Panel Position Statement: Usable Data and Application Security

Calton Pu

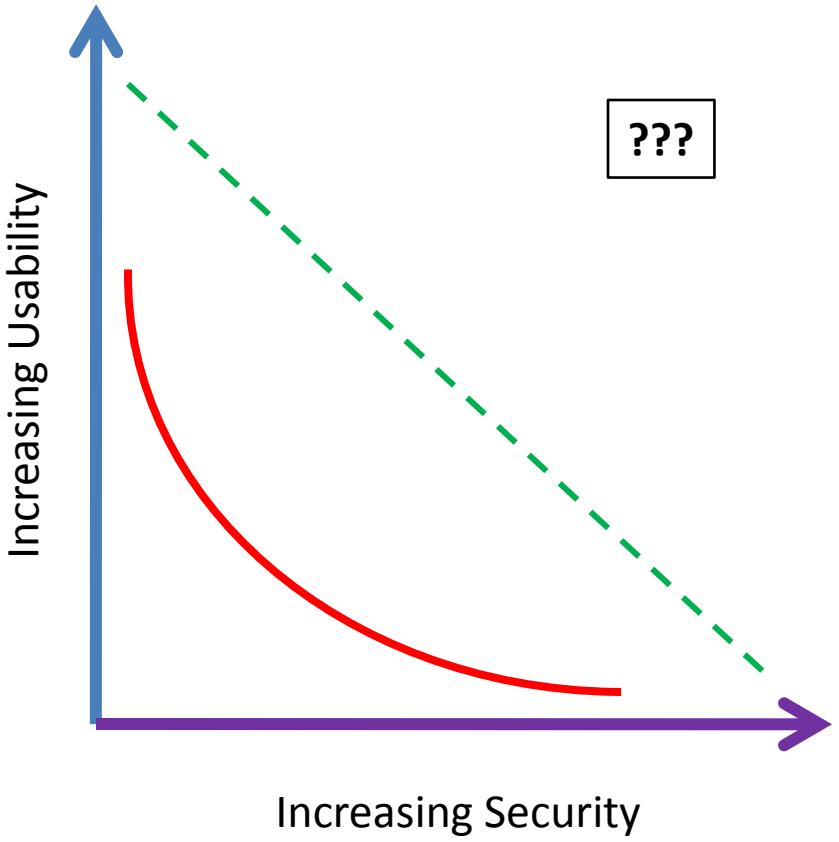
CERCS/GTISC, Georgia Tech

User Is The Weakest Link

- By Doug Maughan, NITRD Cyber Security R&D Themes presentation
- *What about human factors and usability in data and application security?*
  - I don't know much about human factors
  - Usability in system/networking security a problem
  - Can we improve the usability of data & application security?

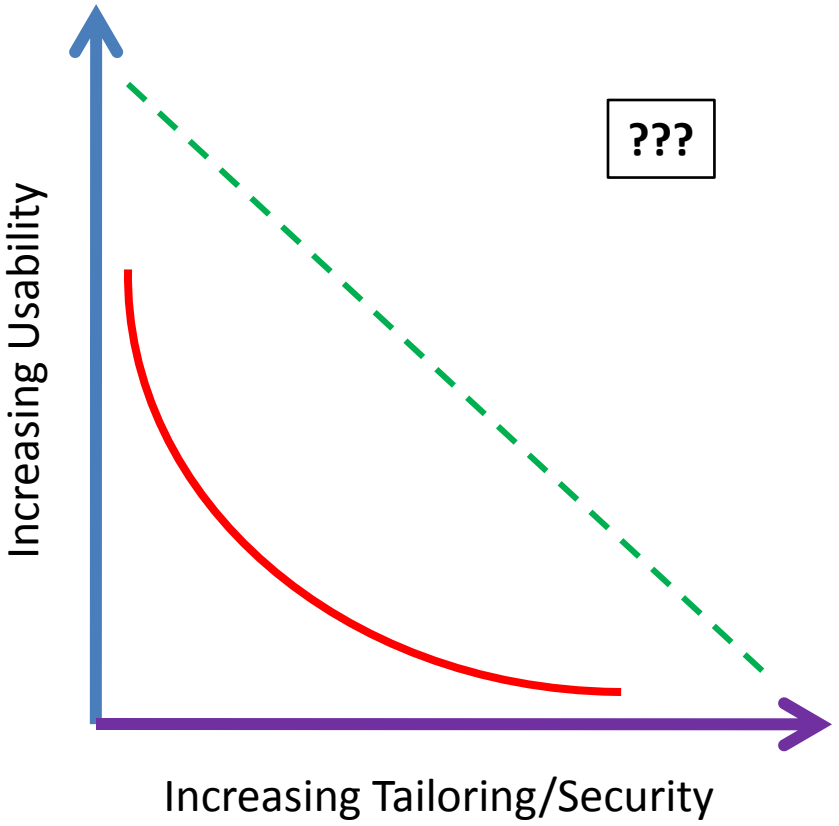
Usable Moving Target

- Trade-offs between usability and security
  - High security means low usability; example: fast rotating passwords
- Challenges in achieving highly usable high security in moving targets; e.g., through automation



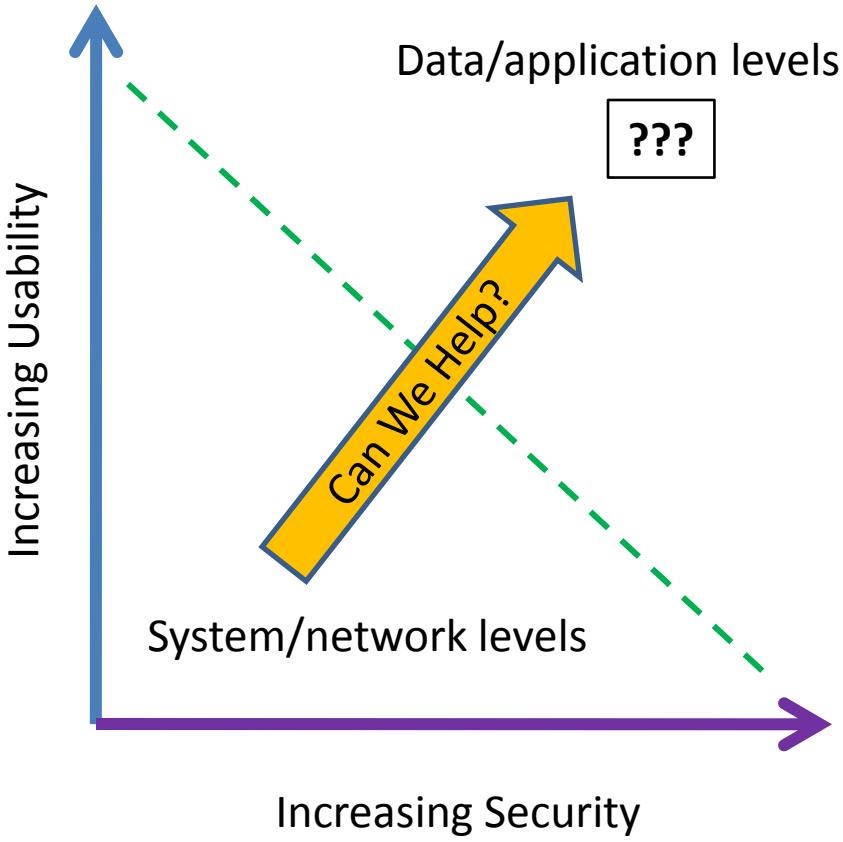
Usable Tailored Trustworthy Spaces

- Trade-offs between usability and tailoring/customization (and security)
  - Fine grain tailoring means constant changes of context and their associated access policies (similar to rotating passwords)
- Similar challenges to achieving highly usable high security in tailored trustworthy spaces



Usable Data & Application Security

- Data and application security can be highly tailored and “moving” (e.g., by automation)
  - Achieving highly usable high security at application level
- Differences between system security and DAS



Unique Aspects of Data & Application Security

- Even if the system software were perfect, data & apps may still be vulnerable
  - Example: insider threat
- Can we distinguish good data from bad data?
  - Examples: deception, spam, phishing
- Can we secure applications despite a malicious kernel?
  - Example: secure multi-party computation