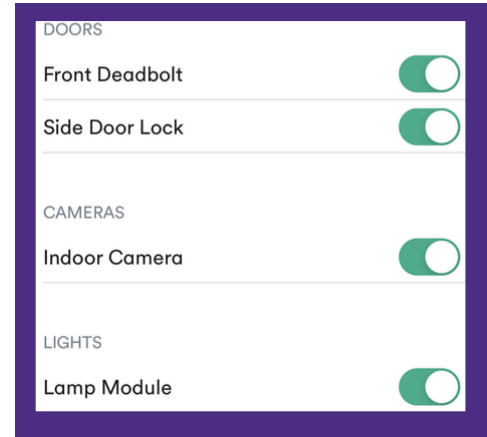


The Need for a New Model

Smart home platforms are becoming increasingly common but pose a heightened risk due to the current permission model, which often leads to apps having more access than they need.

Current permission models are similar to smartphone operating systems where permissions are separated by the device that performs them rather than their functionality. Due to the risk asymmetry, this can lead to over privilege, which can drastically increase the potential for damage if apps are malicious or exploitable. For example, “door.unlock” provides access to burglars but “door.lock” could lead to getting locked out.



Current function-based model

The Tyche Model

Tyche is a secure development methodology that leverages the risk-asymmetry in physical device operations to limit the risk that apps pose to smart home users without increasing the user’s decision overhead.

Permissions	Low-Risk	Medium-Risk	High-Risk
lock	–	lock()	unlock(), lock
alarm	–	strobe(), siren(), alarm	–
switch	switch	–	on(), off()

Tyche risk-level-based model

To do this, Tyche introduces a risk-based permission model, categorizing device operations into high, medium, and low risk rather than physical objects (ie, door). By maintaining permission grouping but instead sorting based on risk rather than function it maintains usability while decreasing risk.

The Tyche model has been validated through a user study showing that user-perceived risk closely matches expert assessments making permission prompt UI designs that focus on incorporating risk indicators viable and safe.

Implementation

- Tyche uses app rewriting techniques to enforce the risk-based permissions and to ensure minimal code changes for developers, promoting ease of adoption.
- Tyche user research methodology and permission model design should serve as a set of guiding principles for developers of future smart home platforms.