



**Safeguard & platform
security update
for
OzTUG
July, 2002**

**NonStop Enterprise Division
Ron LaPedis, Safeguard product manager**

objective of presentation

to present the NonStop enterprise division's approach to enhancing platform security with particular emphasis on the role and future of Safeguard

original Safeguard world security was simple

- relatively small “systems” - 255 users in 255 groups was plenty
- applications owned i/o devices
- private networks prevailed – easy to secure
- simple passwords were “good enough” to insure authentication
- homogeneous system environment
 - Guardian only – no OSS
 - generally Tandem systems only

no zle initiative

no indestructible scalable computing initiative

the world has changed and continues to change

- networked systems becoming more prevalent
 - our own and others
 - must still present single system security image
 - far more “entities” to secure
- networks are open – not closed
 - no one system owns all resources
 - far more important to authenticate access points
 - no consistent security model across systems
- heterogeneous system environment
 - oss, other vendors
 - far more distributed middleware and applications
- more ported software products

oh, yeah - the internet

- high-value applications now distributed and open to far wider access and attack
- internet has driven open standards
 - application environments – java/corba, tuxedo, etc.
 - connectivity environments – tcp/ip, http, soap
 - data formatting standards – xml

platform security strategy

- Safeguard will continue to be the centerpiece of platform security
- platform security will continue to be complimented by 3rd party products
- platform security in the OSS environment will be enhanced
- platform security will be enhanced to support zle, isc, and other key initiatives

Safeguard strategy

- Safeguard must support more systems, more users, more entities
- Safeguard must become more granular – enable role-based security
- Safeguard must include standard interfaces for third-party value-added products

Safeguard must anticipate the future

the future of Safeguard

- support far larger number of users, groups, and “entities”
- support multi-faceted authentication
- single system view of large networks
- role-based security
 - group-oriented security is not granular enough
 - impacts middleware, database, applications and operations
- safeguard must support multiple os environments
 - OSS as well as Guardian – needs of these two are not identical

enhance Safeguard's infrastructure

- expand Safeguard information structures – move toward database/directory
 - enables expanded number of systems, users, entities
 - makes room for more information about systems, users, entities
 - positions safeguard for the future
- expand Safeguard processing structures
 - enable parallel processing
- open Safeguard to additional functionality
 - satisfy customer requirements
 - apis for full oss access
 - apis for 3rd party access
 - more granular control of safeguard operations

***enhanced infrastructure is required to attack the itug big 6
in an integrated, adaptable fashion***

the itug big 6

- priorities based on resources and fit with infrastructure changes
- 2003 planning outlook (**not** fcs) includes
 - support for acls that include wildcard masking
 - warning mode at acl level
- next 2 projects currently “on the bubble” for 2003
 - allow acls to use Expand node names
 - allow creation of disk file acl for non-existent files if “persistent” option used
- remaining items depend on completion of infrastructure changes – not in 2003 plan
 - allow a user/alias to be owned by more than one user
 - allow a description field on user records

how do we insure success?

- ned development committing resources to Safeguard
- security initiative has been created with the following functions:
 - coordinate security requirements across ned development organizations and drive 2003 planning process
 - evaluate, prioritize, and address customer requirements as part of the overall security strategy
 - insure that security functionality supports key hp initiatives (zle, isc, customer satisfaction)
 - investigate and respond to external security exposures (cert, ssrt)

2003 planning proposal including specified itug big 6 and infrastructure changes is currently under review - an update will be given at the fall itug meeting.