

Are Robots Able to Perform Social Engineering Attacks?

Definition:

Robot Social Engineer

A social robot with physical agency and any level of autonomy that uses interpersonal skills and social constructs to manipulate an individual, or set of individuals, into doing or saying something that may or may not be in their best interests.

Step 1:

Robots



Step 2:

Vulnerability

Remote Identification
Embedded Default Passwords
Unencrypted Communications
Man-in-the-Middle Attacks

Step 3:

Social Skills

Gestures	Impersonation
Body Posture	Identity
Authority	Persuasion
Movement	Gaze
Empathy	Trust

Result:

Attacks

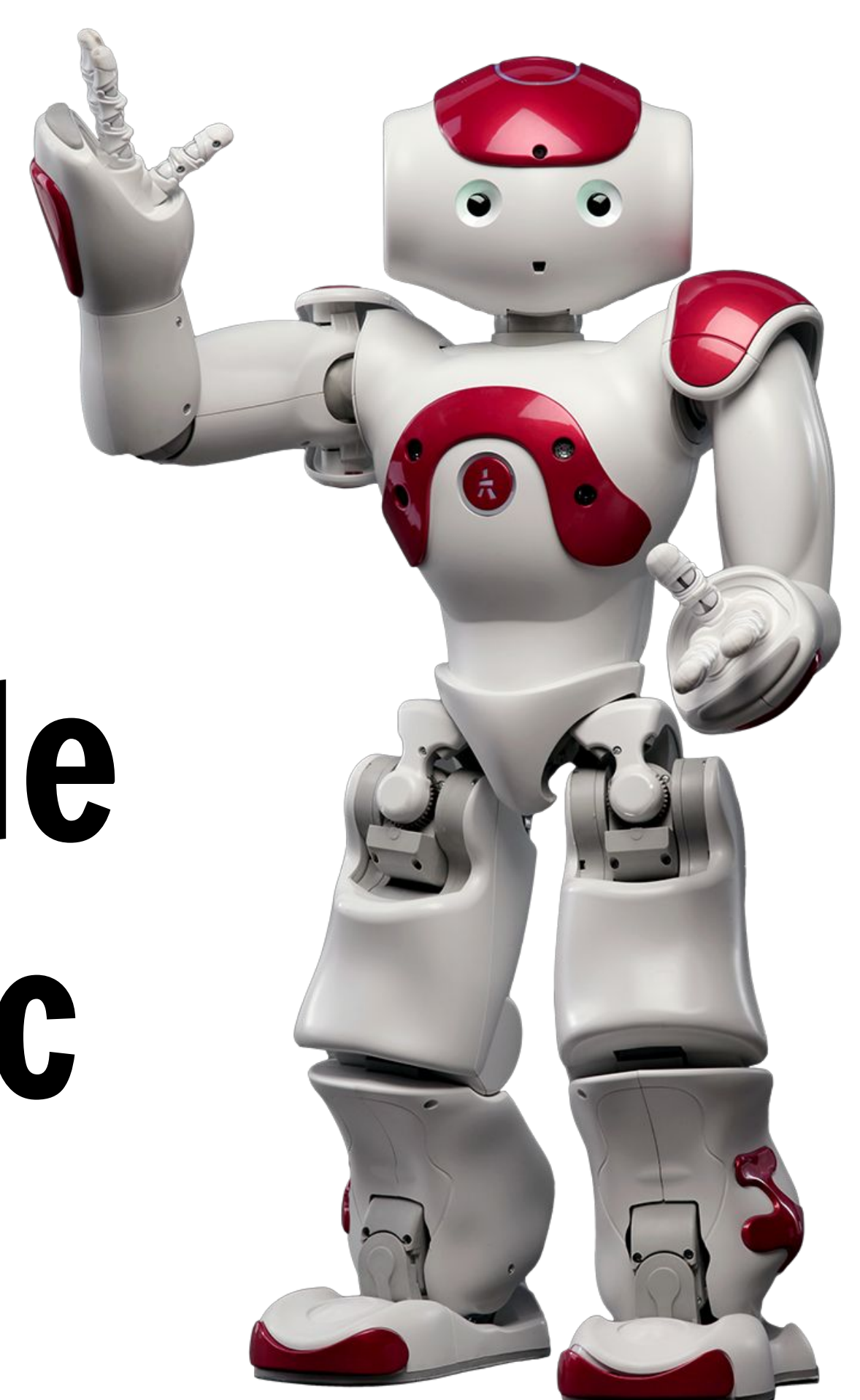
Scenario #1: Leveraging Trust to Map a Space and Sell Data



Scenario #2: Impersonation of Other Delivery Robots to Access Restricted Areas



Scenario #3: Abuse of Authority to Convince People to Take Specific Actions



Our work bridges the gap between social robots and social engineering by comparing and contrasting the two fields. We use this information to define robot social engineering and explore its risks and future defences.