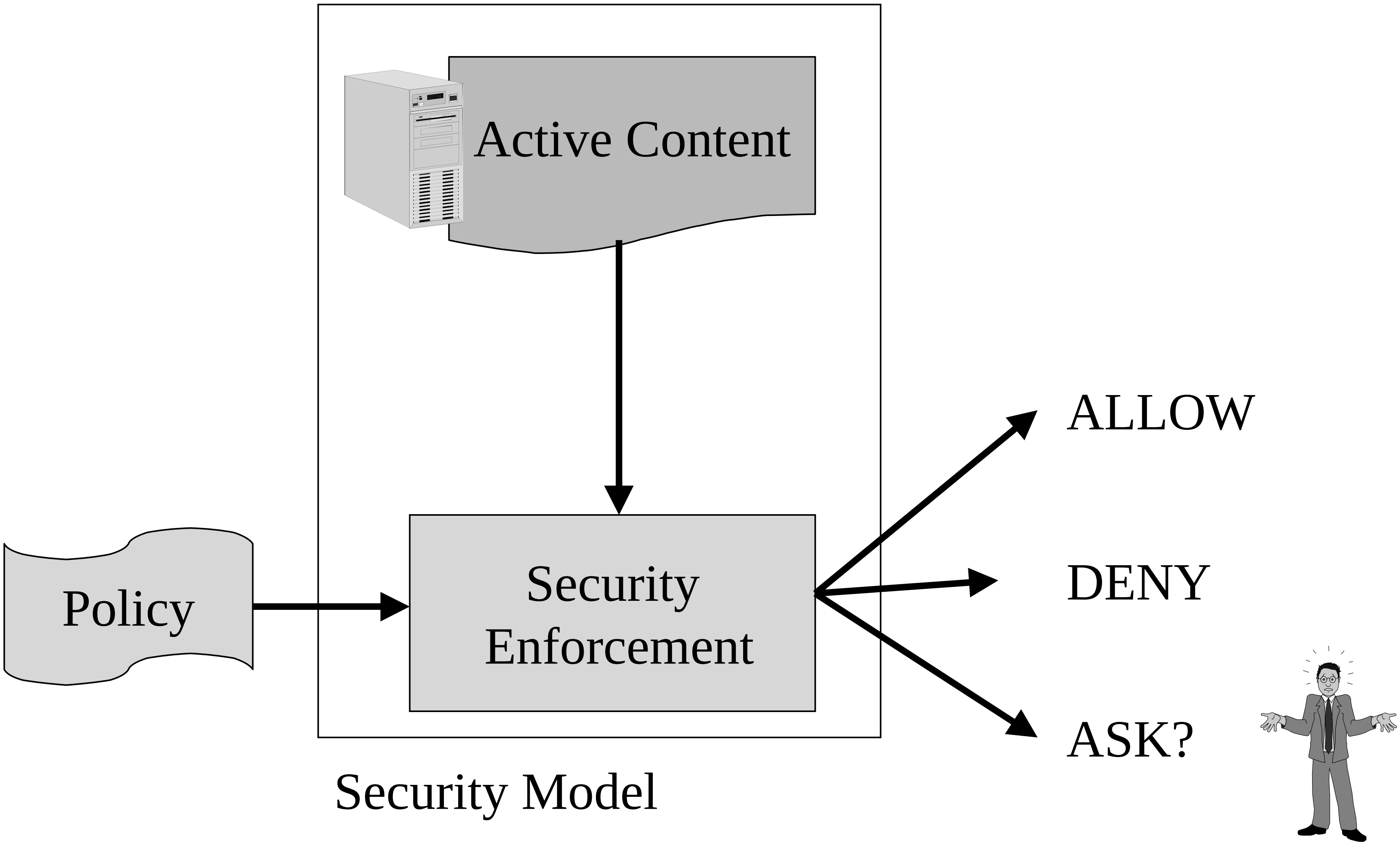
Trust Management and Internet Client Security

Blair Dillaway
Program Manager
Microsoft Corporation

Problem

- Exploiting the Internet will require users download and run active content
  - Java, ActiveX, Scripts
- Raises significant concerns
  - two-way information flow
  - access to system resources
- Managing this requires real-time Trust decisions based on context.

Managing Trust



ActiveX security model

- Download: “signed” = shrink wrap
  - Signature indicates publisher and insure integrity
  - Can designate individual publishers as ‘trusted’
  - No restrictions on functionality
- IObjectSafety: “safe for untrusted calls”
  - Self-assessment of functionality exposed
  - Safety is a subjective judgement

Java Security model

- Standard Java sandbox model (unsigned)
- *plus* Permissions-based model (signed)
  - Indicates publisher and insures integrity
  - States requested permissions
    - Pre-defined High, Medium, or Low permissions
    - Explicitly named permissions
  - Integrated script/Java call-stack security to enforce granted permissions

Trust From the User Perspective

- Given the available information
  - Server am I dealing with
  - Problem I need to solve
  - Properties associated with the active content

  do I trust it to run on my system?
- Usability is important
  - Use policy to limit number of user decisions
  - Aggregate and simplify questions which must be deferred to user

Microsoft Zones

- Aggregate and simplify policy
  - Separate policies for Local Intranet, Internet, Trusted Sites, Restricted Sites
  - Pre-defined High, Med., Low or ‘custom’ make fine-grained choices (‘Custom’)
- Clean mapping from Zone policy to active content security model
- Explicit ‘prompt’ policy when user wishes to make decision interactively

Simplifying User Decisions

- Trusted Publisher's List
  - Suppress prompt for named publishers
  - All other policy constraints must be met
- Java Permissions
  - Permissions requested included in signature
  - User can review permissions once, before application invoked.