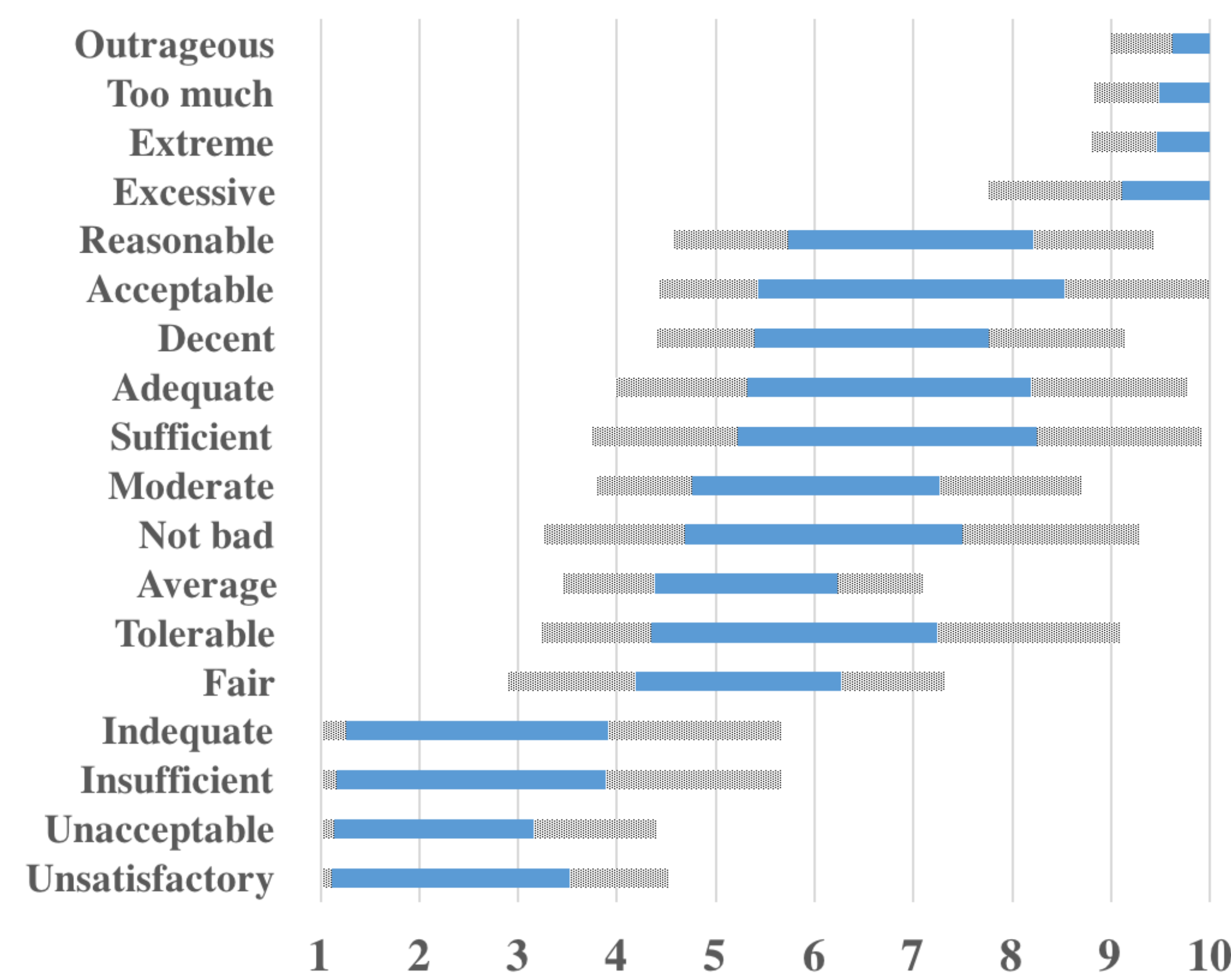


Background

- We rely on experts to evaluate systems' security requirements
- Experts use background knowledge and experience to assess risk and decide on mitigations
- Experts knowledge is diverse (e.g. OS, Networks, Databases)
- We build security requirements reasoning rule base by extracting rules from experts
- Type 2 Fuzzy Logic is can account for interpersonal and Intra-personal uncertainty

Security Requirements Adequacy

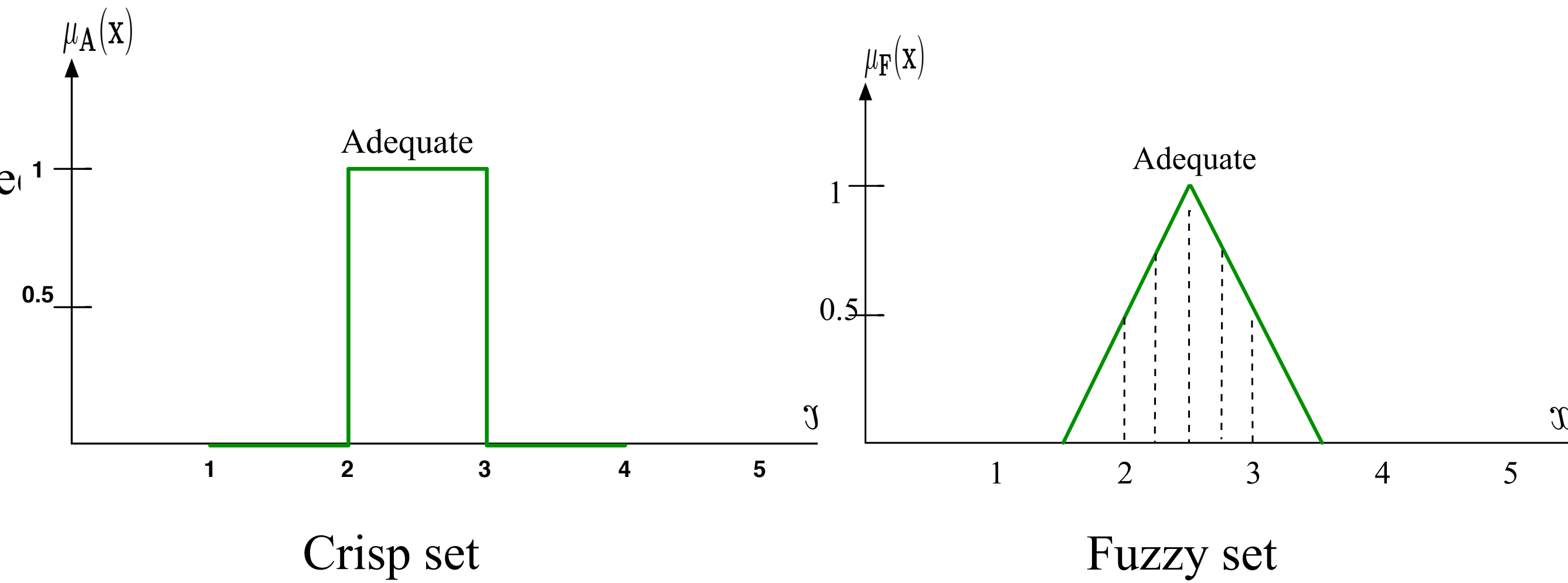
- Security can be expressed in terms of *adequacy*
- A security requirement can be:
 - Inadequate
 - Adequate
 - Excessive
- To represent the linguistic labels on a scale, we need to collect the data from experts.
- We ask experts to select an interval for each label



Intervals start and end means and the standard deviation

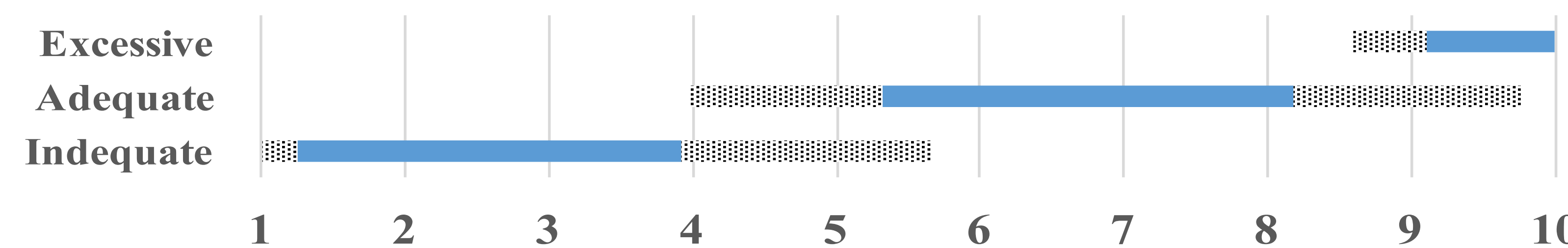
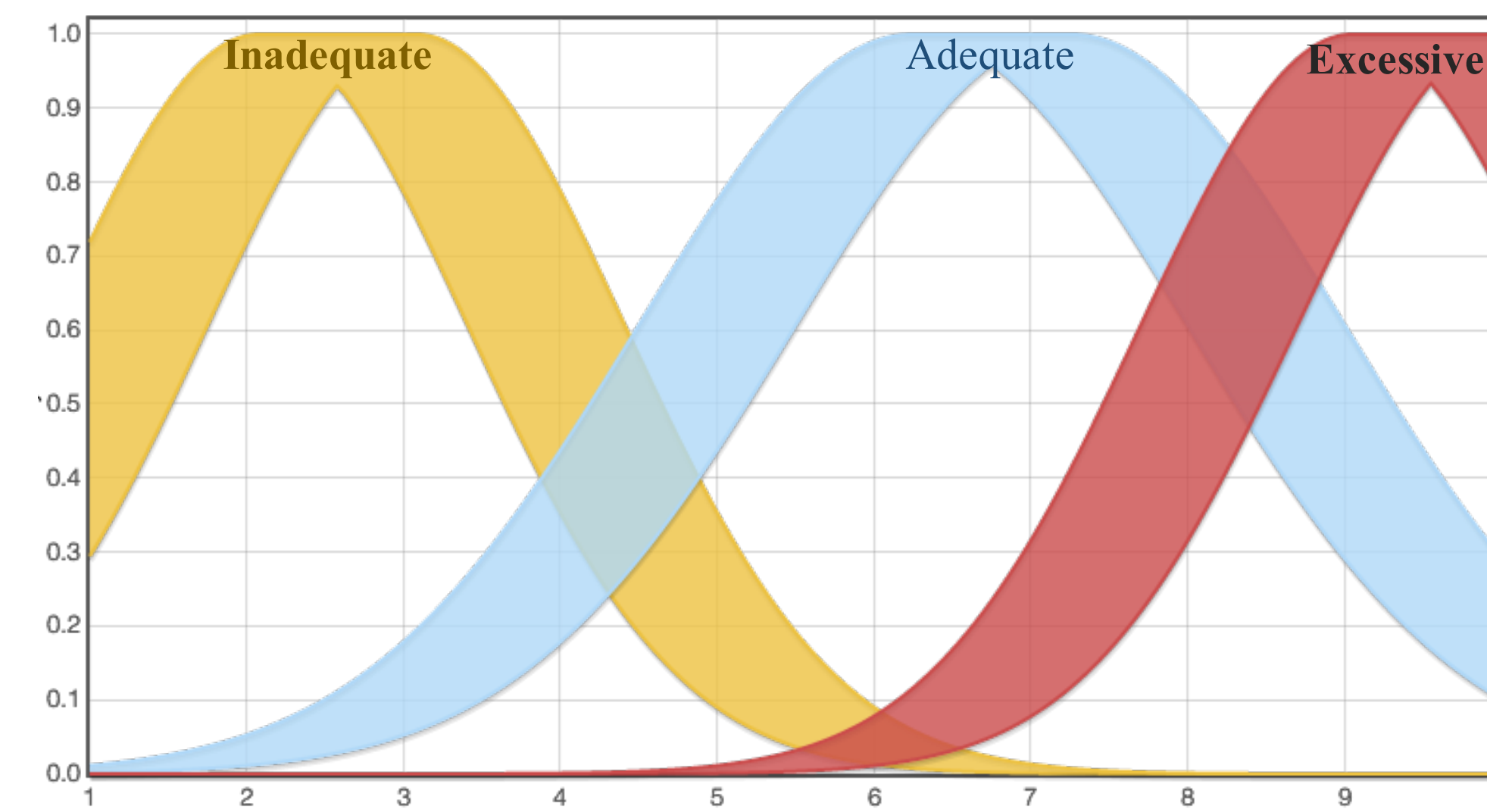
Fuzzy Sets vs Crisp Sets

Fuzzy sets allow to represent to what degree an item x belongs to a set



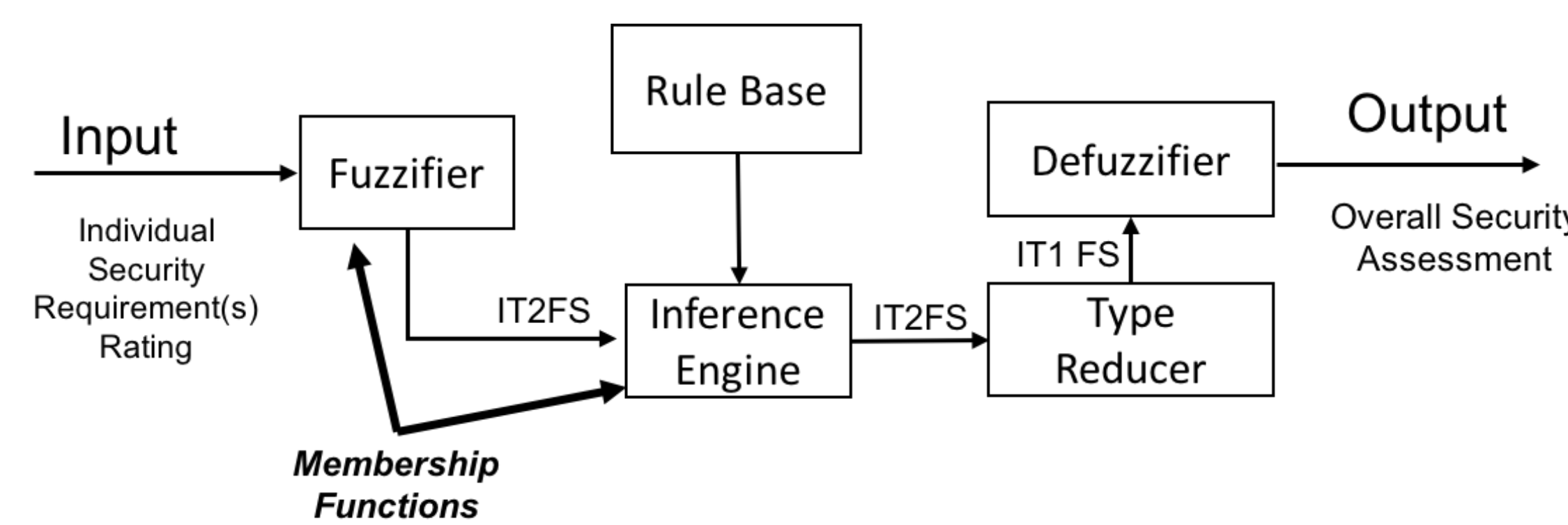
Interval Type 2 Fuzzy Sets

- Created by blurring the lines of the Type-1 Fuzzy Set to handle uncertainty
- Can represent interpersonal and intra-personal uncertainties
- Help reduce the number of labels needed to cover the full interval
- The membership functions are build using the data collected from experts



Interval Type 2 FL System for Security Assessment

- A rule base intelligent system
- Collection of IF-Then statements collected from experts



RULES FOR SECURITY ASSESSMENT SYSTEM					
R #	Antecedents (IF)				Con. (THEN)
	Network	SSL	Password	Timer	Overall
R1	1				1
R2	A	1			1
R3	A		1		1
R4	A			1	1
R5	A	A	A	A	A
R6	E	E	E	E	E

Extracting Rules with Factorial Vignettes

- Asking experts directly about rules puts requirements in a checklist and assume their independence
- Security requirements exist in composition
- We choose to show 174 experts scenarios of different configurations, and we ask them to rate the overall security as well as the overall requirements.

Scenario template:

You are working on your laptop using **\$NetworkType**. You are **\$Transaction**. You are relying on a web browser to perform your task. The browser is already using **\$Connection** for the session. To log in to the system and start your task, you will need to authenticate using a password that **\$Password**. The system will **\$Timer**. The **\$Threat** attack is a serious security concern. Please answer the following questions with regards to mitigating this threat.

- We analyze the results using multilevel-modeling
- We use the statistical results to build the rules and eliminate unnecessary rules

Conclusions & Future Work

- We introduce a new approach to build an automated security assessment system based on IT2FLSs
- We use survey data collected from 174 security experts to derive the IT2FL rules
- In evaluation:
 - Participants assessment was mostly in agreement with systems assessment
 - When not in agreement, system is more conservative
- We plan to:
 - construct scenarios for richer environments
 - study ways to recommend to security analysts which requirements will achieve higher overall security ratings

Acknowledgements

This research was funded by NSA Award #141333 and ONR Award #N00244-16-1-0006