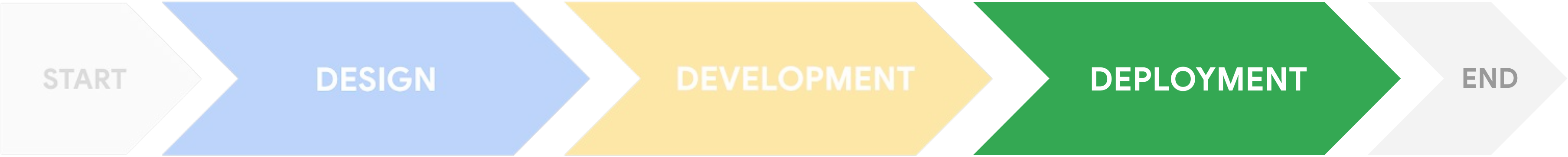
Security

Responsible AI: Human-Centered Design



Course 1

Fundamentals of TinyML

- **What** am I building?
- **Who** am I building this for?
- What are the **consequences** for the user if it ***fails***?

Course 2

Applications of TinyML

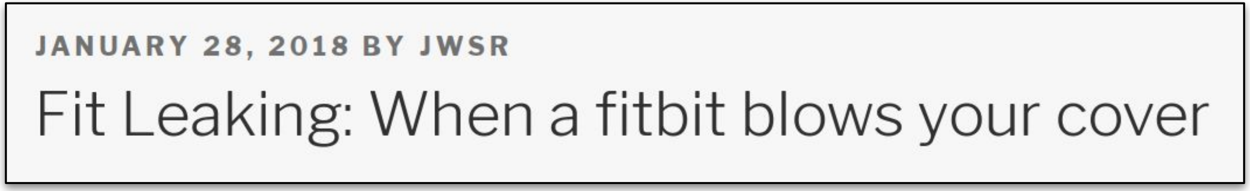
- **What data** will be collected to train the model?
- Is the dataset **biased**?
- How can we **ensure** the model is **fair**?

Course 3

Deploying TinyML

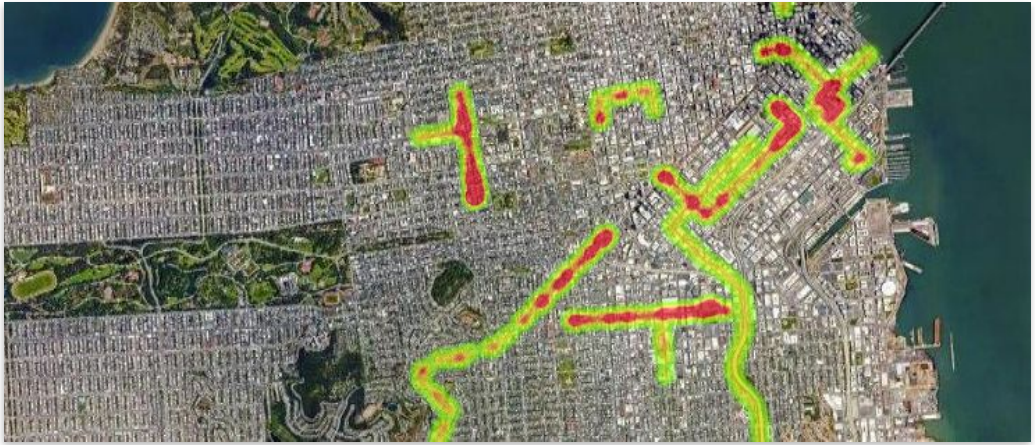
- How will model drift be monitored?
- How should **security breaches** be addressed?
- How should the user's privacy be protected?

Data Leaks

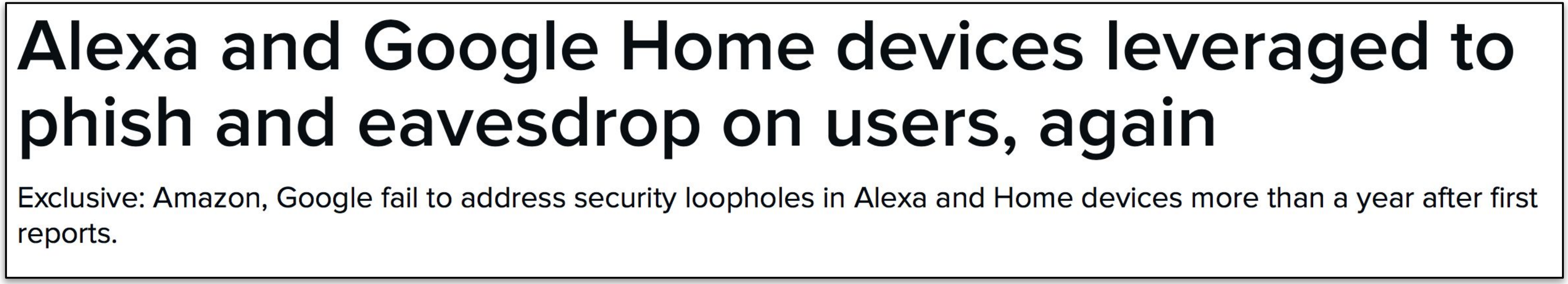


JANUARY 28, 2018 BY JWSR

Fit Leaking: When a fitbit blows your cover

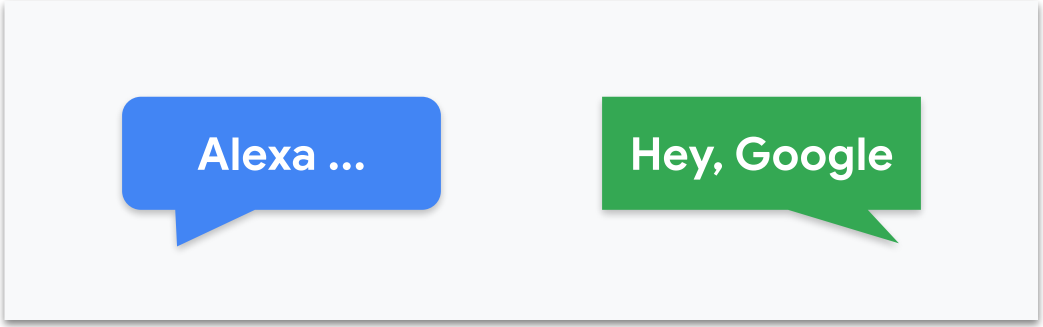


Data Breaches

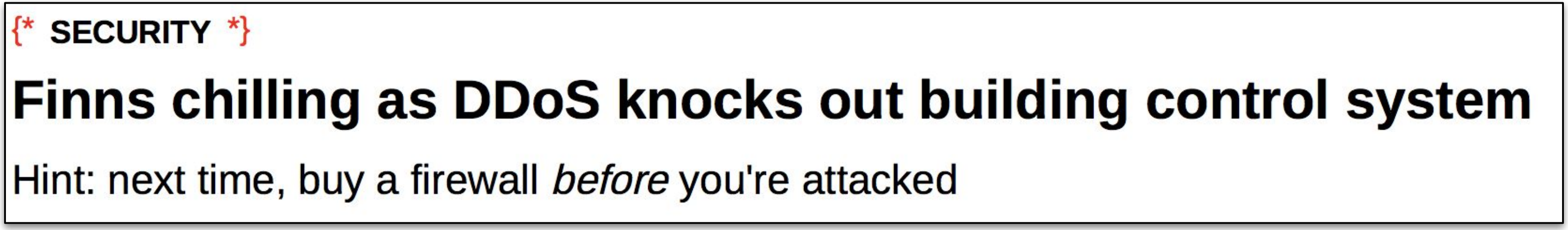


Alexa and Google Home devices leveraged to phish and eavesdrop on users, again

Exclusive: Amazon, Google fail to address security loopholes in Alexa and Home devices more than a year after first reports.



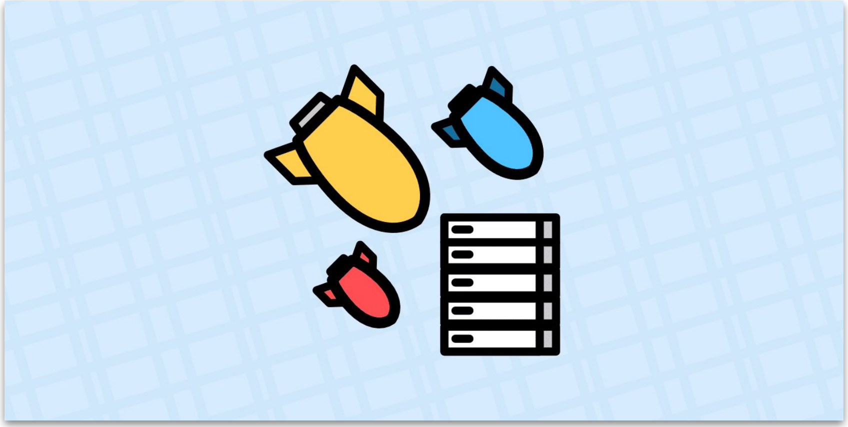
Attack: **DDoS**



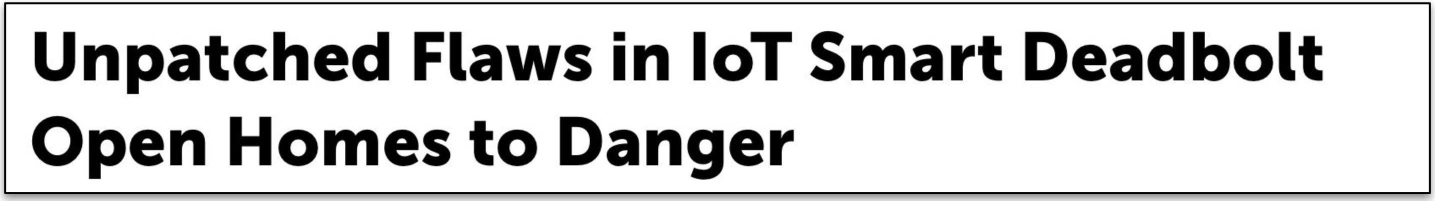
{* SECURITY *}

Finns chilling as DDoS knocks out building control system

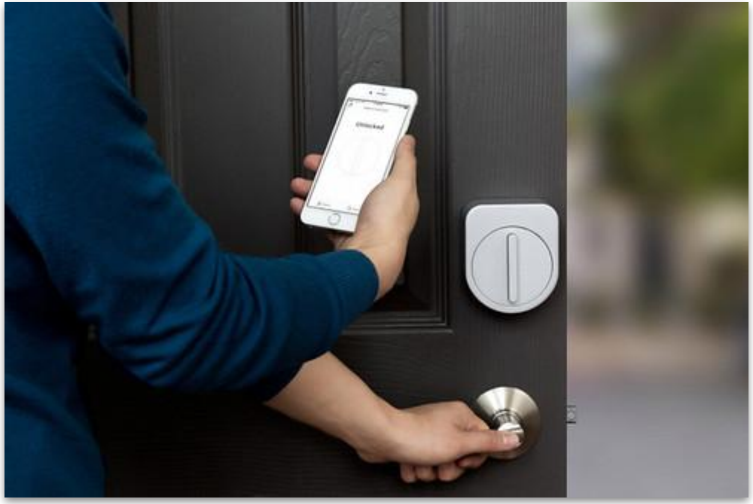
Hint: next time, buy a firewall *before* you're attacked



Attack: Exploiting **Vulnerabilities**



Unpatched Flaws in IoT Smart Deadbolt Open Homes to Danger



Adversarial Attacks: **TinyML**

Fooling the machine

failure to trigger wake word

DolphinAttack

succeeds in triggering wake word

Who values security?

individual user

service provider

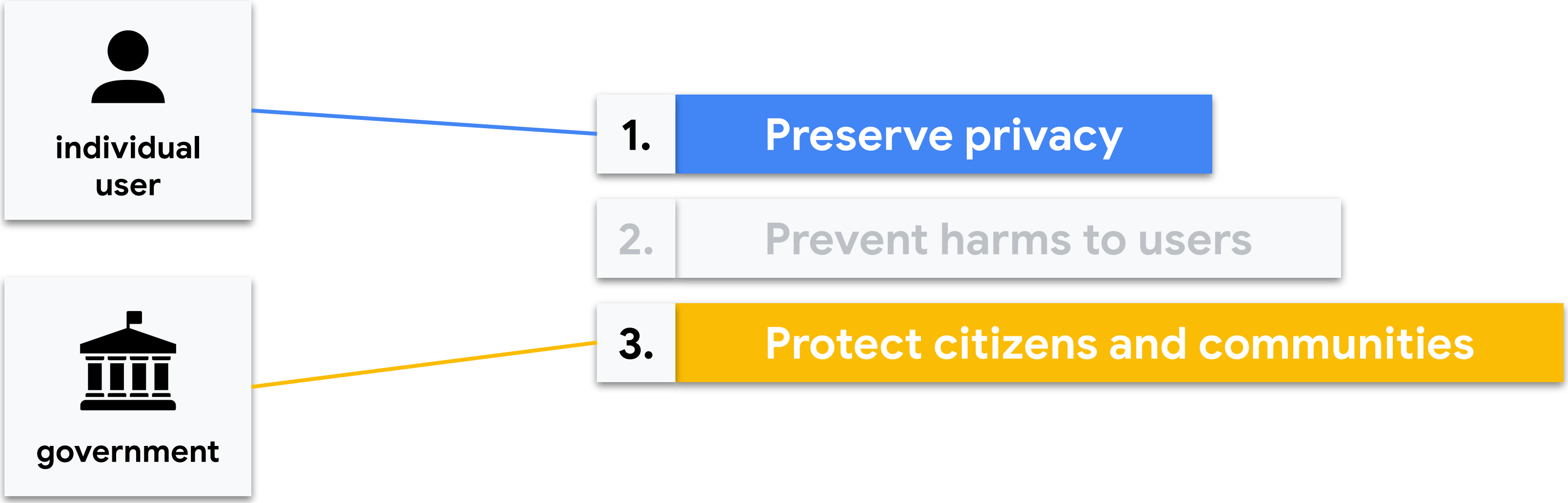
cloud provider

government

Why is security valuable?

1. Preserve privacy
2. Prevent harms to users
3. Protect citizens and communities

Competing reasons



1. Preserve privacy
2. Prevent harms to users
3. Protect citizens and communities

What should we **do**?

- **Minimize** hardware design
  - Limit opportunities for attackers
- Sensor-fusion models
  - Make the **model more resilient** against attacks
- **Encryption** techniques
  - Minimize risk of privacy violations
- Map the stakeholders and reasons to value security
  - Identify **competing interests**