

#ret

---

## 1 | Voice assistant

### 1. What are we protecting?

- (a) User privacy and data
- (b) User mental space (advertising)
- (c) Peace of mind
- (d) Product and brand
- (e) Protect external agendas
  - brand ecosystem, publicity
- (f) User entry points
- (g) User resources (energy)

### 2. Who are we protecting it from, and what are their motivations?

- (a) Data miners
  - Money (companies) or personal gain (blackmailers)
- (b) Advertisers
  - Money
- (c) Foreign state actors
  - Gaining influence
- (d) Physical attackers
  - "Alexa, open the pod bay doors." Digital entry point to physical resources
- (e) Misinformed users
  - To help
- (f) Accidental users
  - !voice assistant actions
- (g) Trolls
  - Fun
- (h) DDOSers
  - Bot net

### 3. What methods of attacks do we prevent?

- (a) External system hijacking (remote control)
- (b) Unauthorized activation for certain actions
- (c) Exploitation of security vulnerabilities for accessing user data and creating bot nets

### 4. What are the possible effects of these attacks?

- (a) Damaged financial well being

- (b) Damaged emotional well being
- (c) Damaged physical well being
- (d) Damage to company brand / ecosystem

**5. What are their resources?**

- (a) Expertise and platform
- (b) Potential for money
  - Which is a commodity
- (c) Exploitable users
- (d) Some have financial resources

**6. What are our resources?**

- (a) Massive company
  - Funding
  - Workers
  - Smart people
  - Infrastructure
- (b) Potential for exploitation / damage
- (c) Intended access to our product

**7. What should we do?**

- (a) Educate users
- (b) Authorization
- (c) Multi-step confirmations / actions for potentially damaging actions
- (d) Patch programmatic security vulnerabilities
- (e) Look secure
- (f) High reward for finding vulnerabilities