







# Security Help

Steven M. Bellovin  
[smb@research.att.com](mailto:smb@research.att.com)






We're from the Security Area,  
and we're here to help you.





# The Problem

- ⇒ The IESG mandates security features in protocols, and "Security Considerations" in RFCs.
  - ⇒ But doing security properly isn't easy, and help hasn't been available.
  - ⇒ We're going to try to change that.
- 



# New Initiatives

- ⇒ Tutorial
  - ⇒ New RFCs
  - ⇒ New Security Directorate structure
  - ⇒ Area Security Advisors
- 




# Tutorial

- ⇒ Jeff Schiller has been giving a security tutorial for about two years.
- ⇒ We will continue with and expand this tutorial.





# Forthcoming RFCs

- ⇒ "Guidelines for Writing RFC Text on Security Considerations" (Rescorla and Korver)
  - ⇒ "Security Mechanisms for the Internet" (Bellovin, Schiller, and Kaufman)
  - ⇒ "Encryption and Security Requirements for IETF Standard Protocols" (Schiller)
  - ⇒ More being planned
- 



# New Security Directorate structure

- ⇒ Working Group Chairs
  - ⇒ Area Security Advisors
  - ⇒ Working Group Security Advisors
- 



# Area Security Advisors

- ⇒ Approximately one per area
- ⇒ They work with the non–Security ADs:
  - ⇒ They help prioritize needs for security assistance.
  - ⇒ Criteria: difficulty of security problem; relative importance of technology.
- ⇒ Help find Working Group security advisors







# Working Group Security Advisors

- ⇒ Work with WG on security design.
  - ⇒ *Not* just sprinkling on crypto — security and cryptography are *not* the same thing.
- ⇒ Security generally has to be designed in from the beginning.
  - ⇒ The earlier a WG gets security help, the better. Semantic models may need to be changed...





# The Bad News

- ⇒ We don't have enough security experts to assign one to each WG.
  - ⇒ We never will...
  - ⇒ But we'll do the best we can, with education and the people we do have.
  - ⇒ The best time to ask ADs and Area Advisors for help is when the WG is being formed.
- 