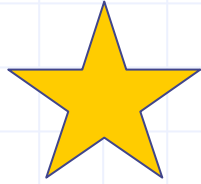# TOG – SF Work Suggestions

Steve Whitlock

PKI ⭐

◆ Deliverable: Guide to trust models
- B2B
- Non prescriptive
- Pros and cons
- Usage examples

◆ Include
- Bridge CAs
- Cross certification
  - Asymmetric cross certification
- PKI + SAML

Middleware

🚫 ◆ SAML interoperability similar to Directory Forum's LDAP interoperability work

🙂 ◆ SAML Certification/Branding

🙂 ◆ Other web services issues
- Architectural guide to ws-xxxxx

RBAC 🙂

- Big gap between theory and real world
- Can we do anything here?
  - Guide to practices and architecture for RBAC systems
  - Longer term – guide to emerging alternatives such as policy based access control

Perimeter ⭐

- **Perimeter becoming soft**
  - More machines outside
  - More B2B inter communication
  - Treat internal network as insecure?
- **How to manage individual machines when the perimeter is the desktop**
  - Eventually move the security to the data

Moving the bar

Typical system

XBSS conformant system

Super secure system

Security level

0   1

Effort
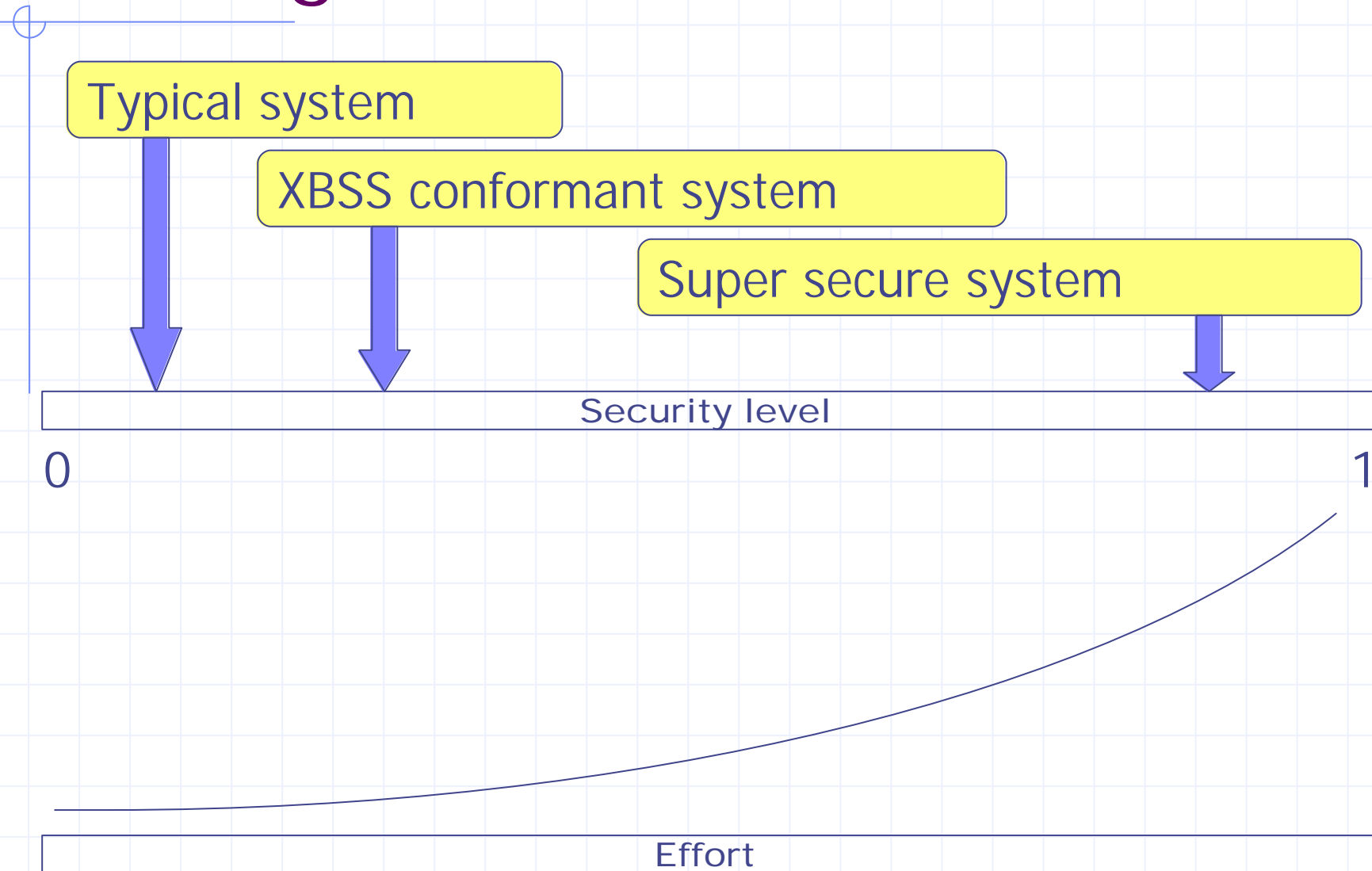
XBSS ⭐

- ◈ Privacy protection standard
- ◈ EU requirements
  - Part of ensuring privacy depends on secure environment
- ◈ Insurance industry requirements

Super secure system

- Secure laptop for executives
- Executive security characteristics
  - One logon to get in
  - None to secure
- Needs
  - Transparent encryption
  - Lock by absence
- Deliverable: secure configuration guide