risk communication

Aad van Moorsel, Newcastle University

risk communication

a common element across quite diverse research:

- cardiovascular diseases
- trust economics

→ how to communicate risk?

→ any advice?

risk communication

some interesting angles:

- trust is more important than trustworthiness
- communication is the access point for trust
- communicate trustworthiness instead of snake-oil

how to best do that?

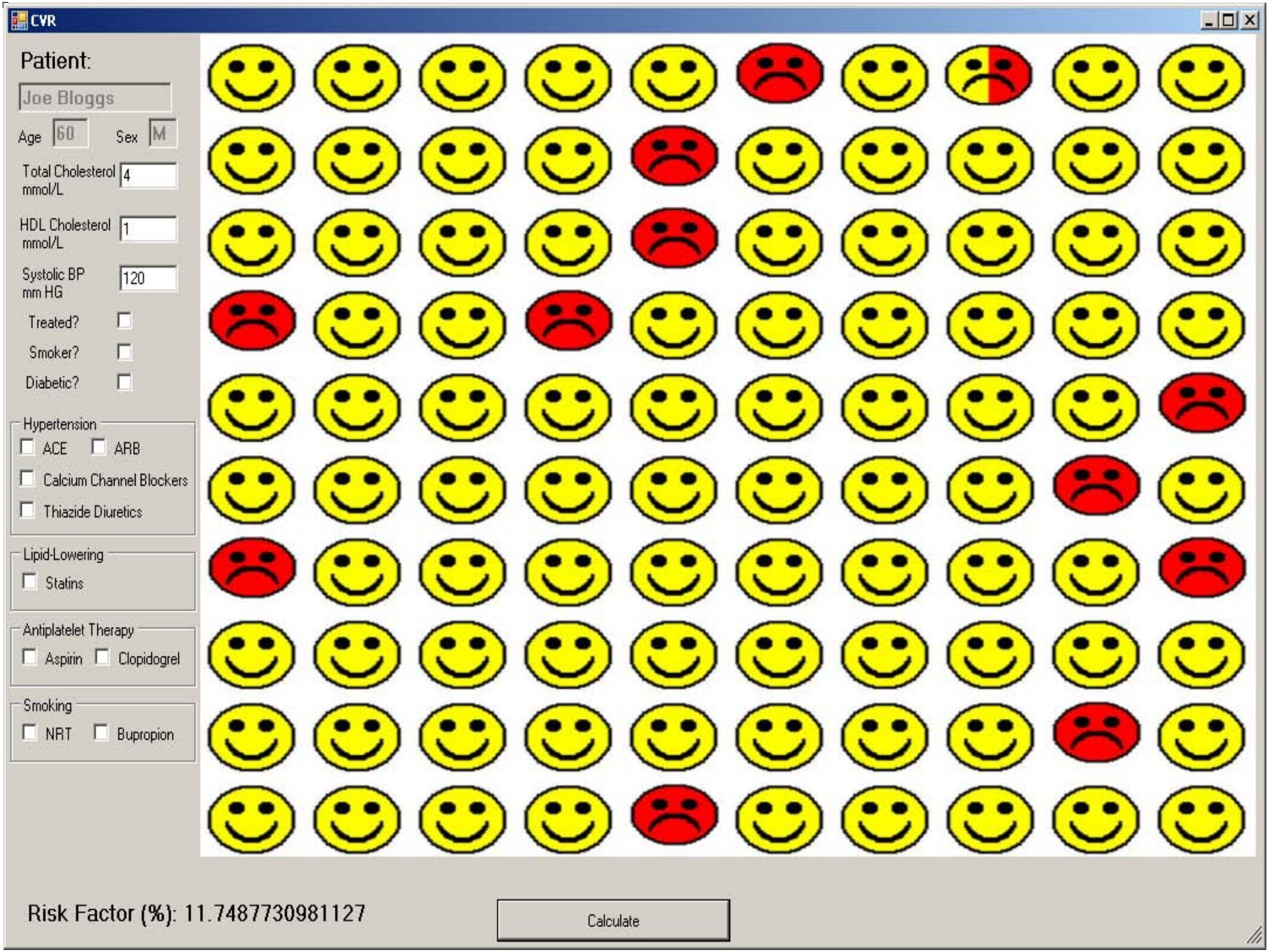
are there proven ways, failed attempts?

1. cardio vascular screening

doctor-patient risk communication

What makes our CVR tool different?

- screening for all 40+ in UK
- interventions
  - Pharmacological – aspirin and other medicines
  - Non-Pharmacological – weight loss, giving up smoking, etc.
- scientifically justified statistical estimates of risk, before and after interventions (i.e., communicate 'trustworthiness')
- has been considerable research in how to best communicate with 'normal people'
- with medical school + private care trust


CVR
Patient:
Joe Bloggs
Age 60
Sex M
Total Cholesterol mmol/L 4
HDL Cholesterol mmol/L 1
Systolic BP mm HG 120
Treated?
Smoker?
Diabetic?
Hypertension
ACE
ARB
Calcium Channel Blockers
Thiazide Diuretics
Lipid-Lowering
Statins
Antiplatelet Therapy
Aspirin
Clopidogrel
Smoking
NRT
Bupropion
Risk Factor (%): 11.7487730981127
Calculate

2. trust economics

communicate aspects of IT security to CISO and IT admin

trust economics

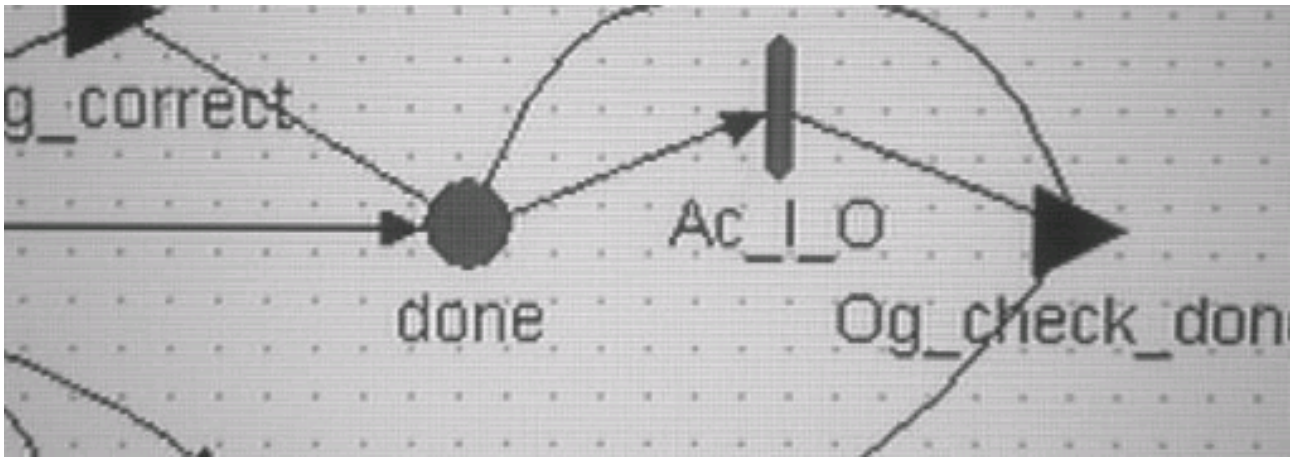
based on the following vision:

- IT security decisions should consider
  (i) technology
  (ii) people / users / employees
  (iii) business concerns
- make use of a set of powerful, formal, mathematical tools, that describe behaviour of a ‘system’ and compute expected states
  - theory of discrete-even dynamic systems
  - modelled using stochastic Petri nets or stochastic process algebras
  - system = technology + people + business

tools

there is an existing set of tools:

- tools for experts
- domain independent

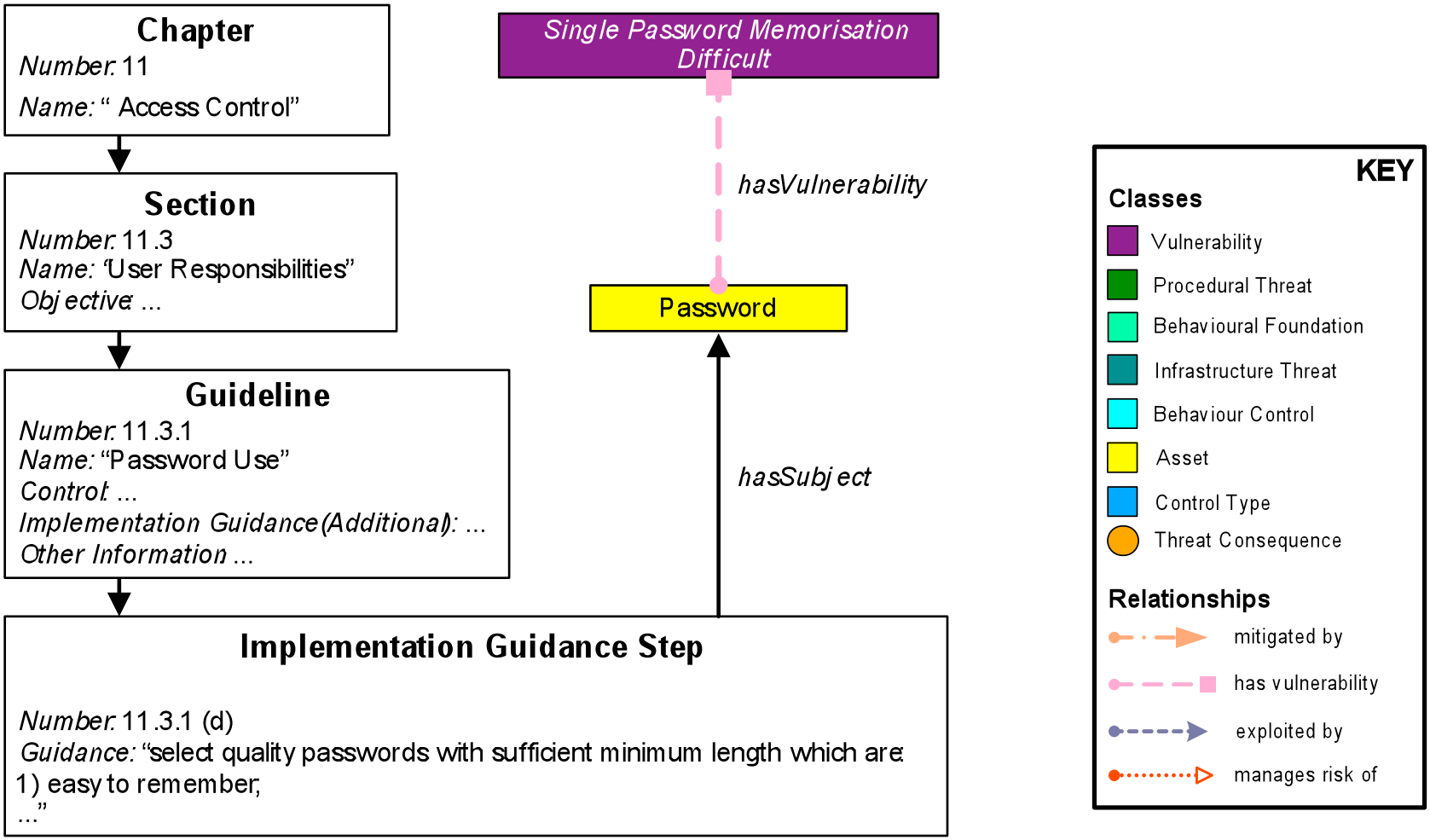


knowledge base

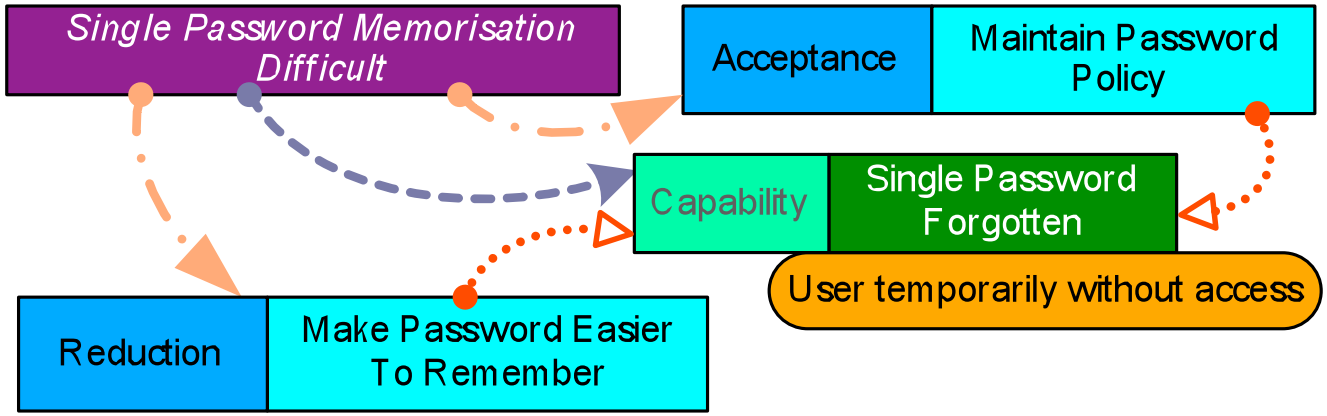
the approach:

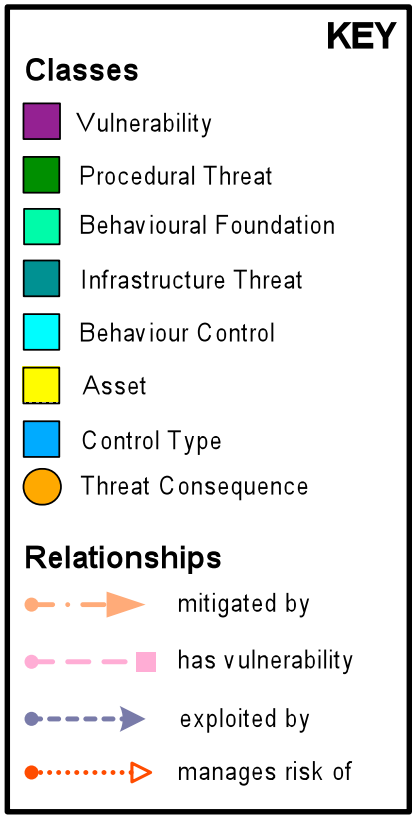
- start from an ISO27k based knowledge base
  - defines the information system space
  - allows us to integrate different levels of abstraction
  - is part of reality of IT admin and CISO
- extend the ontology to include
  - human factors
  - economic and evaluation perspective / abstractions

Example - Link to Guideline



Example – Password Memorisation





(point is not a GUI, it's the use of ontology as a tool for communication)

knowledge base

our strategy:

- identify the right abstractions for the ontology
  - should be useful across case studies (compliance budget?)
- steps
  - point users (CISO etc) to the important issues to consider; (risk) communication
  - introduce economic + behavioural abstractions in meaningful way: introduce rigor in the decision-making
  - compliance; much later: decision-making (risk management)

open questions

what are the fundamental questions in risk communication (communicate trustworthiness to instil trust)

what abstraction can we communicate (eg., compliance budget, preferences, availability/ confidentiality trade-offs?)

are there proven ways? failed attempts?

do other communities have tools (safety?)

other work going on related to information security?

...