents reported that the intangible costs critical to their business included cash-flow interruption, loss of customers, loss of competitive edge, erosion of business image, loss of market share, loss of marketplace confidence, legal or regulatory violation, and loss of investor confidence.

The effect of distribution—positive to business under normal working conditions—can allow risks when the unthinkable, the unexpected, happens. The lack of central control may mean that no plan exists for server access, or at best departmentalization creates fragmented recovery plans. The distributed environment allows not only multiple loss locations, but also multiple threat locations: more sites for hackers or other illicit attempts at accessing data. The increased reliance on PCs for the conduct of mission-critical business can increase security risks.

Protecting the LAN server option

As the business-critical open systems servers are increasingly outside the data center, they are often concomitantly separate from the hot site backup centers. Distributed sites may be administered locally, centrally, or in some combination of both. But even when centrally managed, all too frequently the LAN servers are omitted from the company's disaster recovery plan.

PCs also require consideration. In 1992, $1.4 billion of PC equipment was lost to service. These losses, based on insurance claims, were from theft ($882 million), fire ($119 million), natural disaster ($115 million), power-related ($174 million), and others ($105 million). Some solutions are simple: requiring users to cover their PCs nightly with waterproof covers can guard against water damage.

The dangers for distributed LAN information includes lack of local back-

up or infrequent backups, storing backup data solely on the premise or with employees, and infrequent backups of data bases. The issues to consider are several:

1) Are critical backup data available for each distributed site?
2) How much time is acceptable to restore those systems or the functions those systems serve?
3) What are the personnel impacts?

A California airlines-reservation site created two remote backup sites for both telephone and data access should the primary site be inaccessible. During a recent earthquake, the central site was destroyed and, as planned, the two remote sites received all the diverted business. The only thing they neglected to plan for, however, was the effects of the disaster itself. The two sites were created to handle the load of the original site; in an actual disaster, the increased telephone and hence data-access requirements brought the two backup sites to their knees!

What are LAN recovery options?

A business may have a standalone recovery plan—one in which the corporation can replace or reroute data immediately, regardless of location. Hot spares and mirrored servers provide equipment and redundancy that can alleviate the effects of, for example, fire or water loss. Quick-ship replacement plans from vendors can provide somewhat of an insurance policy; such programs can provide loaners or replacements in one or two days.

Data vaulting allows incremental daily backups over a voice-grade line in unattended mode. Data are compressed, encrypted, and moved to the server. Couriers also pick up backup tapes and transport them to off-site vaults manually. Mobile units offer wireless LAN systems for temporary restoration of service.

Businesses can subscribe to commercially available recovery programs, thus outsourcing either the planning or the total restoration should a catastrophe happen. Such services should be planned for before disaster strikes, however.

Some recovery packages address facility lockouts. These offer the relocation of staff and data into new facilities within 24 hours. Telephones and data lines are all ready for employees to continue work.

Why have a plan?

Some businesses—financial institutions, for example—have federal audit requirements that require approved plans for recovery of data in the event of unexpected disasters. In some cases, corporations with approved contingency plans can receive improved insurance coverage or reduced premiums. The consumer implication of a disaster-recovery plan can be important as well: the ability to guarantee reliability to prospective clients and customers, and the reduction of public awareness when a disaster does occur in that business appears to be conducted as usual.

This in itself can protect against lost revenues. An intangible benefit—peace of mind—can be obtained with the knowledge that a recovery plan is in place, has been tested, and found to work.

Catastrophic failure of business communications can result in serious financial losses. While such disasters are rare, and their uncertainty can make planning difficult, lack of planning can have devastating consequences. Each business that relies on data access should identify its availability requirements and create a plan, *AND TEST IT*, against those requirements. Only by doing so can today's corporations reduce the probability and the amount of loss from a disaster. Δ

***Dr. Katherine Jones** heads Independent Consulting Services of Shrewsbury, Massachusetts, and among other things provides consultancy services on disaster-recovery planning.*

Acquiring good habits

by Katherine Jones, Ph.D.
Special to Focus

As much as it is important to create a network recovery plan, it is equally important to coordinate that plan with other parts of the corporation: the MIS director, the telecommunications director, and the like. Should disaster strike, it may well affect the entire plant.

The network administrator *needs to ascertain what network segments are most crucial:* while every department may clamor for attention, customer service, sales order entry, and financial fund movement may well be more critical than marketing, for example.

Offsite storage for all critical data—mainframe, server, and PC—should be accommodated. And this does not mean backup tapes are located on another floor of the same building as the computers themselves. The backup systems should be modified at the same time as production equipment.

Telephone lists of key personnel need to be kept up to date. In a disaster, getting in touch with people and possibly even moving employees to new locations may be imperative. Hence, a copy of that list has to reside somewhere other than solely in the administrator's desk at work! If employees change telephone numbers frequently, a current list should be kept. Employees who are part of the plan to address disaster at its inception need to practice the roles expected of them. If employees would move from a defunct facility to the hot site and then to a new cold site, that plan should be reviewed with

them. If telephone trees are kept, again, keeping names and numbers current is paramount.

In case the network operations center is inaccessible, the administrator must ensure that all information on all necessary communications equipment is *documented* and *in place* at the hot site. Power and communications lines at that site should be connected to standby equipment and utilities.

Switching and modem facilities need to be tested once installed. Note any specific lines designated as secure, if need be. Passwords, ID codes, etc., should be place at the new environment.

Checklist for planning

- "Who Does What?" list
- Telephone list of key personnel and management
- Contact list of common carriers and power companies to provide emergency backup services
- Recovery priority list
- Hardware configuration
- Software inventory per computer
- Communications gear configurations
- Modem settings
- Autoexec.bat file contents
- Whereabouts of backup tapes
- Automatic routing of main number to alternate location for phone and fax
- Lists of user names, passwords for alternate workstations or PCs
- Security rules for alternate site
- Quick-ship replacement or leasing plan with critical equipment vendors
- Hot spares

Good habits for loss prevention

There are several common-sense steps one should take to prevent loss of data. Some of these include:

- Routine program for daily media back-up.
- Remote off-site storage of backup media over 24 hours old.
- Routine use of computer covers during periods of non-use to protect from accidental discharge of water.
- Routine electrical shutdown of equipment during periods of non-use (electrically active equipment exposed to water may require extensive repair and retesting).
- Inventory listing by type, manufacturer, model and serial numbers, date of purchase, replacement costs, unique configurations.
- Inventory of software including purchased and custom programs.
- Identification of critical data/documents; source and archival documents inventory.
- Location and preservation of vendor warranties, service maintenance policies, third-party service and repair policies.
- Know location and condition of smoke, heat, and water sensor devices.

In addition to planning for disasters, routine precautions taken daily can enhance the likelihood that your site won't be out of operation longer than absolutely necessary. Δ

David Novy

More about the Internet

SYNOPSIS
Learn more about this vast, valuable resource. Get logged in and start exploring.

During just the last month I've received two mailings offering me access to the Internet system from my home computer. Last week (I'm writing this in February) I saw an NBC news program in which viewers were invited to share their opinions either by fax or by mailing replies electronically to an Internet address.

Last month's column addressed Internet access. The subject this month will be Internet functionality. The major Internet functions are:

1) Remote login—***telnet***
2) Moving files—***ftp***
3) Electronic mail
4) Network news
5) Finding software—***archie***
6) Finding someone—***white pages***
7) Internet browsing—***gopher***
8) Searching indexed data bases—***WAIS***
9) Hypertext spanning the Internet—***World Wide Web, or WWW***
10) Other applications

The Internet's remote login application is ***telnet.*** It lets you connect remotely to another computer on the network from your local machine. The connection can be made to a machine in the same room or, if necessary, in a far corner of the world. One of my favorite methods of showing Internet telnet capability is to do a remote login to Tasmania (that's the big island just south of Australia). When you're connected, it's as if you were logged directly into the remote machine. You have access to whatever services the remote machine provides to its local users. Logging into a remote machine is not without inconveniences, however. The most common one is the "erase" key. To determine what key the remote computer uses as the erase key, type in ***stty -a*** and look for the setting after the word "erase". It is usually ***del***, ***^?***, or ***^H***.

del means the delete key; ***^?*** is ***CTRL-?*** (Control-?), and ***^H*** is ***CTRL-H***.

Usually, you can change the erase key setting by typing ***stty erase*** followed by the erase key you want to use. If you can't change the erase key setting on the remote machine, ***stty-a*** at least will tell you what key is being used.

There are many more features to telnet that are beyond the scope of this article. If you understand the functionality of Unix telnet, then you will understand the functionality of Internet telnet. One important telnet feature is the "escape" character. If you type the escape character, your telnet client enters a special command mode. By default, the escape character is *CTRL-]*. It is important not to confuse the telnet escape function with the ***ESC*** key on the keyboard. The escape character to telnet can be any character that you normally *never* want to send to the remote machine. The ***ESC*** key on the keyboard is a special nonprintable character that you *frequently* need to send to remote machines to preface special command sequences.

Moving files—*ftp*

You'll often find interesting information on the Internet that you'll not only want to examine, but get a copy of for yourself. To move a copy of a piece of information from a remote Internet machine to your local machine, use the ***ftp*** tool.

The ***ftp*** tool is named after the application process protocol it uses: the "File Transfer Protocol." As long as both your local *and* remote machines can use the ***ftp*** protocol, *and* you have access to the Internet, you can use ***ftp*** to transfer files. There are often minor differences in ***ftp*** functionality, depending on the local operating system, but the basic commands are the same from machine to machine; ***ftp*** is a complex program because there are many different types of file structures and ways to manipulate files. Different ways of storing files require you to plan for transferring files in a form you can use.

I will not go into great detail about how to log in and browse with ***ftp.*** If you know how to use Unix ***ftp,*** you will feel comfortable using Internet ***ftp.*** The most common problem I have when using ***ftp*** is remembering if the data I'm transferring are in ASCII or binary mode.

In ASCII mode (which should really be called "text mode"), characters transfer as text only; the file-transfer machines try to ensure that the characters transferred have the same meaning on the target computer as they did on the host computer.

In binary transfer mode, the bit sequence of the transferred file is preserved so that the original and the copy are bit-by-bit identical, even if a file containing that bit sequence is meaningless on the destination computer. The default transfer method for ***ftp*** is ASCII. So if you plan to transfer a binary file from one machine to another, you must be sure to tell the ***ftp*** tool that you want to use binary mode transfer procedures. Otherwise, your binary file will be missing several bits.

Thus far, our ***ftp*** discussion applies when you have a username and password on the destination machine. But what if you want to distribute software freely without having to hand out username-and-password combinations?

The answer is ***anonymous ftp.*** It allows users restricted access to a destination machine. Usually, users can only copy files; they cannot install new files or modify files that are already there. And there are strict limits to the files

that may be copied. When using ***anonymous ftp*** you log onto the destination machine using the special login name, ***anonymous***, and use any string as a password. After login, you are transferred to the ***anonymous ftp*** home directory and allowed to access those files that are specifically permitted to anonymous ***ftp***. There are special tricks you can use when using ***ftp*** to reduce the amount of time required for a file transfer, or to copy an entire directory. One of the best tricks is to convert the file or files to a ***tar*** file and then to run ***compress*** on the ***tar*** file. This can reduce the file size by a substantial amount. To recreate the file or files, after they have been transferred, you can run ***uncompress*** on the file and then do a ***tar -xf*** on the uncompressed file.

Electronic mail

Using electronic mail you can converse with any other Internet e-mail user in the world. The communication is generally rapid, it is robust, and it doesn't cost anything extra to send a message. It is said that Internet e-mail was one of the reasons the attempted coup in Russia failed against President Boris Yeltsin. The insurgents took over Russia's television, radio, and phone systems, but they did not take over the Russian Internet system, probably because they didn't know such a system existed. Internet e-mail messages traveled in and out of Russia, allowing Yeltsin's government to retain contact with other parts of Russia and with the outside world. During the recent Los Angeles earthquake, phone communications failed in some places, but the Internet remained online.

You should realize that e-mail has strengths and weaknesses. Security of e-mail systems is usually low. In addition, you might want to avoid statements you could regret later, because your messages can be stored and printed, or even broadcasted. On a telephone, if you have an awkward moment you can claim you were misunderstood. This is not true with an Internet e-mail message, which can be printed and distributed. Another problem with e-mail: the sender's ID can be faked. You may think President Clinton is offering you a cabinet post, when in reality it's just a poor joke.

Using Internet e-mail is similar to using Unix e-mail. It's not spectacular, but it gets the job done. If you want to learn how to use Internet e-mail more fully, I suggest you purchase an Internet "how-to" book.

I hope you find this Internet series to be interesting and helpful, even though it is a bit short on details. What I hope to do is expose you to the Internet and how it works, so you will want to learn more and perhaps obtain your own network account. Δ

David Novy is a technical computer specialist at 3M in St. Paul, Minnesota. He is past chairman of the AOS/VS special interest group, and current chairman of NADGUG's SIG/UX.

Shop Our Million Dollar Data General Inventory And Get "Right-On-Time" Delivery.

· Million dollar inventory of systems, peripherals, parts and equipment · From Nova to MV -- you get "Right-On-Time" delivery · Highly skilled engineers · Valuable assistance, consulting, training and installation · Customer service reps with broad product knowledge · Problem solving advice · All backed by RAVE's 60-day warranty

· Sensible business solutions with significant bottom line value ·

SELL · BUY
LEASE · RENT
Data General &
Compatibles

We Also Sell Sun Microsystems

Sun Microsystems Computer Corporation
Remanufactured Products Reseller

Announcing -
RAVE FINANCIAL SERVICES, INC.

- Complete In-House Financing
- Custom Leasing Packages
- Long or Short Term Programs
- Rentals Available

Rave Computer Association, Inc.

RIDE THE WAVE · RAVE COMPUTER ASSOCIATION, INC. · SAVE WITH RAVE

36960 Metro Court
Sterling Heights, MI 48312
(810) 939-8230 / Fax: (810) 939-7431
International Office
(516) 929-5000 / Fax: (516) 929-5007
1-800-966-7283

Circle 36 on reader service card.

Kim Medlin

Managing your (data) relationships

SYNOPSIS

The author concludes a discussion of the data-modeling process using ERwin/SQL. Part 2 of 2.

One-to-many relationships

Besides order entity, you must define an entity that represents line items for each order. Here we have encountered our first one-to-many relationship. The business rule represented with this relationship can be stated as:

For each order, there must be at least one line item.

Figure 1 shows the ERD with a new entity representing line items.

Notice that the ***order_item*** entity has rounded corners while the order entity has square corners. The order entity is called an *independent entity* because it depends on no other entity for its identification. All you need to know to identify a specific order is the order number, which isn't stored in any other entity. On the other hand, the ***order_item*** entity is called a *dependent entity* because it does depend on another entity for its identification. You must know both the order number and the item number to uniquely identify an ***order_item*** record. The ***order_num*** is obviously stored in another entity, specifically the order entity. The "(FK)" notation in the ***order_item*** entity indicates that the ***order_num*** is a foreign key. That is, the ***order_num*** field is a primary key in another entity, namely, the order entity.

Relationships between entities are indicated by lines, verb phrases, and various symbols. The relationship that associates the order and ***order_item*** entities is indicated by a solid line labeled

Figure 1: Parent and child entities

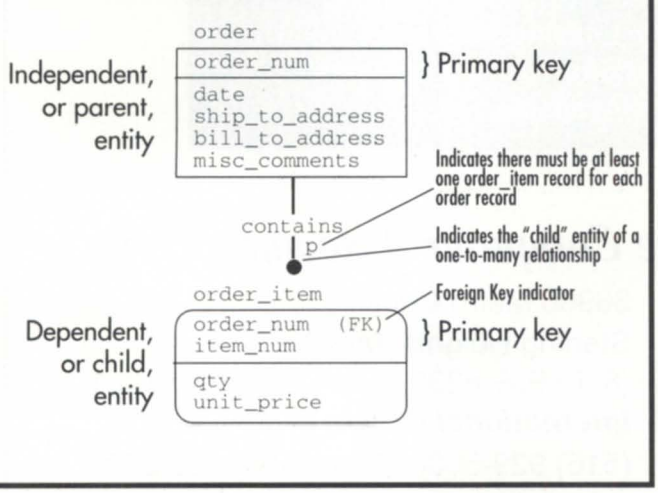


Figure 2: Identifying and nonidentifying relationships

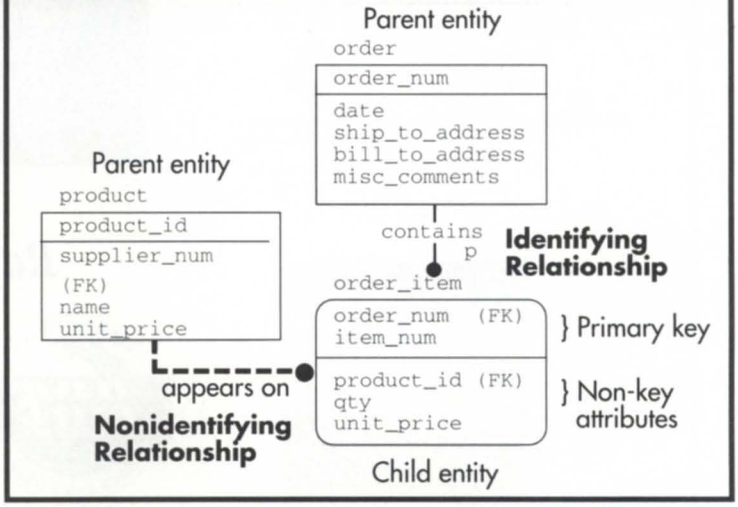


Table 1: Cardinality symbols

This cardinality symbol at the "many" end of a relationship line...	Indicates there are this many child records for each associated parent record.
No symbol	Zero or more
P	One or more (Positive)
Z	Zero or one
N (actual notation would be a positive integer)	Exactly N

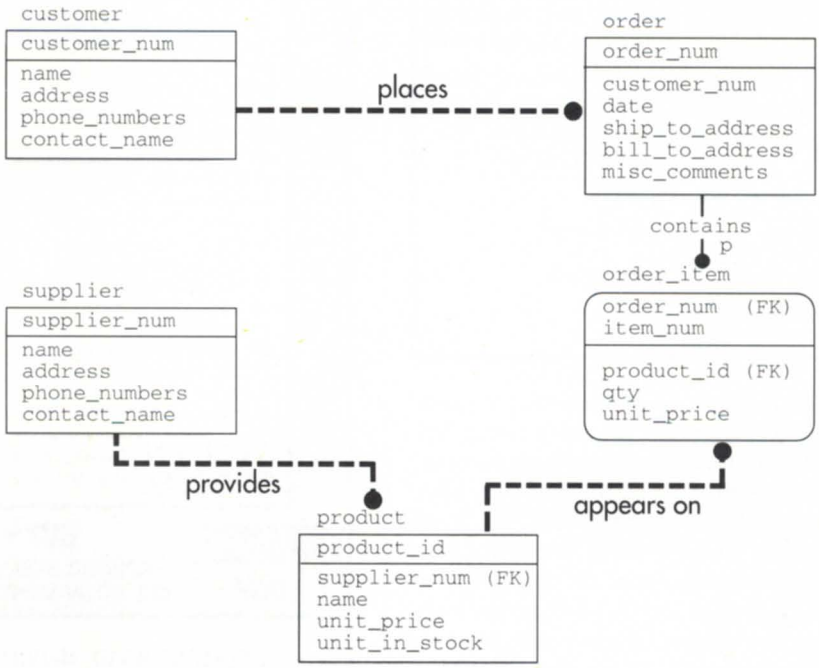
with a single word: *contains*. The solid dot at one end of the relationship line indicates that ***order_item*** contains many records for its related entity, order. Notice also the capital letter "P" at the "many" end of the relationship line. This designates that there must be at least one (a positive number) ***order_item*** record for each associated order record. The "P" is called a cardinality symbol. Table 2 lists cardinality symbols.

With this nomenclature in place, the ERD can be "read" in English-like sentences. For example, see the ERD in Figure 1 on page 28.

Each order contains at least one item.

It shouldn't be any surprise that the ERD sentence above corresponds with the business rule that was stated before the ***order_item*** entity was added. After all, one of the primary objectives of data modeling is to capture an organization's business rules as a part of the data structures. This is what is meant by a "data-driven" application. Using techniques such as stored procedures and data base triggers, the data base itself will enforce business rules like the one above. Notice what a boon to data integrity this is. Because the relational data base can enforce business rules, *application programs don't need to*. This means application programmers *cannot* write program code (3GL or 4GL) that compromises the integrity of this business rule. This approach prevents many bugs from ever occurring. This also represents an application-maintenance feature. If the business rule ever changes, only the referential integrity enforcement in the data base needs to change,

Figure 3: Added entities



not the (perhaps many) application programs that reference it.

Data-integrity features like this make RDBMSs so powerful. Comparing an RDBMS with these capabilities to an older-technology hierarchical file management system is truly comparing apples to oranges.

Other required entities

The ERD in Figure 1 showed line items but didn't indicate which product was being sold. To maintain a normalized data base, we must create an additional entity that represents the product as well as a relationship to associate that product with the line item (as shown in Figure 2).

Several new notations appear in Figure 2. Notice the dashed relationship line between product and ***order_item,*** which is in contrast to the solid line between order and ***order_item.*** The solid line represents an *identifying relationship.* Conversely, the dashed line relationship is called *nonidentifying.* The differences between identifying and nonidentifying relationships is that for identifying relationships, the parent entity's primary key contributes to the child entity's primary key. For nonidentifying relationships, the parent entity's primary key contributes to the child entity's non-key attributes.

To make our working ERD nontrivial, let's add a few more entities.

Figure 3 shows the addition of the customer and supplier entities. Now that there are more than a few entities in our ERD, you can begin to appreciate the number of business rules that can be defined by the diagram. For example:

- A customer may place many orders.
- An order contains at least one line item.
- A supplier may provide many products.
- An individual line item contains exactly one product.

  (This last business rule shows how you can read the diagram from child to parent. To do so, you generally have to somewhat re-word the verb phrase that identifies the relationship.)

Many-to-many relationships

We've been exclusively discussing one-to-many relationships. Figure 3 contains one many-to-many relationship. All properly normalized many-to-many relationships consist of three entities

Figure 4: DDL scripts

```
CREATE TABLE customer
    (customer_num           DECIMAL(9) NOT NULL,
    name                    VARCHAR2(40) NULL,
    address                 VARCHAR2(40) NULL,
    phone_numbers           DECIMAL(10) NULL,
    contact_name            VARCHAR2(30) NULL,
    PRIMARY KEY (customer_num)
);


CREATE TABLE order
    (order_num              DECIMAL(9) NOT NULL,
    customer_num            DECIMAL(9) NOT NULL,
    date                    DATE NULL,
    ship_to_address         VARCHAR2(40) NULL,
    bill_to_address         VARCHAR2(40) NULL,
    misc_comments           VARCHAR2(2048) NULL,
    PRIMARY KEY (order_num),
    FOREIGN KEY (customer_num)
                REFERENCES customer
);


CREATE TABLE order_item
    (order_num              DECIMAL(9) NOT NULL,
    item_num                DECIMAL(4) NOT NULL,
    product_id              CHAR(10) NOT NULL,
    qty                     DECIMAL(7) NULL,
    unit_price              DECIMAL(9,2) NULL,
    PRIMARY KEY (order_num, item_num),
    FOREIGN KEY (product_id)
                REFERENCES product,
    FOREIGN KEY (order_num)
                REFERENCES order
);


CREATE TABLE product
    (product_id             CHAR(10) NOT NULL,
    supplier_num            DECIMAL(9) NOT NULL,
    name                    VARCHAR2(30) NULL,
    unit_price              DECIMAL(9,2) NULL,
    units_in_stock          DECIMAL(7) NULL,
    PRIMARY KEY (product_id),
    FOREIGN KEY (supplier_num)
                REFERENCES supplier
);


CREATE TABLE supplier
    (supplier_num           DECIMAL(9) NOT NULL,
    name                    VARCHAR2(30) NULL,
    address                 VARCHAR2(40) NULL,
    phone_numbers           DECIMAL(10) NULL,
    contact_name            VARCHAR2(30) NULL,
    PRIMARY KEY (supplier_num)
);
```

and two relationships. In Figure 3 the order, ***order_item***, and product entities comprise the many-to-many relationship. Once again, you can "read" the ERD to pick out such relationships. For example, "Each order may contain many products (via ***order_item***), and each product may appear on many orders (again via ***order_item***)."

Data-definition language

The ERwin/SQL product generated our sample diagrams quickly and easily. One of the benefits of ERDs is that they provide an excellent communications medium for discussing data base structures. As important as communication may be, it doesn't directly affect the physical data base that will contain production data. ERwin/SQL assists in this area also. In the process of creating the ERD, ERwin/SQL accumulated the information required to generate a script that can create actual data structures. The language generated is called the Data Definition Language (DDL). With a few mouse clicks we automatically generated the Oracle DDL for our ERD (see Figure 4, page 31).

The role of tools

This article began with an analogy between software development and home building. Evolving software development tools like ERwin/SQL has, over the past few years, provided as much benefit to software developers as modern power tools have provided for the home building industry in the last 50 years.

The analogy goes further than dramatic progress in tool functionality (albeit at strikingly different rates of progress). Suppose you know very little about how to build a house with hand tools. Would providing you with modern power tools—like nail guns and circular saws—allow you to build a better house? Absolutely not! The tools would merely help you make mistakes faster and generate mass quantities of scrap material.

So it is with software development tools. If concepts such as data base normalization, stored procedures, and data base triggers are foreign, then ERwin/SQL absolutely will NOT help you create an efficient and effective data base. The power tools of modern application development are most effective in the hands of those who have been properly trained. To achieve the cost savings and improved environments the tools were designed to provide, users still must be educated in the methodologies the tools were meant to automate. Δ

Kim Medlin *is a senior consultant with Data General's Systems Integration Solutions group in Atlanta, Georgia. Systems Integration Solutions specializes in custom software design, development, implementation, and consulting. Kim's address is 4170 Ashford Dunwoody Road, Suite 300, Atlanta, GA 30319. He can be reached at 404/705-2653. His e-mail address is klm@atlanta.dg.com.*

Continued from page 6

devices to TCP/IP networks. Applications include remote dial-in LAN access, network printing, and high-speed serial data transfer. IORACK can be configured with a host of Unix systems including Data General's Aviion family.

A menu-driven configuration system eases installation. Each port is monitored individually and provides baud rates of up to 115.2 kb with full modem control. Host utilities allow these remote ports to be seen as local Unix ports. Additional IORACK features include BNC/AUI connections, multi-sessions, SNMP, SLIP, telnet, rlogin, and tftp. IORACK is certified by UL, CSA, and FCC.

Pricing for the 8-port version is $1,795; the 16-port version is $2,495.

Chase Research, Inc., *545 Marriott Drive, Suite 100, Nashville, TN 37214; 615/872-0770.*

Document migration

Germantown, MD—Version 3.02 of Data Bank Associates' "ARChive Interface Module" (AIM) offers enhancements as well as the introduction of two new modules and revised CEO command module menus for CEO releases 3.30 and 3.31.

The new AIM_RESET module is designed specifically to support the user migration functions. When a migration is performed under CEO, the archive flag is normally "stripped" during the process. As a result, a user who has been migrated out and back in order to change the username will have the CEO flag settings removed. However, AIM_RESET will check all the documents and reset the flag to correspond to the document's actual status.

Version 3.02 also introduces the AIM Document Disposal Module, an interactive module that allows for deleting documents to the CEO Wastebasket or Shredder, regardless of the document's archive state. Each operation of the Document Disposal will result in the mailing of a report to the user and, optionally, to the operator. Up to four simultaneous AIM updates can now be invoked against different lists of usernames while the main AIM module can provide the ability to limit and control user activities.

In a break with prior tradition, Data Bank will make the AIM survey modules available free of any charges. DBA has also revised AIM pricing for two tiers, one for "standard" systems and the other for low-end systems.

Data Bank Associates, Inc., *20010 Century Blvd., Suite 104, Germantown, MD 20874-1118; 301/540-5562.*

Extended bus

Wilsonville, OR—Applied Concepts has enhanced the Lazer Link III Model ACI-2003 AD to enable SCSI devices to be

CLASSIFIEDS

SOFTWARE

EMPLOYMENT

located up to 6,000 feet (2 Km) from the host computer. The Lazer Link III is a fully transparent SCSI fiber-optic bus extender that supports a new generation of high-performance workstations, file servers, disk, and optical arrays.

The Lazer Link III is used in mission-critical applications that require real-time data redundancy at remote locations, such as in banking and securities computer systems. The publishing and imaging industry use it to place scanners and printers in secure central locations. The extender allows SCSI-based photographic cameras to be operated far from the computer system. The Lazer Link III provides systems integrators, administrators, and users a new order of flexibility and freedom from limited SCSI cable lengths.

Supporting "fast SCSI" data rates of 10 MB per second, the Lazer Link III is transparent to the user, and it supports any combination of asynchronous and synchronous SCSI devices. A single-ended SCSI connector on the real panel connects to the host computer or peripheral. No additional software is needed for installation and operation. Two Lazer Link III units are connected by a standard duplex fiber-optic cable to rear panel "ST" optical connectors. Fiber-optic data communications provide high-speed, reliable data transfers and provide electrical isolation plus immunity from electrical interference. The external unit costs $1,895 complete with 110/220 VAC input. UL, CSA, and TUV certified.

Applied Concepts, Inc., *9130 SW Pioneer Court, Wilsonville, OR 97070; 503/685-9300.* Δ

ON-LINE HELP

Who to call for answers about
NADGUG *and* FOCUS

FOCUS Magazine address:
c/o Turnkey Publishing, Inc.
P.O. Box 200549
Austin, TX 78720
FAX: 512/335-3083

NADGUG address:
c/o Danieli & O'Keefe Assoc., Inc.
Chiswick Park, 490 Boston Post Rd.
Sudbury, MA 01776
FAX: 508/443-4715

NADGUG

Membership, RIGs, SIGs
NADGUG staff **800/253-3902**
(Outside the U.S and Canada.) **508/443-3330**

Electronic bulletin boards
(300,1200, 2400, or 9600 baud modem)
Rational Data Systems **415/382-8413**
DASH bulletin board (2400 bps modem) **800/DASH-CSC**
Data General Customer Support Center **800/344-3577**

FOCUS Magazine

512/335-2286

Editorial comments, article suggestions ..... Doug Johnson
(please send product announcements to the address listed above)

Information about advertising ..... Susan de Blanc

FOCUS back issues ..... Turnkey Publishing staff

AD INDEX

PRODUCTS AND SERVICES

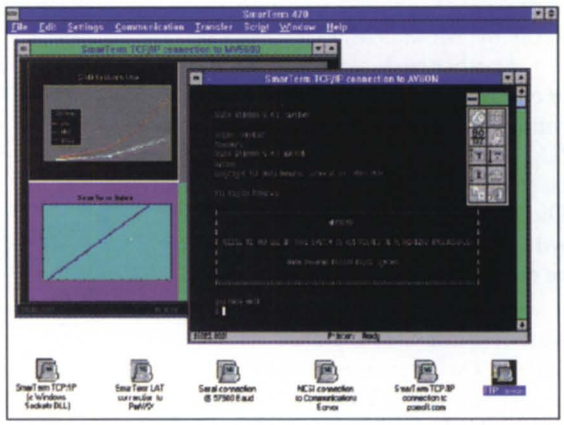
Discover the basic principle of connectivity ...

Look to SmarTerm for visionary DG and VT emulation.

It's a basic principle worthy of Galileo:
SmarTerm's stellar PC-to-host connectivity puts you at the center of your system. New version 3.0 of SmarTerm 470 for Windows is the only software that provides precise, full-featured D470C, VT420, and ANSI-BBS emulation with connectivity to MV and AViiON hosts.

Free Windows Sockets TCP/IP stack and more!
Assure your system a window on the future with great features like SmarTerm TCP/IP stack as a Windows Sockets DLL, drag-and-drop FTP client and server, a connections directory, a script recorder, and *SmartMouse*™ programmable mouse support for host applications.

Test a proven theory for reducing support costs.
It's a fact. You'll save time and money with SmarTerm's pioneering corporate support tools and utilities. These corporate support tools include simplified keyboard remapping, a pop-up keyboard, a customizable help system, and enhanced button palettes with graphics and text.



SmarTerm 470 for Windows provides Dasher graphics terminal emulation and VT text terminal emulation in a true MDI (Multiple Document Interface) format for multiple sessions.

Discover SmarTerm.
SmarTerm 470 for Windows is the only emulation software that includes LAT and SmarTerm TCP/IP (a $199 value) FREE! Discover the basic principle of connectivity today.

Call **1-800-EMULATE (1-800-368-5283).**

persoft®
CONNECTIVITY SOLUTIONS
DOS • Windows • Ethernet • Token Ring

Persoft U.S.A. 465 Science Dr. • Box 44953 Madison, WI 53744-4953 • Phone (608) 273-6000 • Fax (608) 273-8227
Persoft Europe World Trade Center • Beursplein 37 • Box 30237 • 3001 DE Rotterdam, The Netherlands • Phone +31 10 405.3560 • Fax +31 10 405.5073

Circle 34 on reader service card.

DASH Items...

Category: DG/UX

Author: STEVE MASON
Subject: *Removing files with a "-" in the name*

Somehow, we don't know exactly, a file has been created on our Aviion with the name "-GyA[I?" (quotes are not part of the name). We can't use ***rm*** to get rid of it because the "-" gets interpreted as a flag indicator. Anybody know how to get rid of it?

Reply by: TOM HENDERSON

You can remove the file by using an absolute path, such as ***rm*** "./-GyA[I?". Use the double quotes to allow the ? to be interpreted literally, and not as a wildcard.

Reply by: MORRIS M. GALLOWAY JR.

Another trick, which works in lots of circumstances, is to use the ***rm -i*** command with a wildcard (***rm -i *GyAA****). Be sure to use the ***-i*** switch to be prompted before deleting each file. The only thing this misses is filenames with "/" in them, which should never be created.

Author: EUGENE F. O'BRIEN
Subject: *Out of paging area space*

We are using DG/UX 5.4.2 on an Aviion 4605 and running it primarily as a file and print server. Occasionally on the console we get the following message: "From system: Out of paging area space."

It does not show up in the system message log, though. We are not running any memory-intensive applications, and we have double-checked that the swap size is sufficient. Does anyone know what's putting out this message and how to fix it? (One time, the system just hung; another time it continued to work fine.)

Reply by: EARLE MACHARDY

Normally when an application is started, a certain amount of paging area space must be reserved. If the system is out of paging area space or close to it, you will get this message when you start a large application. Also, when a program does a ***malloc()***, and the library needs to increase the amount of private data in the process via ***brk()***, swap space must be allocated to cover the additional space that's allocated to the process. ***Malloc()*** will fail and return an error in these circumstances, but many programs simply ignore this, or they take other actions so you don't notice any problem. Using ***sar -r***, you can find out how much free swap you have. Simply type ***# sar -r 1 1*** to get a snapshot of activity. You can run it in the background and get a reading of swap usage for the entire day (do a ***man 1 sar*** for details). Anyway, the only way to get rid of the message is to add more swap space based on the data from ***sar***. You can add a new swap area using the ***sysadm*** utility.

Author: JOHN NOONE
Subject: *ASCII files on 3.5-inch floppy*

We are using a 3.5-inch floppy in our Aviion to move files from and to PCs. When we move application files it's slow, but it works. When we move ASCII files to the floppy, the records (lines) of the file have no carriage return, so when you try to import this file somewhere it is choked on because it's one long line. How can I get DG/UX to put <CR>s on files that go to this 3.5-inch DOS device?

Reply by: EARLE MACHARDY

Yes, the DOS operating system uses ***\r\n*** to mark the end of a line, while Unix uses just ***\n***. I usually use the ***awk*** command to process each line and use the ***printf*** function to print out the "\r\n" at the end of each line.

Category: Hardware

Author: ED CHARBONNET
Subject: *Dasher CRT modes*

Does anyone know the code sequences to send to a D413 to change it from DG216 native mode to VT320? And how about the codes to send it back to D216 mode? It is getting tedious doing that by hand with the N/C key and selecting a bunch of options.

Reply by: *Elliott Lavy*

In order to switch back and forth under host control, you must first do the following setup: 1) Set the "Host" port to D216, and the "Auxiliary" port to VT320; 2) Set the "mode" (?) to "Host" (as opposed to "Both"; 3) Make any desired changes to the D216 and VT320 configurations under Host and Auxiliary, respectively; and 4) Save the configuration.

At this point, Cmd-Alphalock becomes a toggle between the two configurations. You can switch to VT320 mode with

```
<036>Fm5
```

and to D216 mode with

```
<033>[?G
```

The selection of Host vs. Auxiliary is arbitrary and does not affect the host control. I actually did this with a D412/D412+ and switched to D410/D412 mode instead of D216 mode, but I think it all still works. If there is a difference, it should be documented under "hot-key sequence" in the manual. Δ

DASH runs on an Aviion 5200 server located at the Customer Support Center in Norcross, GA. The bulletin board is available 24 hours per day, 7 days per week, free of charge. DASH is accessible via Internet address 128.222.159.141, or by calling 800-DASH-CSC (800/327-4272) for the modem rotary.

Bits and bytes

Please note that the NADGUG/Rational Data Systems electronic bulletin board number has changed. It is now ***415-382-8413.*** *The board is available to all NADGUG members. There are no fees other than telephone charges.*

SCOTT McINTYRE & ASSOCIATES, INC.

"YOUR GLOBAL COMPUTER SOLUTION!"

313-299-0040

A Shower of Spring Specials

CPU's

MV2000 II W/4MB & 21MB CTD $795
MV2500 W/8MB & 130MB CTD $1,995
MV2500 W/8MB & 21MB CTD $2,500
MV3500 W/8MB & 150MB CTD $5,900
MV9500 $6,950
MV9600 W/32MB $23,750
AV4300 W/16MB & 525MB CTD $5,950
AV4605 W/16MB & 525MB CTD $6,950
AV6200 W/32MB $8,995

DISK & TAPE

6363 160MB Disk $595
6236-A 354MB Disk $350
6239-A 592MB Disk $950
6491 322MB SCSI Disk $595
6554 662MB SCSI Disk $1,250
6585 1GB SCSI Disk $1,450
6590 2GB SCSI CTD $1,450
6675 525MB CTD $1,450
6588 1600/6250BPI Tape $6,750

CRT's

D210 CRT W/KB $110
D214 CRT W/KB $135
D215 CRT W/KB $150
D460 CRT W/KB $135
D216+ CRT W/KB $195
D412 CRT W/KB $250
D1400I CRT W/KB $450
D411 CRT W/KB $195
D413 CRT W/KB $450

MEMORY

8926 2MB For MV2000II $150
8972 4MB For MV2000II $350
8941 8MB For MV2500 $1,950
8942-C 16MB For MV2500 $3,500
80108-C 32MB For MV9XXX $4,995
8990-E 32MB MV15/20000 $3,750
7015-C 64MB For AV5/6000 $6,500
7016-C 128MB For AV5/6000 $12,900
7019-C 32MB For AV4300 $2,900

COMMUNICATION

4369 IAC-8 W/TCB $295
4817 Termserver $1,850
4619 8 Port Trans. $995
7419 VDC-16 $1,495
4623 IAC-24 W/TCB $1,495
7425 VME Term Cont. $2,995
7428 VSC-3 for AV $1,695
4626 LAC-32 W/TCB $950
4626-C LAC-32 W/TCB for MV5500 $2,500

MISC./PRINTERS

D210 Logic Board $55
D216 Keyboard $70
6580 Rams Disk Cont. $450
7430 SCSI Cont for AV $1,500
8992-N Bus Repeater $750
8762 Expansion Chassis $400
6238 Intel/Argus Disk Cont $350
MV2000 II CPU Board $450
MV2500 CPU Board $1,500

"WE HAVE OVER $1,000,000 OF EQUIPMENT IN STOCK AND READY TO SHIP!"

BUY! SELL! TRADE!

*** DATA GENERAL * HEWLETT-PACKARD * SUN * IBM * UNISYS ***

GLOBAL REFERENCES AVAILABLE
UPON REQUEST!

CALL TODAY!

*Scott McIntyre *Terry Smith*
*Robert McIntyre * Michael Nowacki *
* Lorraine LaCroix

SCOTT McINTYRE & ASSOCIATES, INC.

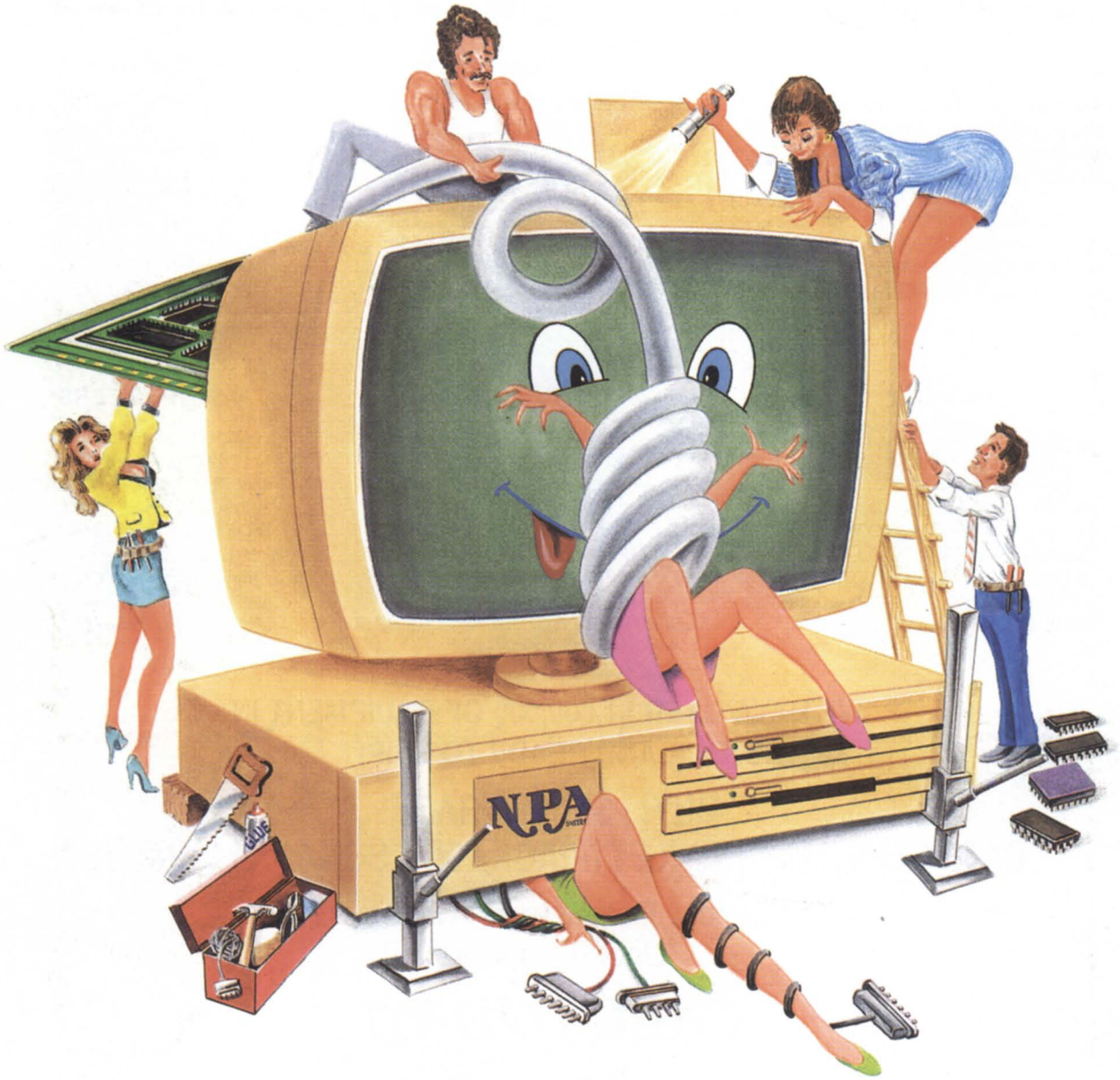
313-299-0040
FAX: 313-299-0041

P.O. BOX 82115
ROCHESTER, MI 48308-2115

VISA MasterCard AMERICAN EXPRESS

Circle 40 on reader service card.

"We Satisfy All Your D.G. Needs"



We will buy your excess computer equipment

Call Us **1-800-USE-NPA4**

ALL YOUR COMPUTER NEEDS

OVER 140 MANUFACTURERS

24 HOUR SERVICE • SALES • LEASES • WIRING • RELOCATION

INSTALLATIONS • LAN'S • WAN'S • TRADE-INS • COMPUTER ROOM • SPARES

N.P.A SYSTEMS INC.
Dedicated To Excellence
Since 1978

761 COATES AVE., HOLBROOK, NY 11741 • (516) 467-2500 • Fax: 516-467-5609

Circle 55 on reader service card.