[12] D. E. Denning, D. L. I
A prototype IDES—a r
Computer Science Labo

[13] P. A. Karger. Limiting
ceedings of the 1987 IEE

[14] D. E. Denning and P. C
intrusion detection syste
national, Menlo Park, C

[15] D. E. Denning. An intr
neering, 13(2), February

[16] *Department of Defense*

Acknowledgment

This work was supported by t
9-X5H-4074J-1 with the Los

References

[1] J. P. Anderson. Comput
James P. Anderson Com

[2] R. Alan Whitehurst. E
cal report, Computer S
November 1987.

Auditing can be controlle

Audit allows analysis of t

based on the system manag

three reports: a security sum

(as defined by a predetermine

parameters); a security even

to be considered high-risk; an

log to support the conclusion

include sessions outside busin

business hours and holidays o

of the AUTHORIZE or SYS

other alarms (alarms can be

attempts; sessions with dial-

and attempts to turn off aud

Discovery is an expert sys
inquiries to the data and co
detect variances in normal su
by type of service and acces
activity for the user access co

Discovery is system-spec
specific application-dependen
also monitors some variables
time of access, type of acces
Discovery allows the security
parameters, so that the syste
be determined. The security c
as service offerings change.

is developed by having the us
Once a user's electronic sign
user.

BioPassword is automati
when a user logs off, and can
word prompts the user for an
dynamics of each against the
mal work only if the verificat
for a prespecified period of t
user before continuation of th

BioContinuous incorporat
time verification of users. Bio
its own high-speed processor,
in parallel with the user's wo

NAURS monitors networ
trollers (NACs). It collects d
open and close connections, a
NAURS provides both backg
rent use. It provides periodi
triggered by the events them
Incident reports, generated e
that satisfy one of three rul
sessions.

The threats addressed are
TAC id and password) and
work hosts). (Authorized TA
network.)

A prototype NAURS exi

3.4 Ask the Experts

access to sensitive objects, an
MIDAS uses rules involving
for project. To detect Troj
modification to system files
(e.g., two talking automatically
A preprocessor on the W
sor collects audit data from
collection software that was
In its current implementa
to take, and then the take i
implementation phase.

encodes a priori rules that d
sion Detection and Alerting
Security Center to monitor s
MIDAS is implemented o
expert system shell, capable
engine and an explanation f
profiles are maintained in LI
the time of writing, MIDAS
MIDAS is based on Dem
user command line level and
rules:

- Immediate—These are
expected user behavior

confirmation measure is one w

session (e.g., connect time, C

To determine whether user

to base or acceptable behavi

profile is a description of the e

The profiles are periodically

rate based using a decay facto

technique a moving time window

that deviates from the expec

user profile for that measure.

user behavior, if is beneficial

that cannot be detected by f

The IDES prototype use

31 A riori Rules

Paul Karger has suggested w
names and types of objects
program with the names and
an example a FORTRAN co
a user's LOGIN.CMD file w
the FORTRAN compiler to
suffix of .FOR and to create
the compiler attempts to cre
would recognize that such a f
a Unix system for example, c

Although Karger envisio
it could also be used as a r

business hours, an appropriat
hours or off hours. Other use
distinctive pattern of use (e.g
5 and 9); for such users, an
the user is likely to be logged
for whom "normal" could be
not be meaningful at all.

There are obvious difficul
departures from observed no
established patterns of behav
and having a characteristic l
may differ radically from day
the computer in several diffe

CPU time, time of day, etc.)
ate probability distribution fo
to determine a rule for classi
point in the multivariate spa
intrusive job probability dist
tion. The points with the la
normal jobs belonging to tha
has been determined, a new
critical region, and normal o

Because audit data conta
were taken to determine a h
jobs:

- Nonintrusive profile ap

run, number of files accesse
records inserted, retrieved, u

They created a database
users. They selected a job as
users (both are referred to as
as CPU time used, terminal
variables to construct a profi
user.

The SRI researchers deve
the profiles developed for eac
true positive rate (percentag
positive rate (percentage of n
percent means that all intrus
divided by the false positive

records within a session that
for a session as the sum of th

In tests to analyze for i
classifier successfully detecte
was high (between 40 and 7
longer training period were u

Four of the selected feat
features were very good at d
rates. Believing that comma
between normal and abnorm
their performance. It decide
value for a user's session to be
session was flagged as abnorm

determined from the audit o
discriminate between normal
was flagged as intrusive by a
outside the user's range or s
staged intrusions were combi
normal ranges for each featu

Sytek wrote software to
to data available in general-
command name, associated fi
a user issued a command.

The Sytek team collected
tify features of the audit trail
Each identified feature was th

Anderson suggested that
attempts and that some wou
access attempts to files, pro
could be detected by observ
users. All of these approache
Anderson offered no sugge
To detect such abuse howev
this approach has been taken
the class of user to which the
is under consideration by the
The classifier user can
a level below which sufficie
of functions that run on or

11th tionl Comp
u

Automtec
nd Intrusio

C

e