

#ret

0.1 | Voice assistant

1. What are we protecting?

1. User privacy and data
2. User mental space (advertising)
3. Peace of mind
4. Product and brand
5. Protect external agendas
 - brand ecosystem, publicity
6. User entry points
7. User resources (energy)

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

1. Data miners
 - Money (companies) or personal gain (blackmailers)
2. Advertisers
 - Money
3. Foreign state actors
 - Gaining influence
4. Physical attackers
 - "Alexa, open the pod bay doors." Digital entry point to physical resources
5. Misinformed users
 - To help
6. Accidental users
 - !voice assistant actions
7. Trolls
 - Fun
8. DDOSers
 - Bot net

3. What methods of attacks do we prevent?

1. External system hijacking (remote control)
2. Unauthorized activation for certain actions
3. Exploitation of security vulnerabilities for accessing user data

4. What are the possible effects of these attacks?

1. Damaged financial well being
2. Damaged emotional well being
3. Damaged physical well being
4. Damage to company brand / ecosystem

5. What are their resources?

1. Expertise and platform
2. Potential for money
 - Which is a commodity

3. Exploitable users
4. Some have financial resources

6. **What are our resources?**

1. Massive company
2. Potential for exploitation / damage

7. What should we do?