Risk Management, Identity Management

CAMP
Tempe, February 2006

RL “Bob” Morgan,
University of Washington and Internet2
IdM Infrastructure Goals

Support institutional requirements for management of access to resources

- more resources
- more variety of resources
- more types of access
- more kinds of accessing parties
- more compliance drivers
- more threats, external and internal

... with acceptable risk, at acceptable cost
App/service component of EAI assessment suite
risk-based approach to determining authn reqs, to avoid "technology-centric approach"
intended by USG to be broadly used, not just govt uses NIST/EAI LoAs by default, can use others also uses OMB-developed risk-tolerance criteria consider threats to app if no authn were in place primitives: data, transactions, users output is authn level for each transaction

Note: When downloading the e-RA tool and opening the application, you may receive Security Warnings. These warnings may be ignored.
Campuses doing app risk assessment?
Exercise to compare assessments via e-RA?
Develop HE standards for risk-tolerance/impact criteria?

OMB: reputation, $$ loss, program harm, info release, personal safety, violation of law

Get IdM community together with audit, risk assessment communities?
Some UW examples

UDub

300,000 UW NetID holders

50K fac/staff, 80K student/applicant, 100K alum,
K-12 students, comm college students, "shared",
patients ...

NetID password authn via Kerberos

passwords in clear for central services stamped out in 2001
two-factor via RSA SecurID (5,000)

applied to terminal/ssh/su and WebISO access

homegrown X.509 CA, but not for user certs

SSL server certs, certs for process-to-process
University Policies

Privacy policy
"must protect privacy", but not how

Machine/network security standards
No data classification, yet

One personal UW NetID per person

One password policy for all
No forced password changes
used to, but cost perceived to be high
turned off when passwords-in-clear stamped out
reconsidering now, but requirements vary
Two-factor: when to use?

SecurID

originally for telnet access to admin apps on mainframe
used for Web signon as admin apps moved to Web
used for new apps "if they're like existing apps"
    ie, users (so no extra cost to deploy) and xaction types
but no policy on when it should be used for new apps
new app server for both SecurID and non- apps?
    modify app server, buy two copies?
    no, put in mitigating procedures so SecurID not needed for
    apps that normally would have used it
3rd-party credit card app

Procurement card / travel card services
web site to reconcile, budget, pay, etc
UW required integration with WebISO (ca 2000)
vendor got our code, integrated it
but never asked about LoA ...
their negligence? wouldn't happen today?
risk covered by credit card rules? or contract?
victim of bad UW authn is just UW?
no different than delegated admin used otherwise ...
NetIDs for local community college students

- didn't want to use UW student process,
- didn't want to give us SSN,
- but do have AD user database

so: add Shib IdP, make get-NetID app Shib-protected

NetIDs for wireless access

- wireless users authn via web for off-campus access,
- usual sponsored accounts too slow, intrusive

so: "temporary" NetIDs, sponsorable by any staff,
- system-assigned name, week max duration, recycled
Improving password reset

Password resets lose
cost, insecure, undoes initial verification
(as many people reset pw as change in the usual way)
many sites do question/answer resets, but isn't this another potential vulnerability?

Implemented Q&A system
must answer 3 questions, 1 can be self-composed
no one forced to use it, users encouraged to test regularly
no observed abuse so far ...
but what is additional risk, effect on LoA?
Inter-organizational risk?

Not much real experience in assessment
Apps today often coming from really-bad practice
e.g., IP address, weak passwords, email proofing
Who sets requirements for whom?
strongly influenced by business relationship
Increasingly driven by compliance, standards
up to us to decide where we will go as a community