



IT Security Audit

Scope of Effort

Mike A'Hearn



Background



- Audit is meant to assess node operations within its larger environment
 - i.e., not intended to set an absolute standard
 - intended to find significant weaknesses
 - focused on operational computers, not personal laptops or general purpose office computers
- SBN-UMD environment
 - a very open campus network
 - campus provides some limited security tools
 - Department of Astronomy manages accounts and maintains operating systems for LINUX machines across the entire departmental research network – main security
 - SBN can add on some security within the Astro Dept environment



Audit Effort



- Includes all people involved, whether or not supported by SBN
 - 5 active participants (3 SBN + 2 Astro Dept; no campus)
 - 2 management (mfa & lk)
- Total effort
 - 9 person days
 - mostly ACR organizing schedules and extensive background reading
 - others were all < 0.5 d



Remediation Effort



- None yet expended – only crude estimates
- Remediate only the high priority items as discussed in outbrief
- Some we clearly should do, some we can't control or don't have expertise to implement
- Total estimate
 - One time costs ~9 person weeks, possibly new hardware and/or purchased software
 - Ongoing costs near 3 person weeks/year