Repeat the Audience Questions!! ~~how commonly~~

work on transition to Mark

Security in a Client-Server Environment

Gerry Bernbom, Mark Bruhn, and Dennis Cromwell

Indiana University

Gerry Bernbom, Assistant Director - Data Administration & Access

Mark Bruhn, Manager - Security Administration

→ Third author...

Dennis Cromwell, Manager - Information Technology & Standards

Quote:

"Securing a client-server environment
is like throwing mud at the invisible man --
it may be messy,
but pretty soon you get an outline
of what you're up against."

We hope to share with you
what we've seen of this outline.

Overview

Security in a Client-Server Environment

- Security: Some basic messages
- Two-minute tour of IU's computing environment ... context
- Security: Principles, objectives, strategy ... for security design
- Securing the mainframe in an open environment
- Client-server security
- State of the industry ... as it pertains to security & client server computing
- Conclusion

Security: some basic messages

- Security should enable access - not restricted access
  provide access at levels of risk that are known and accepted
  - the more access we deliver
  - the greater our attention to security
- There is no single solution
  complex computing environment
  multiple points of entry
  - security is NOT like locking a door ... need to understand and address all of them
- A security strategy is essential
  - even if security actions are tactical ... responses to specific exposures
  need to work from principles, objectives & overall plan

a lot more opportunity for access

Two-minute tour:

IU's computing environment

- give you context for the work we're doing in security

- Network multi-protocol, TCP/IP, IPX, Appletalk

  → integrating force in our environment

- Workstations Intel-DOS/Windows, Macintosh, Unix
- Host computers
  - MVS host, VMS cluster, HP/UX application hosts
- Database systems DB2, Sybase, Ingres
- Application development/CASE tools
  - Bachman (data modeling, database design)
  - Uniface (application development)

There is a lot of client-server computing happening at U...
... users have desktop clients for e-mail, newsreaders, network navigators, etc

Two-minute tour (cont.)

Our focus is on client-server computing for administrative info. systems

- The target client-server environment - for administrative information systems
  - — HP/UX host
  - — Sybase DBMS
  - — Uniface development
  - — TCP/IP connectivity
- The target client-server application
  - — financial information system - stringent security requirements
  - — update transactions (e.g., accounting, budget)
  - — document routing and approval

Security: Principles and objectives

- **Principles**
  - — **risk analysis**
  - — **risk reduction**
  - — **manage risk at an acceptable level**

All stakeholders need to:
- understand the risk
- understand actions taken to reduce risk
- accept the results

- **Objectives** – high level – provide continuity and focus to security efforts
  - — **user identification** – who the user is
  - — **user authentication** – they are who they say they are
  - — **user authorization** – what's permitted/prohibited
  - — **user accountability** – keep a record of who does what

Security: Design strategy

- Iterative - not linear
  - identify exposures
  - respond to highest risk exposures
  - assess the effect of our security actions - did they do what we intended?
  - evaluate remaining exposures
- Collaborative
  - involve multiple stakeholders
    ↳ all need to understand/accept risks
  - involve many areas of expertise
    ↳ more complex computing environment... more expertise needed

    users, ~~...~~ university administrators, developers, ~~network operators~~ network designers, security administrators
- Responsive
  - technology change is constant
  - reassess risk in light of changed technology

    - new risks and exposures
    - new opportunities to address risks

Security: Design strategy (cont.)

- **Accumulative**
  - security actions are response components
    ↳ respond to specific exposures
  - security solution grows, but is never completed ... security actions: built on foundation of prior security actions : builds foundation for future security actions
- **Evolutionary** Challenge → to
  - chose components that work together
  - minimize constraints on future security actions
  - fit with, or anticipate, the industry
    ↳ announced, promised or rumored

~~(workon transition...)~~

Having given you these introductory comments to our overall approach to security design — I would like to turn this over to Mark Bruhn who can describe in more detail some of our specific security actions.

get started quicker

7:25

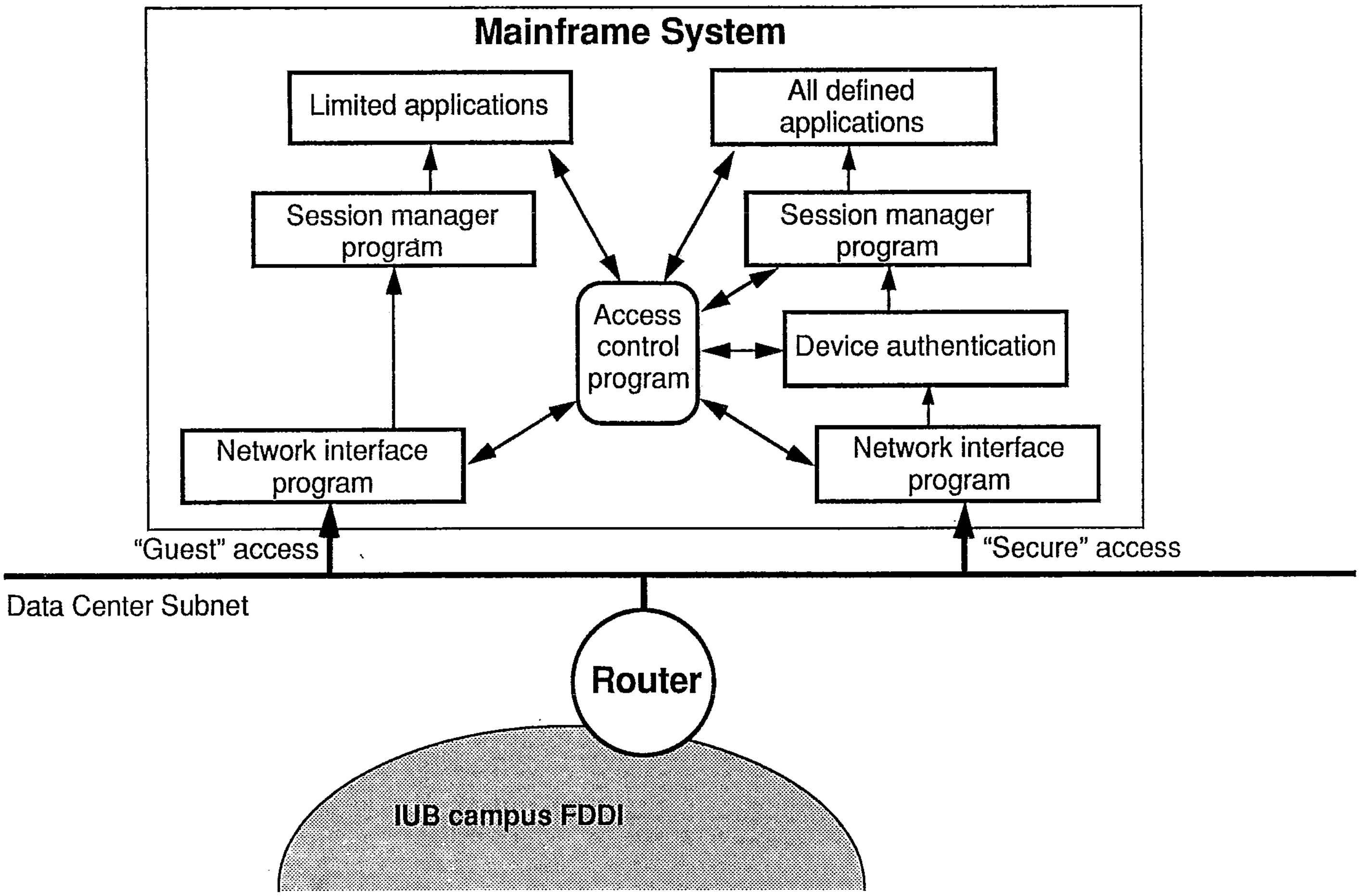
Securing the mainframe in an open environment

- Objectives
  - provide anonymous access to a secure machine
  - route traffic on an “open” network
  - protect passwords on the network
  - improve on password as sole authentication
- Segregate anonymous from secure connections
  - separate network interfaces
  - “Guest” interface: library catalog, etc.
  - secure interface: all mainframe services

Securing the mainframe (cont.)

- Network filters on secure connections
  - exclude foreign (non-IU) addresses
  - exclude “high risk” addresses in IU domain
- Host security software
  - CA/TSS: identify, authenticate, authorize
  - password management
- Password token (SafeWord) authentication
  - required for all connections through secure port
  - unique challenge/response for each user login
  - “playback” of captured login not usable

Mainframe Security



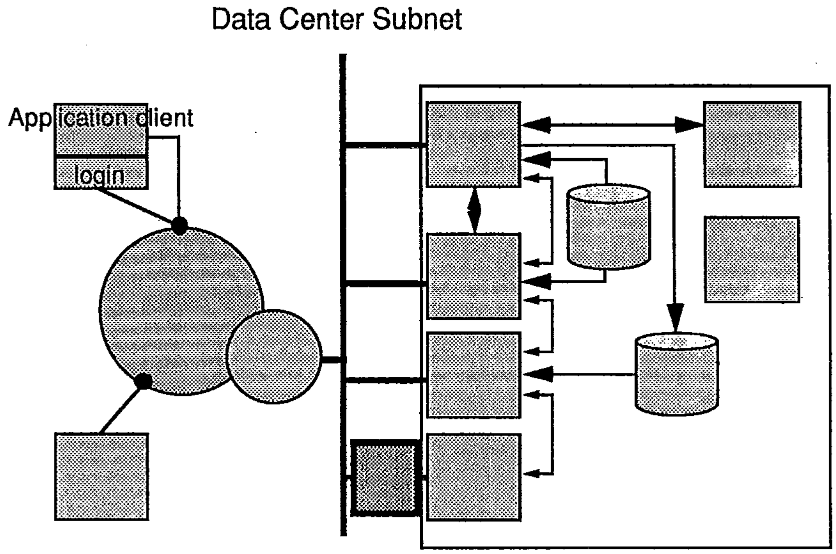
Network interface program ... 'several'
↳ should be "two"

Client-server Security

- FIRST iteration of a security design
  - all solutions are interim
  - planned for enhancement, replacement
  - protects against highest risk exposures
- Objectives
  - reduce network exposure
  - protect host passwords
  - require challenge/response authentication
  - protect database passwords
  - restrict database server to authorized connections

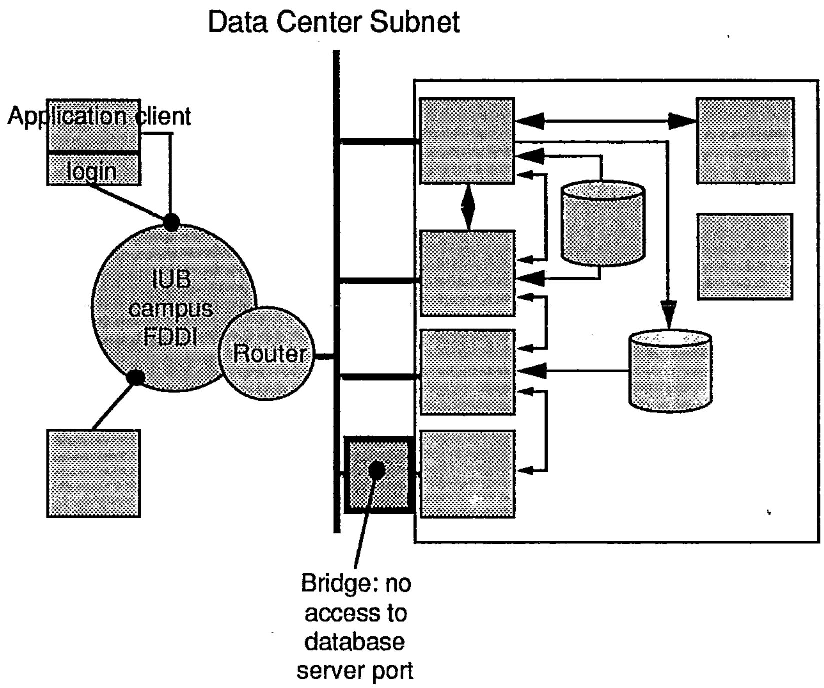
Client-server Security (cont.)

- **Client application**
  - user interface to Security server
  - user dialogue with challenge/response protocol
  - password encryption



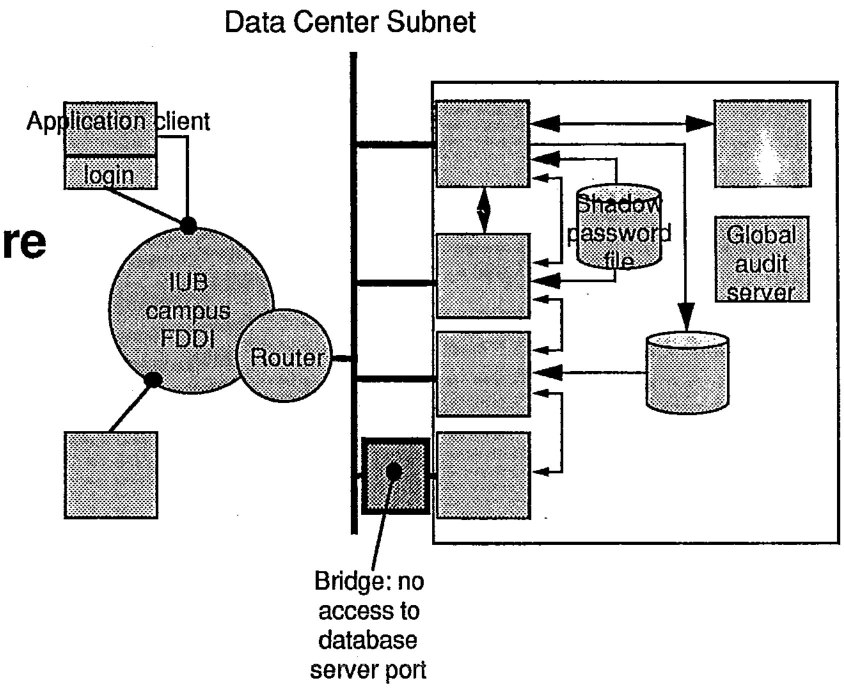
Client-server Security (cont.)

- **Network filter**
  - exclude foreign (non-IU) addresses
  - exclude "high risk" addresses in IU domain
  - NO direct access to database server port



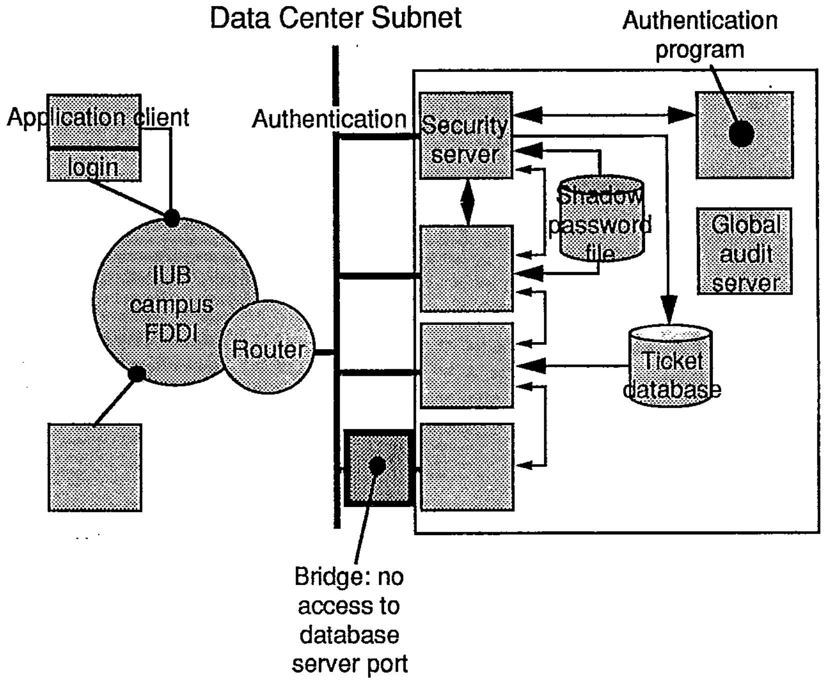
Client-server Security (cont.)

- **Host security software**
  - operate HP/UX as a "trusted system"
  - shadow password file
  - audit functionality



Client-server Security (cont.)

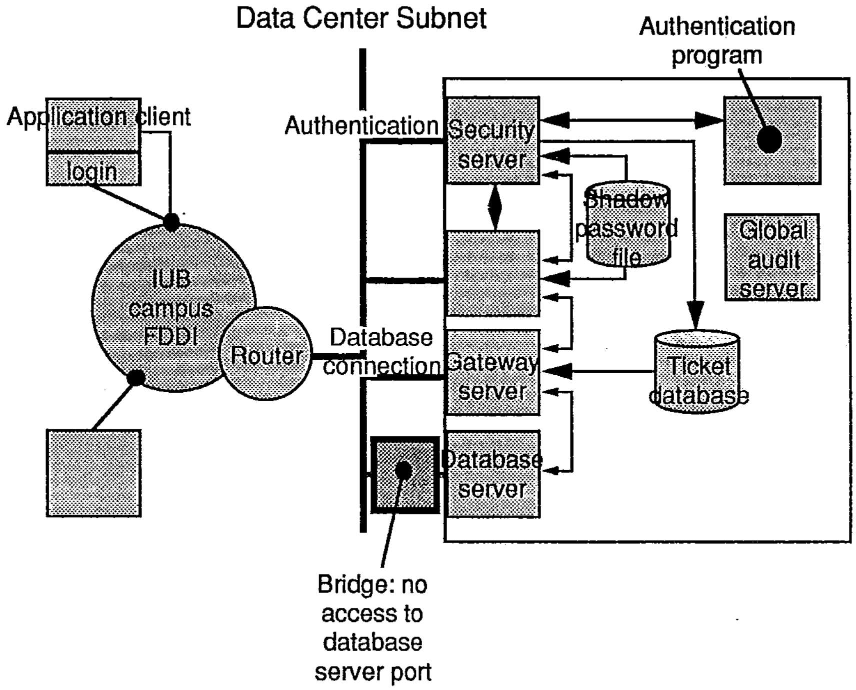
- **Client connection: Security server**
  - manage challenge/response protocol (UnixSafe)
  - issue ticket for access to Sybase server
  - set ONE-TIME user password to database



user never knows the password...

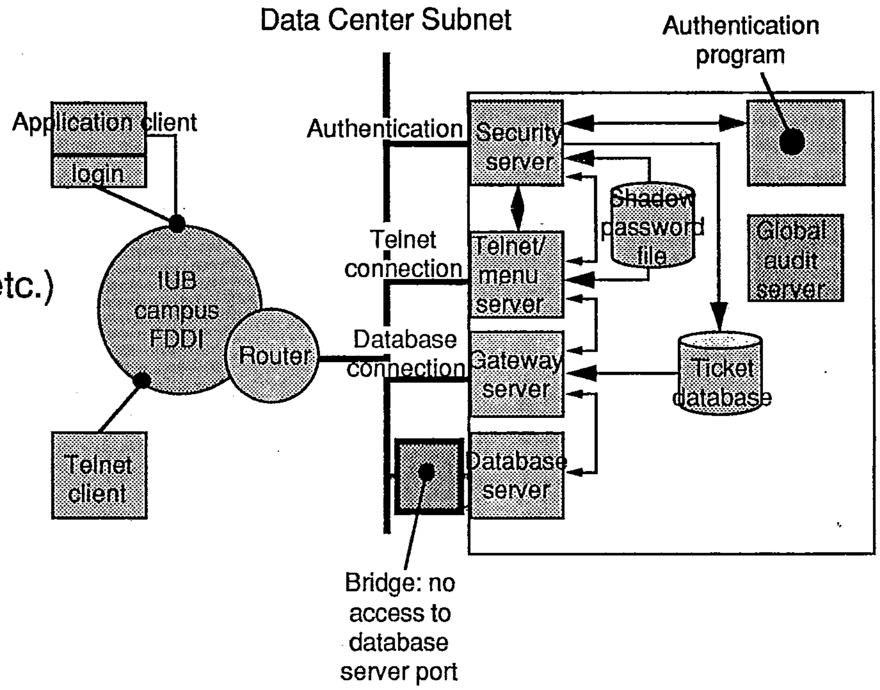
Client-server Security (cont.)

- **Client connection: Gateway server**
  - manage ALL access to Sybase
  - the only allowed connection to Sybase server port
  - only take connections approved by Security server



Client-server Security (cont.)

- **Telnet connection**
  - invoke Security server (challenge/response, etc.)
  - pass database connection to Gateway server

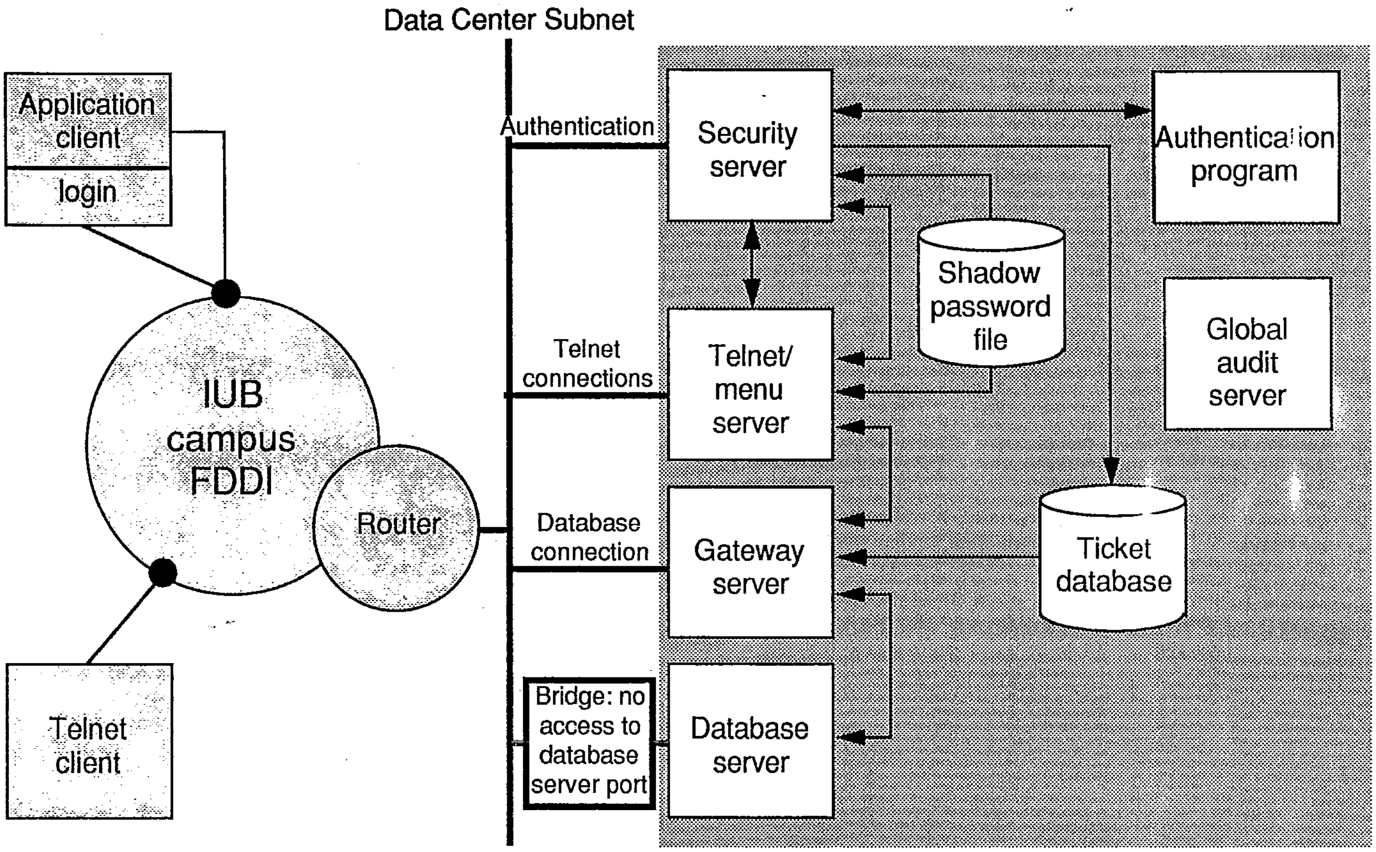


"know that all PCs can't ~~cause~~ run Uniface..."

Instead: "Also need to provide Telnet access..."

Don't repeat everything about the connection

Client-server Security



7:41

Security: The state of the industry

"No significant headway has been achieved in any of the competing visions of enterprisewide security"

"It is left to the user to build together the available technologies with sound business practices to guarantee the integrity of business information."

- Gartner Group
Symposium on Client/Server Security

This quote accurately captures
the experiences we have had
in working with client-server security.

These are some generalizations about the industry
— based on products we use and products we evaluated
NOT an analysis of specific vendor products.

The state of the industry (cont.)

Quality vendors . . . no multi-vendor solutions

Many quality vendors in the client-server computing market place
... but no integrated solutions for client-server security

- Database and tool vendors
  - — basic security services
  - — focus on authorization services — improvements in 'groups' and 'roles' to better manage authorization
  - — incomplete authentication services*
  - — emphasis on proprietary solutions
  - — require enhancement/add-ons
    - but don't always provide the "hooks" to other software products

* - not familiar with university environment of open/public network traffic
- have seen security/authentication "nightmares" ... like static passwords permanently entered in clear-text on user workstations

The state of the industry (cont.)

- Hardware and operating system vendors
  - higher awareness of security issues
  - focus on basic system integrity
  - best support for security standards (OSF/DCE)

Distributed Computing Environment - Security Services from the Open Software Foundation

Responding to the industry

- Assemble your own security solution
  - specialty software products
  - features in primary products
  - home-developed code to tie the pieces together
- Design with the future in mind ... be aware of, and plan for
  - future software features (announced ~~or~~, promised, or rumored)
  - future of standards-based features
  - plan on feature replacement

    ↳ design and implement in replacable modules

Responding to the industry (cont.)

- **Collaborate and create market pressure**
  - **make your case to your current vendors**
  - **take business to vendors who work with you**
  - **place security standards prominently in RFPs**
  - Example of collaboration and influence:
    Big Ten computing directors have
    ... collectively endorsed OSF/DCE standards for distributed computing
    ... focusing attention influencing key hardware & software vendors to adopt these standards

Conclusion

- Security design is our first iteration
- A collection of tactical security actions
- Change is anticipated/planned
- Confidence in our security strategy
  - iterative risk reduction ~~each step is an improvement~~
  - evolutionary growth

↳ each step builds on what went before

↳ ~~each step~~

↳ each security action is a step in a process of continuous improvement

Thank you.

Mark and I would now be happy to answer any questions

Repeat the Audience Questions!!!