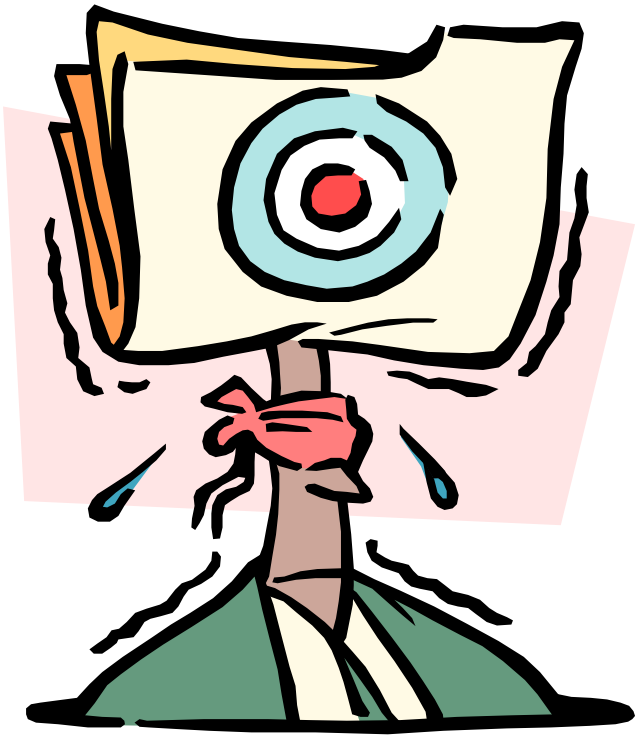
Strategy Session

Tim Grance / Bill Burr

Where do we go from here?



Questions for discussion …

- **How can the IEEE/WiFi Industry partner with NIST and the Federal Government?**
- How do we shorten the time to RSN?
- Who is looking at the RSN-based solution holistically?
- Where are the gaping holes that need filling?
- How can we improve RSN further?

Other questions for discussion …

- How do we ensure that RSN-based WiFi products can be FIPS140-2 validated?
- What are the pitfalls with WPA and what should be done in the interim between WPA and RSN?
- How do we shorten the time to RSN?
- What else?

High-level Strategy for WiFi Industry (1)

- Thoroughly and holistically analyze WLAN based on WPA and develop advice for proper use (e.g.,SP800-48)
  - Burton Group has a plan to prepare this kind of literature
- Launch evangelism and education campaign to drive organizations off WEP and that long-term solution, RSN, is coming
  - Burton Group will be doing – “part of their job”
- Develop a better means to liaison from the IEEE to the IETF (like 3GPP) → this will help harmonize efforts around WiFi
  - Liaison relationship (codifying the work items); 1 persistent FTE
  - Currently there are three work items: specification of EAP authentication methods, specification of keying, specification of RADIUS key wrap

High-level Strategy for WiFi Industry (2)

- Ensure that no elements of RSN preclude it from FIPS140-2 validation
  - Jesse Walker and team need to review NIST FIPS140-2 DTR
  - Randy Easter (with Bill Burr) review RSN (CCM, CCMP, etc.) material to highlight potential problems and work closely with IEEE TGi
- Ramp up/review/analyze RSN holistically to make sure it is what it should be and develop contributions/changes to draft 3.0
  - Provide complete analysis by April 2003
- Provide resources and help to address “desperately needed” things: back-end protocols, provisioning, roaming, and rogue access points.

High-level Strategy for WiFi Industry (3)

- Develop threat model in IEEE TGi RSN document
  - Like models in IETF documentation
- Fund research on denial-of-service attacks on “networks” of today and tomorrow (?)