THE REFERENCE FOR THE OPEN HOUSE CARD GAME · V1.0 · 2026-11-03

Smart Home Threat Taxonomy

169 threats in 13 suits, and 10 structural hazards. Every entry has the threat, the mitigation principle a sound design follows, design measures, and mappings to STRIDE, CAPEC 3.9 and CWE 5.0. The ID on each entry is the ID printed on its card.



LICENCE

Smart Home Threat Taxonomy v1.0. © 2026 Jonathan Brett Crawley. Licensed under CC BY-NC-ND 4.0 (https://creativecommons.org/licenses/by-nc-nd/4.0/), with additional permissions from the copyright holder: you may use it in commercial threat modeling work, use it for internal training, and quote individual entries with attribution. Shipping it in a product or service, in whole or in part, needs the author's written permission. Attribution: Smart Home Threat Taxonomy v1.0, Brett Crawley, https://ostering.com/taxonomies/smart-home/

OSTERING.COM/TAXONOMIES/SMART-HOME/ · © 2026 JONATHAN BRETT CRAWLEY

HOW TO READ THIS TAXONOMY

Suits and IDs

Each ID has three parts joined by hyphens: OPH for Open House, the suit and the card value. OPH-CM-Q is the Queen of Cameras and Doorbells; OPH-TR-3 is the third structural hazard. Within a suit, values rank severity: A is the most severe, 2 the least. † marks a physical-safety consequence. Empty CAPEC or CWE cells are deliberate: many smart home threats have no equivalent.

CODE	SUIT	DECK	ENTRIES	WHAT IT COVERS
OPH-HB	**Hub and Bridges**	The Things	13	The hub is the house's local brain: it holds the network keys for every device, runs the rules and speaks for the house to the cloud. Whoever owns the hub owns the house.
OPH-RF	**Radio and Mesh**	The Things	13	Zigbee, Z-Wave, Thread, Bluetooth, Wi-Fi and the 433 and 868 MHz bands carry the house's commands through walls and past the property line. Anyone within range is part of the network's threat model.
OPH-DM	**Domotics**	The Things	13	Lighting, heating and cooling, blinds, plugs and relays, water valves and leak sensors: the building services that the house runs on. A bad command here is a physical event: heat, cold, water or darkness.
OPH-CM	**Cameras and Doorbells**	The Things	13	Indoor and outdoor cameras, video doorbells, recorders and their clips put the inside of the house, and the people in it, on the network. Every flaw is a window into a private space.
OPH-AL	**Alarms and Locks**	The Things	13	Intrusion alarms, smoke and carbon monoxide alarms, smart locks, keypads, garage doors and gates: the devices that decide who comes in and whether anyone hears about it.
OPH-AP	**Appliances**	The Things	13	Ovens and hobs, washing machines, fridges and freezers, robot vacuums and mowers, televisions and water heaters. Connecting them adds remote commands to machines that heat, spin, cut and see.

CODE	SUIT	DECK	ENTRIES	WHAT IT COVERS
OPH-EN	**Energy**	The Things	13	Solar inverters, home batteries, EV chargers, heat pumps as flexible loads, smart meters and the energy manager that plays them against the tariff. Connected energy devices act on the grid as well as on the house.
OPH-NW	**Home Network**	The Control	13	The router, the Wi-Fi, the guest network and the house's path to the internet. Most smart home products assume the home network is friendly; it rarely is.
OPH-CL	**Vendor Cloud**	The Control	13	The vendor's service that binds devices to accounts, relays commands, stores events and links to other ecosystems. One cloud serves a million houses, so its mistakes are made a million times.
OPH-RC	**Remote Control**	The Control	13	The phone in a pocket, the computer at work, the tablet on the wall and the watch on a wrist: the clients that control the house from anywhere. Each one is a key that can be lost, copied or borrowed.
OPH-VA	**Voice and Automations**	The Control	13	Voice assistants, routines and scenes, rules and scripts, third-party skills and AI agents: the layer that turns words and events into actions on the house without a person pressing a button.
OPH-HH	**Household**	The Control	13	The people in the house: partners, children, lodgers, guests, cleaners, landlords and installers. A smart home has many users with different interests, and most products model one owner.
OPH-LC	**Lifecycle**	The Control	13	Manufacture, onboarding, updates, support, resale and disposal. A house lasts for decades, its devices are supported for a few years, and the house changes hands with the devices still on the walls.
OPH-TR	**Structural Hazards**	Both decks (Trumps)	10	Structural hazards are properties of the connected home as a whole, not single faults. In the game they play as Trumps, in both decks; deal them against the whole design before the suits.

HB · Hub and Bridges

The hub is the house's local brain: it holds the network keys for every device, runs the rules and speaks for the house to the cloud. Whoever owns the hub owns the house.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-HB-A †	**Hub Holds Every Key.** The hub stores the Zigbee, Z-Wave and Thread network keys, every pairing secret and the tokens for each linked cloud in one place, so a single compromise of the hub is a compromise of the whole house.	Treat the hub as the home's root of trust, and limit what any one compromise of it yields.	1. Keep network keys and tokens in a secure element or the platform keystore, never in plain configuration files. 2. Scope each integration's token to the devices and actions it needs, so one leak does not hand over every device. 3. Support re-keying each radio network after a suspected compromise without re-pairing every device by hand.	E, I	CAPEC-37	CWE-312 CWE-522
OPH-HB-K †	**Unauthenticated Local API.** The hub exposes an HTTP, WebSocket or MQTT interface that trusts anything on the home network, so any compromised device or visitor's phone on the Wi-Fi can drive the locks and the alarm.	Authenticate every local client; the home network is not a trust boundary.	1. Require paired, per-client credentials (tokens or mutual TLS) for every local interface. 2. Separate read scopes from control scopes, and require confirmation for locks, alarms and heat appliances. 3. Ship unused local protocols (MQTT, Telnet, UPnP control points) disabled.	S, E	none	CWE-306

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-HB-Q	**Admin Page Driven from a Web Page.** The hub's admin pages can be driven by any web page a household browser visits, through cross-site requests, DNS rebinding or script in device names, so a malicious advert reconfigures the house.	Treat every browser on the home network as an untrusted intermediary.	1. Check the Host and Origin headers on every request to block DNS rebinding. 2. Protect every state-changing call with anti-forgery tokens and SameSite cookies. 3. Encode device-supplied names and labels wherever the interface renders them, behind a strict Content Security Policy.	T, E	CAPEC-62	CWE-352 CWE-346
OPH-HB-J	**Integration Runs as the Hub.** Third-party integrations, add-ons and community components run inside the hub process with its full rights, so one malicious or compromised integration reads every key and drives every device.	Run each integration with least privilege, isolated from the core and from the others.	1. Run integrations in separate processes or containers with declared permissions per device class. 2. Sign and review integrations in the store, and show the publisher and permissions before install. 3. Let the owner revoke an integration and every token it holds in one step.	E, T	CAPEC-446	CWE-829

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-HB-10	**Device Reports Become Commands.** The hub renders or evaluates whatever a device reports (its name, model string or attribute values), so a malicious or spoofed device injects script into dashboards or expressions into rules.	Treat everything a device reports as untrusted input.	1. Validate reported values against the device type's schema and physical range. 2. Encode device-supplied strings everywhere they are displayed. 3. Never pass device data into shell commands, templates or rule expressions without escaping.	T	CAPEC-592	CWE-79 CWE-1287
OPH-HB-9	**Join Mode Left Open.** The hub accepts new devices whenever join mode is on, for minutes at a time, from a remote command and without an install code, so a device within radio range joins the network and receives its key.	Make joining a short, deliberate, local and authenticated act.	1. Require install codes, QR setup codes or a DSK (Zigbee install codes, Z-Wave S2, Matter setup payloads). 2. Open join windows only from a physical action, keep them short, and show that they are open. 3. Notify the owner of every new device and hold it out of automations until confirmed.	S, E	CAPEC-151	CWE-1390
OPH-HB-8	**Debug Port Left Open.** Hubs ship with UART consoles, JTAG, SSH, Telnet, ADB or a vendor support tunnel enabled, so anyone with the box in hand, or on the network, gets a root shell.	Ship hubs in release configuration, with every non-production interface closed.	1. Lock or fuse debug interfaces, and require authentication on any console that remains. 2. Open a vendor support tunnel only per session, with the owner's consent, and log it. 3. Inventory listening services in release testing and fail the build on any that are unexpected.	E	CAPEC-121	CWE-1191 CWE-1269

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-HB-7	**Backup Carries the House.** Hub backups hold every key, token, the Wi-Fi password and the camera credentials, and are written unencrypted to cloud drives, network storage or email.	A backup holds the same secrets as the hub, so protect it like the hub.	1. Encrypt backups by default under a key the owner holds. 2. Wrap secrets separately so a partial backup can be shared for support without them. 3. Warn when backups go to a location outside the owner's control.	I	CAPEC-150	CWE-312
OPH-HB-6	**Bridge Flattens Trust.** A bridge translates a weak link (433 MHz, legacy Zigbee, a cloud-only device) into a strong one (Matter, the hub's own API) and drops its security level, so the controller treats an unauthenticated device as authenticated.	Carry the security level of the weakest hop through to the controller and the user.	1. Expose each bridged device's underlying link security as an attribute the controller can read. 2. Refuse unlock and disarm commands through links that cannot authenticate. 3. Mark bridged devices visibly in every app and dashboard.	S, T	CAPEC-700	none
OPH-HB-5 †	**Hub Down, House Dumb.** When the hub crashes, reboots, loses power or its storage fails, the devices that depend on it stop working: lights, heating schedules, the alarm, the door.	Design for the hub being absent; every device keeps a safe state and a manual control.	1. Have devices hold their last safe state and keep local manual control when the hub disappears. 2. Add a watchdog and battery backup to hubs that control security or heating. 3. Alert the owner when the hub stops checking in, through a path that does not need the hub.	D	none	CWE-754

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-HB-4	**Chatty Device Starves the Hub.** A faulty or malicious device floods the hub with reports or joins, so rule processing backs up and an alarm or leak event is acted on minutes late.	Give safety events their own lane, and bound what any one device can consume.	1. Rate-limit reports per device and quarantine a device that exceeds them. 2. Process alarm, smoke, leak and lock events in a priority queue ahead of telemetry. 3. Report queue delay as a health metric and alert when it grows.	D	CAPEC-125	CWE-770
OPH-HB-3	**Clock Moved, Rules Fire.** The hub takes its time from unauthenticated NTP or the network, so an attacker who shifts the clock fires 'morning' rules at night, expires certificates or replays one-time codes.	Authenticate time, and bound how far and how fast it may move.	1. Use authenticated time (NTS) from more than one source, with a real-time clock as a sanity check. 2. Reject or flag jumps larger than a set threshold, and hold security schedules until time is trusted. 3. Log every time correction with its size and source.	T	none	none
OPH-HB-2	**Logs Without Names.** The hub records that the door unlocked or the alarm disarmed, but not which user, app, integration or rule caused it, and a reset wipes the log, so an incident cannot be reconstructed.	Attribute every security-relevant action to a person or a rule, and keep the record off the hub.	1. Record the actor, channel and rule behind every lock, alarm and access change. 2. Forward security events to storage that survives a hub reset. 3. Let every adult in the household read the security log.	R	none	CWE-778

RF · Radio and Mesh

Zigbee, Z-Wave, Thread, Bluetooth, Wi-Fi and the 433 and 868 MHz bands carry the house's commands through walls and past the property line. Anyone within range is part of the network's threat model.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-RF-A †	**Replayed Command.** Fixed-code or weakly protected radio commands (garage doors, gates, alarm fobs, some locks) can be recorded and replayed, and rolling codes fall to jam-and-replay. *Seen: RollJam (Samy Kamkar, DEF CON 23, 2015)*	Every actuation command must be fresh and authenticated.	1. Use challenge-response or authenticated encryption with counters for every command that opens or disarms. 2. Reject out-of-window counters, and alert when jamming is followed by a valid code. 3. Do not ship fixed-code radios for doors, locks or alarms.	S, T	none	CWE-294
OPH-RF-K †	**Jammed Alarm Link.** Wireless alarm sensors and sirens are jammed, so an intrusion or a fire never reaches the panel, and the panel reads the silence as normal.	Treat jamming and loss of supervision as alarm events in their own right.	1. Supervise every wireless sensor with heartbeats and alarm on a missed deadline. 2. Detect sustained RF interference and report it to the monitoring path. 3. Give critical zones a wired or second-band fallback.	D	CAPEC-601	CWE-754

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-RF-Q	**Network Key Sent in the Clear.** Devices join under a publicly known key (the Zigbee default trust centre link key, the all-zero Z-Wave S0 temporary key), so a sniffer in range during pairing captures the network key.	Never transport a network key under a key the world knows.	1. Require Zigbee 3.0 install codes, Z-Wave S2 with a DSK, or Matter commissioning with a PAKE. 2. Refuse legacy security for lock, alarm and garage device classes. 3. Re-key the network when a legacy device must join, and log it.	I, S	CAPEC-157	CWE-1394 CWE-322
OPH-RF-J	**Downgrade to Legacy Security.** An attacker forces a device to pair in an older mode (Z-Wave S2 to S0, Bluetooth legacy or Just Works pairing), so the weak key exchange becomes the one in use. *Seen: Z-Shave (Pen Test Partners, 2018)*	Pin a minimum security level per device class and refuse to go below it.	1. Have controllers refuse S0 and legacy pairing for security device classes. 2. Record the negotiated security level and alert when it is lower than the device supports. 3. Use Bluetooth LE Secure Connections only.	T, I	CAPEC-620	CWE-757
OPH-RF-10	**Mesh Worm.** A firmware flaw spreads device to device across the mesh, and from house to house, because devices accept updates signed with a shared key that has been extracted from one of them. *Seen: IoT Goes Nuclear: Philips Hue worm (Ronen et al., IEEE S&P 2017)*	Each device verifies updates against a key that is on no device, and the mesh does not extend trust.	1. Sign firmware with an asymmetric key held off-device, and verify before install. 2. Have the coordinator authorise each over-the-air update, rather than any neighbour. 3. Disable proximity commissioning (Zigbee Touchlink) that lets one device take over another.	E, T	CAPEC-186	CWE-347 CWE-321

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-RF-9	**Spoofed Sensor.** Sensor reports (door contacts, leak, temperature, motion) are not authenticated, so a forged frame says 'door closed' during a break-in, or 'leak' to shut the water off.	Authenticate what sensors report, not only the commands sent to actuators.	1. Use authenticated encryption on sensor frames, bound to the identity set at pairing. 2. Cross-check reports for plausibility (contact closed while motion inside the door). 3. Alert on frames from unknown or duplicated device identities.	S, T	CAPEC-194	CWE-290
OPH-RF-8 †	**Phone Key Relayed.** Phone-as-key and Bluetooth proximity unlock trust that a reachable phone is a nearby phone, so a relay over any distance opens the door while the owner is in town. *Seen: Bluetooth LE relay against smart locks (NCC Group, 2022)*	Measure proximity; do not infer it from a radio that answers.	1. Use secure ranging (UWB distance bounding) for proximity unlock. 2. Require a user action (tap, biometric) on the phone to unlock. 3. Ship auto-unlock off, with a short time window when turned on.	S	CAPEC-94	CWE-290
OPH-RF-7	**Malformed Frame Crashes the Stack.** A crafted radio frame crashes or takes over the device's radio stack, because the chip vendor's SDK parses hostile input with known flaws that the product never picked up. *Seen: SweynTooth (SUTD, 2020)*	Treat the radio stack as an internet-facing parser and keep it current.	1. Fuzz the radio interfaces in release testing. 2. Track the chip vendor's SDK advisories and ship their fixes. 3. Recover from radio stack faults with a watchdog rather than a hung device.	D, E	CAPEC-28	CWE-1395

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-RF-6	**Rogue Coordinator.** A rogue Thread border router or Zigbee coordinator advertises a better route, or lures reset devices onto its network, and so sees or steers their traffic.	Devices join and route only through authenticated network authorities.	1. Authenticate border routers and coordinators before devices route through them. 2. Have devices rejoin only the network they were commissioned to, unless re-commissioned locally. 3. Alert on a second coordinator or border router on the home's network.	S, T	CAPEC-616	CWE-940
OPH-RF-5	**Stolen from Down the Street.** Proximity commissioning and remote reset (Zigbee Touchlink, factory reset over the air) work from outside the house with a high-gain antenna, so bulbs and plugs are reset and taken over.	Reset and re-commissioning need a physical act at the device.	1. Disable Touchlink and remote reset by default. 2. Require a button press or power-cycle sequence at the device to reset. 3. Alert the owner when a device leaves the network unexpectedly.	D, E	none	CWE-306
OPH-RF-4	**Battery Drained by Design.** An attacker keeps a sleepy battery device awake with traffic or join requests, draining a sensor that should last years in days, so it dies silently.	Bound the radio work a battery device does for anyone it does not know.	1. Ignore unauthenticated traffic before waking the main processor. 2. Report battery drain rate, not just level, and alert on sudden change. 3. Treat a battery-dead safety sensor as a fault alarm.	D	none	CWE-920

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-RF-3	**Leaky Airwaves.** Telemetry and advertisements go out in the clear or with fixed identifiers, so someone outside can tell which devices are present, when doors open and when the house is empty.	Encrypt what is sent, and keep identifiers from becoming trackers.	1. Encrypt telemetry on every band, including sub-GHz sensors. 2. Rotate Bluetooth and Wi-Fi addresses and avoid static identifiers in advertisements. 3. Advertise only while pairing or when a client needs it.	I	CAPEC-157	CWE-319 CWE-359
OPH-RF-2	**Crowded Spectrum.** The design assumes a clean 2.4 GHz band, but Wi-Fi channels, microwave ovens and the neighbours' networks overlap the mesh, so commands are lost and nobody can tell attack from accident.	Plan channels and measure link quality as part of the system.	1. Choose mesh channels clear of the home Wi-Fi and re-check them over time. 2. Retry with acknowledgement for actuation commands, and report delivery failure. 3. Expose link quality per device so a degraded link is visible before it fails.	D	none	none

DM · Domotics

Lighting, heating and cooling, blinds, plugs and relays, water valves and leak sensors: the building services that the house runs on. A bad command here is a physical event: heat, cold, water or darkness.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-DM-A †	**Heating Driven Out of Range.** Thermostats, boilers and heat pumps accept setpoints from the app or cloud with no limit in the device, so a command, bug or attacker drives the house to dangerous heat or cold.	Enforce physical safety limits in the device, not in the app.	1. Hold hard minimum and maximum setpoints in firmware that no remote command can override. 2. Keep frost protection active whatever mode the system is in. 3. Alert the household on extreme or sudden setpoint changes.	T	CAPEC-153	CWE-1284 CWE-602
OPH-DM-K †	**Plug Powers a Hazard.** Smart plugs and relays switch whatever is plugged in, so a remote 'on' energises a heater, iron or hair straightener with nobody home, or rapid switching overheats the load.	Safe switching depends on the load, so the device must know what it is switching.	1. Ask for the load type at setup and block remote 'on' for heat loads unless confirmed at the plug. 2. Build overcurrent, overtemperature and maximum on-time protection into the plug. 3. Rate-limit relay switching in firmware.	T	none	CWE-799

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-DM-Q †	**Water Valve Turned on the House.** A whole-house shut-off valve can be closed or opened by any app user, rule or integration, and its state on power loss was never chosen, so the house floods or loses water for heating and sprinklers.	Treat a valve that controls the whole supply as a security-critical actuator.	1. Restrict valve control to named roles and confirm every remote change. 2. Keep a manual override at the valve that no software can disable. 3. Choose and document the fail state on power loss for each installation.	T, D	none	CWE-862
OPH-DM-J †	**Thermostat Held to Ransom.** A malicious update, a PIN set by an attacker or a hostile setting puts a device in a state the owner cannot recover, and the heating is held to ransom. *Seen: Thermostat ransomware demonstration (Pen Test Partners, DEF CON 24, 2016)*	The owner keeps a recovery path that an attacker cannot remove.	1. Provide a physical reset that restores signed factory firmware. 2. Keep a known-good firmware image and roll back to it on failed boot. 3. Never let a remote command disable the local controls.	D, E	CAPEC-186	CWE-494
OPH-DM-10 †	**Window Opened, Blind Closed.** Motorised windows, skylights, blinds and shutters move on a remote command or a rule while someone is in the way, or open the building envelope while the house is empty.	Moving parts need local interlocks, and opening the envelope needs the security context.	1. Build obstacle detection and force limits into the motor controller. 2. Block opening windows and skylights when the alarm is armed or the house is in away mode. 3. Ship remote opening of ground-floor windows off.	T	none	none

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-DM-9 †	**Wall Switch Disconnected.** Smart relays and bulbs detach the wall switch from the light, so when the hub, network or cloud fails, nobody can turn on a light at night or in a fire.	Keep a local manual path that works without any software.	1. Wire wall switches so they always control the load directly, or through local logic only. 2. Have bulbs and relays fall back to 'on' when switched off and on at the wall. 3. Test lighting with the hub and the internet both down.	D	none	none
OPH-DM-8 †	**Wrong State After a Power Cut.** After a power cut, devices return to 'on' (heaters, plugs) or 'off' (a freezer plug, a sump pump) by a default nobody chose for that load.	Define power-on behaviour per load, with a safe default per class.	1. Make the power-on state configurable, defaulting heat loads to off and essential loads to on. 2. Tell the household which devices changed state when power returned. 3. Never let a heat load start unattended after a power cut.	D, T	none	CWE-1419
OPH-DM-7 †	**Strobe from a Command.** Smart lights accept colour and brightness changes as fast as they can be sent, so a malicious app or rule can strobe a room at a rate that can trigger photosensitive seizures.	Limit flash rate in the bulb's firmware.	1. Cap the rate of brightness and colour change in firmware, whatever the source. 2. Make any 'effects' mode a local, opt-in setting. 3. Throttle commands per source at the hub.	T	none	CWE-799

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-DM-6	**Cycled to Destruction.** Commands toggle a compressor, boiler or heat pump on and off faster than it is built for, wearing it out or tripping it into lockout in cold weather.	Protect equipment in firmware with minimum on and off times.	1. Enforce minimum run and rest times in the equipment controller. 2. Rate-limit setpoint changes from any one source. 3. Alert on abnormal cycling patterns.	T, D	none	CWE-799
OPH-DM-5	**Someone Else's Thermostat.** A utility, energy supplier or the vendor can change the setpoint for demand response without the household seeing it in time, and the house gets too hot or too cold. *Seen: Texas heat wave demand-response thermostat adjustments (June 2021)*	Third-party control is visible, bounded and overridable by the people at home.	1. Show any third-party adjustment on the device and in the app as it happens. 2. Bound how far and for how long a third party can move the setpoint. 3. Let the household override, and record who changed what.	T, R	none	none
OPH-DM-4	**All Off Means All.** An 'all off' scene or group switches off loads that must stay on (a fridge, freezer, aquarium, sump pump or equipment someone relies on), and one changed scene affects them all.	Mark essential loads, and keep them out of bulk commands.	1. Let installers and owners flag essential loads at setup. 2. Exclude essential loads from groups and scenes unless explicitly added. 3. Confirm bulk commands that include an essential load.	D	none	CWE-1220

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-DM-3	**One Sensor Decides.** A single cheap temperature or humidity sensor drives the heating and frost protection, so a failed, moved or spoofed sensor decides for the whole house.	Cross-check safety decisions against more than one source.	1. Compare room sensors with the boiler or heat pump's own readings. 2. Flag readings that are flat, out of range or out of step with others. 3. Fall back to a safe schedule when a sensor is in doubt.	T, D	none	CWE-1357
OPH-DM-2	**Predictable Away Mode.** Away mode runs a fixed lighting and blind schedule, and the away state is readable by integrations, so the empty house is easy to recognise from the street or a feed.	Presence simulation should be unpredictable, and away status private.	1. Randomise simulated presence within plausible ranges. 2. Do not expose away status to integrations unless the owner grants it. 3. Keep away-mode changes out of notifications visible on lock screens.	I	none	CWE-359

CM · Cameras and Doorbells

Indoor and outdoor cameras, video doorbells, recorders and their clips put the inside of the house, and the people in it, on the network. Every flaw is a window into a private space.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CM-A	**Someone Else's Feed.** A cloud, cache or relay fault serves one household's live view, events or thumbnails to another household's app. *Seen: Wyze cameras showed other users' events (Sept 2023 and Feb 2024)*	Bind every frame and event to its home at every layer, and test the binding.	1. Check the requesting account's ownership on every stream, clip and thumbnail request, not just at login. 2. Key caches and CDN paths by household as well as by device, and test for crossover. 3. Encrypt end to end so a routing fault exposes ciphertext, not video.	I, E	none	CWE-639 CWE-524
OPH-CM-K	**Default Login on the Recorder.** Cameras and recorders ship with default or weak credentials, or hidden support accounts, and are reachable from the internet through P2P services or port mappings. *Seen: Mirai botnet (2016)*	Every device has unique credentials and no hidden accounts.	1. Ship a unique per-device password, or force one to be set before the device works. 2. Remove hidden, support and hard-coded accounts from release firmware. 3. Disable P2P and port mapping until the owner turns remote access on.	E, S	CAPEC-70	CWE-1392 CWE-798

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CM-Q	**Stranger in the Camera.** Camera accounts protected by a password alone are taken over by credential stuffing, and the attacker watches and talks to the household through the camera. *Seen: Ring camera takeovers (Dec 2019)*	Protect a camera account as if it were the camera.	1. Require multi-factor authentication or passkeys at setup. 2. Check passwords against breach corpora and flag unusual logins. 3. Notify every household member of new logins and live-view sessions.	S, I	CAPEC-600	CWE-307 CWE-308
OPH-CM-J	**Local Only That Isn't.** The product says video stays local or is end-to-end encrypted, but thumbnails, clips or face data still go to the cloud, unencrypted or viewable by URL. *Seen: Eufy cloud thumbnails and unencrypted streams (Nov 2022)*	The data flow must match the promise, and be tested against it.	1. Keep a data-flow inventory per feature and test it in every release. 2. Hold end-to-end keys only on the owner's devices. 3. Publish what leaves the home, and when.	I	none	CWE-359 CWE-319
OPH-CM-10	**Insider Watches the Feed.** Vendor staff, contractors or support agents can view customer video, or an installer adds their own account to a customer system. *Seen: FTC action against Ring (2023); ADT technician case (disclosed 2020, guilty plea 2021)*	No standing human access to customer video.	1. Encrypt end to end so staff cannot view video at all. 2. Grant support access only with the customer's consent per session, and log it where the customer can see it. 3. Expire installer accounts at handover.	I, E	CAPEC-122	CWE-1220

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CM-9	**Device ID Is the Password.** A vendor P2P SDK treats the device's UID as enough to connect, so anyone who learns a UID can impersonate the device or intercept its stream. *Seen: ThroughTek Kalay, CVE-2021-28372 (Mandiant, 2021)*	Identifiers are not secrets; authenticate with per-device keys.	1. Use mutual authentication with per-device keys for P2P and relay connections. 2. Keep third-party camera SDKs on supported, patched versions. 3. Treat UIDs as public in the threat model.	S, I	none	CWE-290 CWE-1395
OPH-CM-8	**Stream Open on the LAN.** RTSP and ONVIF streams answer on the home network without authentication or encryption, so any compromised device on the Wi-Fi can watch.	Authenticate and encrypt local streams as you would remote ones.	1. Require credentials for every local stream, unique per device. 2. Use encrypted transport for local streaming. 3. Ship local streaming off until the owner enables it.	I	CAPEC-158	CWE-319 CWE-306
OPH-CM-7	**Recording Without the Light.** The camera can stream or record with its indicator light off, under software control, so people in the room cannot tell they are being watched.	Tie the indicator to the sensor in hardware.	1. Wire the recording indicator to the camera and microphone power. 2. Provide a physical shutter or microphone switch on indoor cameras. 3. Show who is watching live, in the app, to every household member.	I	CAPEC-634	CWE-359

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CM-6	**Footage Shared Beyond the Owner.** Clips are shared through neighbourhood apps, police portals or links that never expire and can be guessed, and the owner cannot see who has them. *Seen: Ring disclosures to police without consent (2022)*	Sharing is opt-in, scoped, expiring and visible to the owner.	1. Use signed, expiring share links with enough entropy. 2. Show the owner a log of every disclosure, including legal requests. 3. Publish the vendor's policy for emergency and legal requests.	I	none	CWE-340 CWE-359
OPH-CM-5	**Camera Sees the Neighbours.** Doorbells and outdoor cameras record the street, the neighbours' gardens and conversations by default, putting the household in breach of privacy law. *Seen: Fairhurst v Woodard (England, 2021)*	Capture only the owner's property by default.	1. Ship privacy zones and audio-off as outdoor defaults. 2. Show the field of view at setup and prompt for masking. 3. Explain the household's obligations where recording reaches beyond the boundary.	I	none	none
OPH-CM-4	**Doorbell Off the Wall.** A video doorbell comes off the wall with a standard screwdriver, and its flash holds the home Wi-Fi password and account tokens in plain text.	Removal is a tamper event, and no secret survives in plain text.	1. Alert the owner when the doorbell is removed from its mount. 2. Encrypt stored credentials with a device-bound key. 3. Use a mount that needs a security screw.	T, I	CAPEC-401	CWE-312

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CM-3	**Alerts Until They're Off.** An attacker trips the motion alerts again and again, until the owner mutes them or turns the camera off, and then comes back.	Design alerting so it stays on when it matters.	1. Rate-limit and summarise repeated alerts rather than leaving muting as the only option. 2. Time-limit any mute, and confirm when the camera is turned off. 3. Escalate when alerts are muted while the alarm is armed.	D	none	none
OPH-CM-2	**Clips Kept Forever.** Clips and event history are kept with no limit, so years of comings and goings, children and visitors sit in the account for anyone who gets into it.	Keep the least footage for the shortest time.	1. Ship a short default retention and let the owner extend it. 2. Delete clips everywhere, including backups and analytics, on schedule. 3. Show the owner how much history is held.	I	none	none

AL · Alarms and Locks

Intrusion alarms, smoke and carbon monoxide alarms, smart locks, keypads, garage doors and gates: the devices that decide who comes in and whether anyone hears about it.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-AL-A †	**Unlocked Without Intent.** Any authenticated call (app, voice, automation or integration) can unlock the door or disarm the alarm without fresh intent from a person, so a stolen token or a misfiring rule opens the house.	Unlocking and disarming need fresh, explicit intent from an authorised person.	1. Require step-up authentication (biometric or PIN) on the device that sends the unlock or disarm. 2. Keep voice unlock and disarm off by default, and require a spoken PIN when on. 3. Allow unlock in automations only by explicit, per-rule approval, and notify on every use.	E, S	none	CWE-308 CWE-862
OPH-AL-K †	**Smoke Alarm Silenced.** Connected smoke and CO alarms can be hushed or tested remotely, or the smart layer suppresses the local siren because the alert was 'handled in the app'.	The local siren never depends on the network.	1. Keep the siren path independent of the networking firmware. 2. Time-limit and log remote hush, and never allow it for carbon monoxide. 3. Escalate an unacknowledged alarm to every household member and contact.	D, T	none	CWE-1320

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-AL-Q †	**Fails Open, Fails Shut.** On a flat battery, power loss or crash the lock fails open (insecure) or fails locked, trapping people in a fire, because no one chose the failure state for that door.	Choose and document the failure state per door, and always allow exit.	1. Keep mechanical exit from inside at all times. 2. Document the fail state per installation and test it. 3. Warn weeks ahead of a flat battery, through more than one channel.	D	none	CWE-636
OPH-AL-J	**Keypad Code Guessed.** Keypads accept short codes with no lockout, show wear and smudge on the used digits, and shared codes never change.	A keypad code is a password: long enough, rate-limited and changed.	1. Lock out after repeated failures, with an alert. 2. Support longer codes and decoy digits (scramble before or after the code). 3. Prompt code changes when a code holder leaves.	S	CAPEC-49 CAPEC-626	CWE-307 CWE-521
OPH-AL-10	**Guest Code Outlives the Guest.** Temporary codes and e-keys for cleaners, holiday guests and trades never expire, or stay valid offline after revocation because the lock caches them.	Time-bound credentials are enforced by the lock, even offline.	1. Enforce validity windows in the lock itself. 2. Give cached credentials an expiry that does not need the network. 3. Show the owner every live credential, and who issued it.	E	none	CWE-324
OPH-AL-9	**Garage Is the Side Door.** The garage door or gate has weaker controls than the front door (a fixed code, a cloud API with no step-up, auto-open by geofence), yet it opens onto the house.	Any door into the house gets front-door controls.	1. Apply the same authentication and notification to garage and gate as to the front door. 2. Alert when a garage door stays open past a set time. 3. Close and lock the internal garage door when the house is armed.	E, T	none	CWE-1390

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-AL-8	**Arming State Leaks.** Armed or disarmed status, entry delays and lock state are readable by integrations, voice assistants and widgets, so someone outside learns when the house is open.	Security state is shown only to those who need it.	1. Require a scope for reading arming and lock state, granted per integration. 2. Keep security state off lock screens and voice answers by default. 3. Log every read of security state by an integration.	I	none	none
OPH-AL-7 †	**Unlocked by a Fake Arrival.** The lock opens or the alarm disarms when the owner's phone 'arrives' in a geofence, so a spoofed location or drifting fix opens the door while the owner is away or in bed nearby.	Location is a hint, not an authenticator.	1. Combine location with a second, local signal and a prompt on the phone. 2. Ship geofence unlock and disarm off. 3. Never act on location alone at night or when the house is armed.	S	CAPEC-627	CWE-807
OPH-AL-6	**Tamper Goes Unreported.** A lock forced off the door, a sensor cover opened or a siren wire cut raises no tamper alarm, or raises one only when the network is up.	Tamper is an alarm event, sent by more than one path.	1. Fit tamper switches to locks, sensors, sirens and panels. 2. Report tamper over a backup path when the main one is down. 3. Keep tamper alarms active when the system is disarmed.	T	CAPEC-390	none

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-AL-5	**Monitoring Path Spoofed.** The path to the alarm receiving centre (IP or cellular) can be blocked or spoofed, so the centre gets a false all-clear or a flood of false alarms.	Authenticate the alarm path and supervise it from both ends.	1. Authenticate and sequence every message to the receiving centre. 2. Have the centre poll the panel and act when polls fail. 3. Use dual-path signalling with independent networks.	S, D	CAPEC-194	CWE-290
OPH-AL-4	**Smashed in the Entry Delay.** An intruder destroys the panel during the entry delay, before it has sent anything, so the alarm never reaches anyone.	Signal at the start of the entry delay, not the end.	1. Send a pre-alarm to the monitoring path when the entry delay starts. 2. Treat a pre-alarm with no disarm as an alarm. 3. Mount the panel away from the entry door.	D	none	none
OPH-AL-3	**Digital Lock, Mechanical Weakness.** A smart lock is fitted to a weak cylinder or keeps a pickable key override, and the threat model covers only the electronics.	Model the physical lock with the digital one.	1. Specify cylinders that meet an anti-snap or anti-pick standard for retrofit locks. 2. Document the mechanical override and its rating. 3. Report forced or unusual mechanical operation where the lock can detect it.	E	CAPEC-393	none
OPH-AL-2	**Shared Code, No Name.** The household shares one code or one account, so the log says 'code 1 unlocked the door' and nobody can tell who it was.	Every person who can open the door has their own credential.	1. Issue a code or e-key per person, including regular visitors. 2. Name every credential in the log. 3. Make shared codes a visible exception with an expiry.	R	none	CWE-1220

AP · Appliances

Ovens and hobs, washing machines, fridges and freezers, robot vacuums and mowers, televisions and water heaters. Connecting them adds remote commands to machines that heat, spin, cut and see.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-AP-A †	**Oven Lit Remotely.** An oven, hob, kettle or tumble dryer can be started from the app or cloud with nobody home, so a stolen account, a bug or a mistaken tap starts a fire.	Heat appliances start remotely only after someone at the appliance has allowed it.	1. Allow remote start only after a local 'remote start' action at the appliance within a set time. 2. Never allow remote start of a hob, and cap remote run time for ovens and dryers. 3. Check door, load and sensor state before starting.	T, E	none	CWE-654
OPH-AP-K †	**Safety Limit in Software Only.** Over-temperature and pressure limits (water heaters, dryers, ovens) live in updatable firmware rather than an independent cut-out, so malicious firmware or a bad update removes them.	Keep an independent hardware safety limit that firmware cannot override.	1. Fit a thermal cut-out or pressure relief that works with the firmware off. 2. Verify the firmware's own limits against the hardware's at boot. 3. Sign firmware and refuse images that change safety parameters.	T	none	CWE-1338

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-AP-Q †	**Mower Starts with the Children Out.** A robot mower or pool cleaner starts on a remote command or schedule without anyone seeing the area, with children or pets in it.	Outdoor robots with blades start only when the area is known to be clear.	1. Require a local confirmation or a camera check before a remote start. 2. Stop on lift, tilt or contact detection in hardware. 3. Pause schedules when the household says people are in the garden.	T	none	none
OPH-AP-J †	**Child Lock Bypassed by App.** The appliance's physical child lock does not apply to commands from the app, cloud or voice assistant, so they start a machine a child can reach.	Remote commands honour every local safety lock.	1. Apply child lock to every command path, not just the front panel. 2. Require the lock to be released at the appliance. 3. Show lock state in the app before any remote action.	E	none	CWE-288
OPH-AP-10	**Vacuum Maps the House.** Robot vacuums with cameras and LiDAR build floor plans and take pictures inside the home, which go to the cloud, to training sets and to contractors. *Seen: iRobot development-robot images leaked by data-labelling contractors (MIT Technology Review, 2022)*	Keep maps and images on the device unless the owner chooses otherwise.	1. Process maps and images on the device and upload only with explicit consent. 2. Exclude images of people from any training or review set. 3. Let the owner delete maps and images everywhere.	I	none	CWE-359

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-AP-9	**Appliance as Foothold.** A fridge or television with an old Linux or Android build sits on the main network, so an attacker uses it as a foothold to reach the hub and the household's computers.	Appliances are untrusted network neighbours, and stay patched for their working life.	1. Keep appliance software patched for a stated support period. 2. Put appliances on an isolated segment with only the flows they need. 3. Close every inbound service the appliance does not need.	E	none	CWE-1104
OPH-AP-8	**Service Mode Password.** A hidden service mode, reached by a button sequence or a service app with a hard-coded password, lets anyone change parameters, including safety settings.	Service access is authenticated per technician and per visit.	1. Remove hard-coded service passwords; authenticate technicians individually. 2. Keep safety parameters out of reach of service mode. 3. Log service mode use where the owner can see it.	E	none	CWE-798
OPH-AP-7	**TV Watches Back.** Smart televisions recognise what is on screen and listen for voice commands, and send viewing data to advertisers and data brokers. *Seen: FTC settlement with Vizio (2017)*	Content recognition and listening are off until the owner turns them on.	1. Ship automatic content recognition off, with a clear prompt to enable. 2. Keep voice listening push-to-talk by default. 3. Disclose every recipient of viewing data.	I	none	CWE-359
OPH-AP-6 †	**Started Without Being Ready.** A washing machine or dishwasher starts on a remote command with the door open, the hose loose or the load wrong, and floods the kitchen with nobody home.	Remote start checks that the appliance is ready.	1. Check door, water supply and load sensors before a remote start. 2. Stop and alert on leak detection. 3. Require the appliance to be armed for remote start locally.	T	none	CWE-841

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-AP-5	**Freezer Off Without a Word.** A rule, scene or remote command turns off a fridge or freezer, or changes its temperature, and nothing tells the household until the food has spoiled.	Changes to cold storage are always reported.	1. Alert on any power or setpoint change to a fridge or freezer. 2. Alert on temperature drift, whatever its cause. 3. Exclude fridges and freezers from bulk scenes.	D, T	none	none
OPH-AP-4	**Setup Hotspot Left Open.** The appliance's setup hotspot stays open, or reappears with a default password, so someone nearby re-provisions it or captures the home Wi-Fi password.	The setup channel opens only on a local action and closes after setup.	1. Open the setup hotspot only after a button press, and close it after a short time. 2. Use a unique password or a PAKE for setup. 3. Never send the home Wi-Fi password in the clear during provisioning.	S, I	none	CWE-1188 CWE-319
OPH-AP-3 †	**Recipe Drives the Heat.** Ovens and cooking machines run programs downloaded from the cloud or a community, so a malicious or broken program sets temperatures and times the user never saw.	Downloaded programs run inside limits the appliance enforces.	1. Check every program step against the appliance's safe ranges. 2. Sign programs and show their temperatures and times before running. 3. Keep community programs out of remote start.	T	none	CWE-1284

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-AP-2	**Usage Data Shows the Routine.** Appliance usage (cooking times, laundry, coffee, vacuum runs) is collected and shared, and shows when the household wakes, eats and goes out.	Collect only what the feature needs, and say who gets it.	1. Collect usage data only for features the owner uses. 2. Aggregate or remove timestamps before sharing. 3. Disclose every third party that receives usage data.	I	none	CWE-359

EN · Energy

Solar inverters, home batteries, EV chargers, heat pumps as flexible loads, smart meters and the energy manager that plays them against the tariff. Connected energy devices act on the grid as well as on the house.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-EN-A †	**Fleet Switched at Once.** The vendor's cloud can command every inverter, battery or charger at once, so a compromise or a rogue operator switches thousands of homes together and destabilises the grid. *Seen: MadIoT (Princeton, USENIX Security 2018); SUN:DOWN (Forescout, 2025)*	No single control path can move a fleet at once.	1. Stagger and randomise fleet commands, and cap the power any one command can move. 2. Enforce ramp-rate limits in the device itself. 3. Require several people to approve fleet-wide commands, and log them.	T, D, E	none	CWE-1357
OPH-EN-K †	**Grid Protection Switched Off.** Inverter grid-protection settings (anti-islanding, voltage and frequency trips) can be changed through the app or an installer tool, putting line workers at risk during an outage.	Grid-code protection is locked, and changed only by an authenticated installer, with a record.	1. Lock grid-code settings to the region's approved profile. 2. Require an authenticated installer role and log every change. 3. Refuse settings outside the grid code, whoever sends them.	T, E	none	CWE-15

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-EN-Q †	**Battery Pushed Past Its Limits.** Battery management parameters (charge limits, temperature limits, charge rate) can be changed by the app, cloud or firmware, and a bad value starts thermal runaway.	Keep battery protection in hardware that firmware cannot override.	1. Enforce cell voltage and temperature limits in an independent protection circuit. 2. Sign BMS firmware and refuse parameters outside the cell maker's limits. 3. Alert and isolate on abnormal temperature rise.	T	none	CWE-1338
OPH-EN-J †	**Undisclosed Radio Inside.** An inverter or charger carries a communication path the owner cannot see or turn off (a cellular modem, a vendor tunnel), giving remote control outside the owner's network. *Seen: Undocumented communication devices reported in inverters (Reuters, May 2025)*	Every communication path is declared, and the owner can switch it off.	1. List every radio and remote path in the product documentation and the SBOM. 2. Let the owner disable vendor remote access without losing local function. 3. Show remote sessions to the owner as they happen.	I, E	none	CWE-912
OPH-EN-10	**Any Charger by Its ID.** The charger's cloud API takes a charger or account ID without checking ownership, so anyone can start, stop or reconfigure other people's chargers. *Seen: Charger API flaws at Wallbox and Project EV (Pen Test Partners, 2021)*	Check ownership on every request, not just at login.	1. Authorise every API call against the caller's ownership of the device. 2. Use identifiers that cannot be guessed, and rate-limit enumeration. 3. Test for cross-account access in every release.	E	none	CWE-639

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-EN-9 †	**Modbus Open on the LAN.** Inverters and batteries answer Modbus TCP or SunSpec on the home network without authentication, so anything on the Wi-Fi can write their registers.	Local control interfaces are authenticated, and read-only unless enabled.	1. Ship local Modbus read-only, with writes enabled by the owner. 2. Restrict local control to named clients. 3. Place energy devices on their own network segment.	T, E	none	CWE-306
OPH-EN-8	**Tariff Signal Spoofed.** Price and demand-response signals arrive unauthenticated, so a fake low price sets every charger charging at once, or a fake high price switches off the heat pump.	Authenticate price and grid signals before acting on them.	1. Verify signatures on tariff and demand-response messages. 2. Bound how much the house changes in response to any one signal. 3. Alert on signals that are outside the expected range.	S, T	CAPEC-194	CWE-290
OPH-EN-7	**Installer Portal Holds Every Site.** Installer and fleet portals reach thousands of customer systems through shared or weakly protected logins.	Installer access is per person, per site and time-limited.	1. Require multi-factor authentication for installer accounts. 2. Grant access per site and expire it after commissioning unless renewed. 3. Let owners see and revoke installer access.	E	none	CWE-308

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-EN-6	**Export Limit Lifted.** The export limit agreed with the network operator can be changed in the app, so the house exports more than its connection allows and overloads the local network.	Export limits follow the connection agreement and are enforced in the device.	1. Lock export limits to the approved value and log changes. 2. Require an installer role to change them. 3. Report exports above the limit to the owner.	T	none	CWE-15
OPH-EN-5	**Energy Manager Empties the Battery.** The energy manager chases tariffs and exports, and drains the battery that the household relies on for backup, or switches off heating, in the hour it is needed.	Backup reserve and comfort limits come before optimisation.	1. Keep a reserve the optimiser cannot use. 2. Let the household set comfort floors the optimiser respects. 3. Show what the optimiser did and why.	D	none	none
OPH-EN-4	**Meter Data Shows the Household.** Detailed consumption data shows when people wake, cook, shower and leave, and which appliances they own, and is shared with suppliers and third parties.	Collect at the resolution the purpose needs, and share only with consent.	1. Default to the lowest resolution the tariff needs. 2. Ask consent separately for each third party. 3. Let the household see and delete detailed data.	I	none	CWE-359
OPH-EN-3	**Phantom Generation.** Production and consumption readings can be forged, so billing, feed-in payments and carbon claims rest on numbers nobody can trust.	Readings that are paid for are signed at the meter.	1. Sign readings in the meter or inverter. 2. Cross-check generation against irradiance and neighbouring systems. 3. Keep an audit trail of corrections.	T, R	none	none

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-EN-2	**Charger Knows Who's Home.** Charging sessions, contract certificates and vehicle identifiers collected by the charger show when each car comes and goes.	Collect vehicle data only for billing and safety, and keep it short.	1. Do not store vehicle identifiers beyond the session unless needed for billing. 2. Keep session history on the device by default. 3. Disclose who receives charging data.	I	none	CWE-359

NW · Home Network

The router, the Wi-Fi, the guest network and the house's path to the internet. Most smart home products assume the home network is friendly; it rarely is.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-NW-A	**Port Forwarded to the House.** Devices open inbound ports through UPnP, or setup guides tell owners to forward them, so cameras, recorders and hubs face the internet's scanners directly. *Seen: Mirai botnet (2016), built from internet-exposed cameras and DVRs*	No inbound exposure by default; remote access goes through an outbound, authenticated connection.	1. Never request UPnP port mappings from the device. 2. Provide remote access through an authenticated relay or tunnel that the device opens outward. 3. Test the home's exposure from outside at setup and warn when a device is reachable.	E, I	CAPEC-310	CWE-1188
OPH-NW-K	**Flat Network.** Bulbs, cameras, appliances, the hub and the household's laptops share one network, so the weakest device reaches the hub's local interface and every computer. *Seen: Casino fish-tank thermometer breach (Darktrace, 2017)*	Separate devices by trust, and allow only the flows each one needs.	1. Put devices on their own network or VLAN, with client isolation. 2. Allow only the device-to-hub and device-to-cloud flows each device needs. 3. Document the flows each product needs so the network can enforce them.	E, T	none	CWE-653

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-NW-Q	**Router Taken Over.** The home router runs with default or weak admin credentials or unpatched firmware, and whoever owns it controls DNS, routing and every device's path to the internet. *Seen: VPNFilter (Cisco Talos, 2018)*	The router is the house's perimeter and is secured and updated like one.	1. Ship unique admin credentials and disable remote administration by default. 2. Update router firmware automatically, with signed images. 3. Alert on DNS or admin setting changes.	E, T	CAPEC-70	CWE-1392
OPH-NW-J	**Trusts Whoever Answers.** Devices trust whatever DNS returns and accept any TLS certificate, or skip the hostname check, so whoever controls the network path receives commands and serves updates.	Authenticate the far end, whatever the network says.	1. Validate certificates and hostnames on every connection, with pinned roots for vendor services. 2. Use encrypted DNS where the platform supports it. 3. Test every release against an interception proxy.	S, T, I	CAPEC-94 CAPEC-142	CWE-295 CWE-297
OPH-NW-10 †	**Cut the Cable, Silence the House.** Alarms and cameras report only over the home broadband, so cutting the cable or the power to the router stops every alert before a break-in.	Safety and security reporting has a second, independent path.	1. Give alarms a cellular or other backup path. 2. Treat loss of connectivity while armed as an alarm at the receiving end. 3. Keep the router and the backup path on battery power.	D	CAPEC-583	none

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-NW-9	**Evil Twin at Setup.** During setup the app or device joins an access point that copies the home's network name, or sends the Wi-Fi password in the clear, so an attacker nearby captures it.	Provisioning authenticates both ends and never exposes the Wi-Fi password.	1. Provision over an authenticated channel (BLE with a PAKE, Wi-Fi Easy Connect). 2. Confirm the network the device joined matches the one chosen. 3. Never send credentials in the clear during setup.	S, I	CAPEC-615	CWE-319
OPH-NW-8	**IPv6 Walks Past the NAT.** Devices take public IPv6 addresses and the design assumes NAT keeps them unreachable, but the router's IPv6 firewall lets inbound traffic through.	Do not rely on NAT; filter inbound traffic on every address family.	1. Bind local services to link-local or private addresses only. 2. Test reachability over IPv6 as well as IPv4. 3. Ship routers with inbound IPv6 blocked by default.	E	none	none
OPH-NW-7	**Guest Network Bridged.** The guest network can reach smart devices through discovery reflection or casting features, so a visitor's infected phone reaches the hub.	Guests reach the internet, not the house.	1. Isolate the guest network from device networks. 2. Keep discovery reflection off for guest networks. 3. Offer guest control through invitations, not network membership.	E	none	CWE-653

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-NW-6	**Wi-Fi Knocked Off.** Deauthentication frames or a Wi-Fi jammer knock cameras and doorbells offline before a break-in, and the system does not notice. *Seen: Wi-Fi jammers used in burglaries (LAPD and other US police warnings, 2024)*	Treat loss of a security device's link as an event, and harden the link.	1. Use WPA3 with protected management frames. 2. Alert when a camera or doorbell drops off while the house is armed. 3. Record locally during a link loss and upload afterwards.	D	CAPEC-604	none
OPH-NW-5	**Discovery Lists the House.** The hub and devices announce themselves by mDNS and SSDP with names like 'Front Door Lock' and 'Nursery Camera', and their firmware versions, to anything on the network.	Announce only what a client needs to connect.	1. Use generic service names and leave out firmware versions. 2. Answer discovery only on the device network. 3. Let the owner turn off announcements once setup is done.	I	CAPEC-292	CWE-497
OPH-NW-4	**Sharing the House's Network.** Devices join a vendor's shared neighbourhood network by default, carrying neighbours' traffic over the home's connection. *Seen: Amazon Sidewalk enabled by default (June 2021)*	Sharing is opt-in.	1. Ship shared-network features off. 2. Explain what is shared and with whom before asking. 3. Let the owner see the bandwidth used.	I, E	none	CWE-1188

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-NW-3	**The House Attacks Others.** Compromised devices flood other people's services or scan the internet from the home connection, and nothing in the design notices. *Seen: Mirai DDoS attacks (2016)*	Bound what a device can send, and watch for change.	1. Rate-limit outbound connections per device. 2. Alert on traffic far outside a device's normal profile. 3. Publish the endpoints each device talks to, so the network can block the rest.	D	CAPEC-125	CWE-770
OPH-NW-2	**Phones Home to Everyone.** Devices talk to analytics, advertising and unknown third parties with no stated list, so the owner cannot tell normal from exfiltration.	Every destination is declared.	1. Publish the destinations each device contacts, and why. 2. Remove third-party trackers from device firmware. 3. Support a manufacturer usage description so routers can enforce it.	I	none	none

CL · Vendor Cloud

The vendor's service that binds devices to accounts, relays commands, stores events and links to other ecosystems. One cloud serves a million houses, so its mistakes are made a million times.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CL-A †	**Cloud Commands Every Home.** Devices obey whatever the vendor's cloud sends, so a compromise of the command plane, its admin console or its signing keys is a compromise of every home at once.	Devices verify that commands come from the owner, not just from the cloud.	1. Sign security-critical commands on the owner's device and verify them on the target. 2. Protect cloud admin access with phishing-resistant MFA and just-in-time grants. 3. Limit the blast radius by region and tenant, and rate-limit bulk commands.	E, T	none	CWE-1357
OPH-CL-K	**Device Claimed by Someone Else.** The cloud binds a device to whichever account first presents its serial number or MAC address, so an attacker pre-claims or re-claims devices from the label or the box.	Claiming a device needs proof that you hold it.	1. Require proof of possession at claim (a secret shown only on the device, or a local challenge). 2. Use claim tokens that cannot be guessed from the serial number. 3. Notify the current owner of any claim attempt.	E, S	none	CWE-283 CWE-340

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CL-Q	**Other Homes by ID.** API endpoints accept a device or home ID without checking that the caller owns it, so enumerating IDs reads or controls other people's houses.	Authorise every object on every request.	1. Check ownership of every device and home ID in every handler. 2. Use non-sequential identifiers and rate-limit enumeration. 3. Run automated cross-tenant tests in every release.	E, I	none	CWE-639
OPH-CL-J	**One Device Speaks for Another.** Devices authenticate to the cloud with a shared or derivable credential (a fleet-wide certificate, a key from the MAC address), so cloning one device impersonates others.	Each device has its own key, provisioned in manufacture.	1. Provision a unique key pair per device in a secure element. 2. Bind cloud identity to that key, never to a derivable value. 3. Revoke individual device credentials when cloning is detected.	S	CAPEC-151	CWE-798 CWE-1394
OPH-CL-10	**Credential Stuffing the House.** Home accounts protected by a password alone fall to credential stuffing, and the attacker gets every device in the house.	A home account needs stronger authentication than a password.	1. Offer passkeys and require MFA for accounts that hold locks, alarms or cameras. 2. Check passwords against breach corpora. 3. Rate-limit and fingerprint login attempts.	S	CAPEC-600	CWE-307 CWE-308

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CL-9	**Linked Service Overreach.** Linking to a voice assistant, automation service or insurer grants a broad, non-expiring token for every device, so a breach at the third party is control of the house.	Linked services get the least access for the shortest time.	1. Scope linking tokens by device and action, and exclude locks and alarms unless chosen. 2. Expire linking tokens and require renewal. 3. Show the owner every linked service and what it can do.	E, I	none	CWE-1220
OPH-CL-8	**Support Desk Hands Over the House.** Customer support can move devices between accounts or reset MFA on a phone call with weak identity checks.	Account recovery is as strong as account login.	1. Require proof of possession of a device or a recovery code for transfers. 2. Delay and notify on recovery, so the real owner can stop it. 3. Log support actions where the owner can see them.	S	CAPEC-407	CWE-640
OPH-CL-7 †	**App Says Locked.** The cloud's copy of device state goes stale, so the app shows 'locked' or 'armed' while the device is not, and the owner relies on it.	Show state with its age, and confirm critical state from the device.	1. Show when each state was last confirmed by the device. 2. Confirm lock and alarm state from the device before displaying it as current. 3. Alert when the device and the cloud disagree.	T	none	CWE-451

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CL-6	**One Region, Every Home.** A single cloud region's outage stops cameras, doorbells, locks and vacuums in every home that depends on it, because nothing works locally. *Seen: AWS us-east-1 outage (Dec 2021)*	Core functions work without the cloud.	1. Keep locks, alarms, lighting and heating working on the local network. 2. Run the cloud across regions with tested failover. 3. Tell owners which functions need the cloud.	D	none	none
OPH-CL-5	**Data Kept and Reused.** The vendor keeps telemetry, voice, video and maps beyond their purpose and reuses them for training or advertising. *Seen: FTC action against Amazon over Alexa retention of children's voice recordings (2023)*	Keep data for its stated purpose and period, then delete it.	1. Set retention per data type and enforce it in storage and backups. 2. Ask for consent before reuse for training or advertising. 3. Give the owner an export and a verified deletion.	I	none	CWE-359
OPH-CL-4	**Fake Notification.** Push notifications and webhooks are not authenticated, so an attacker sends a fake 'door locked' or a fake alarm prompt that tricks the owner into acting.	Notifications carry no authority on their own.	1. Sign webhook payloads and verify them. 2. Make any action from a notification open the app and re-check state. 3. Keep sensitive details off lock-screen notifications.	S	none	CWE-290

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-CL-3	**Device Floods the Tenant.** A device can post any volume of telemetry, so a malicious one exhausts a household's quota, runs up costs or poisons analytics.	Bound what each device can send.	1. Rate-limit and size-limit ingestion per device. 2. Validate telemetry against the device type's schema. 3. Quarantine devices that exceed their limits.	D	CAPEC-125	CWE-770
OPH-CL-2	**Vendor Access Unseen.** The owner cannot see when vendor staff, support or authorities accessed their data or devices.	Every access by someone other than the household is visible to the household.	1. Log vendor and legal access to each home. 2. Show that log to the owner, unless a court forbids it. 3. Publish a transparency report.	R	none	CWE-778

RC · Remote Control

The phone in a pocket, the computer at work, the tablet on the wall and the watch on a wrist: the clients that control the house from anywhere. Each one is a key that can be lost, copied or borrowed.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-RC-A †	**Lost Phone Opens the Door.** A stolen or borrowed phone with a long-lived session, a widget or a watch complication unlocks the door with no check that the holder is the owner.	Security actions need the person, not just the phone.	1. Require biometric or PIN confirmation in the app for unlock and disarm. 2. Make widgets and watch actions for locks require the phone to be unlocked. 3. Let the owner revoke a device's sessions from any other device.	S, E	CAPEC-507	CWE-308
OPH-RC-K	**Token Lifted from the App.** The app keeps refresh tokens and API keys in plain storage, logs or backups, so malware or a backup extraction gives lasting control of the house.	Store secrets in the platform's hardware-backed keystore.	1. Keep tokens in the iOS Keychain or Android Keystore, bound to the device. 2. Exclude tokens from backups and logs. 3. Rotate refresh tokens on use and detect reuse.	I, E	CAPEC-37	CWE-922
OPH-RC-Q	**Fake App, Real Password.** A cloned app or a look-alike login page captures the owner's credentials for the house.	Make credentials useless to anyone who copies them.	1. Offer passkeys, which cannot be phished. 2. Monitor app stores and domains for impersonation. 3. Alert the owner on logins from new devices.	S	CAPEC-98	none

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-RC-J	**Dashboard Session Hijacked.** The web dashboard keeps tokens in browser storage, renders device data unencoded or accepts cross-site requests, so a malicious page or script takes over the session.	Treat the browser dashboard as a high-value web application.	1. Use HttpOnly, SameSite session cookies rather than tokens in browser storage. 2. Protect state-changing requests against forgery. 3. Encode all device-supplied data and enforce a Content Security Policy.	E	CAPEC-593	CWE-1004 CWE-79
OPH-RC-10 †	**Link Opens the Lock.** A custom URL scheme, app link or intent triggers unlock, disarm or share without confirmation, so a link in a text message acts on the house.	Links can open screens, never perform security actions.	1. Route every deep link to a screen that asks for confirmation. 2. Validate the source and parameters of every link handler. 3. Exclude security actions from deep-link handlers entirely.	E	none	CWE-939
OPH-RC-9	**Other Apps Drive This One.** Exported activities, services or broadcast receivers in the Android app let other apps on the phone send commands to the house.	Export only what other apps need, and check who is calling.	1. Mark components as not exported unless required. 2. Protect exported components with signature permissions. 3. Use explicit intents for anything security-related.	E	CAPEC-502	CWE-926
OPH-RC-8	**First Hub That Answers.** The app finds the hub on the local network by discovery and trusts the first device that answers, so a rogue hub collects credentials.	The app authenticates the hub before sending it anything.	1. Pin the hub's identity at pairing and verify it on every connection. 2. Warn when a new device claims to be the hub. 3. Send no credentials to an unverified hub.	S	CAPEC-616	CWE-940

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-RC-7	**Wall Panel Runs as Owner.** A wall tablet or shared family tablet stays signed in with the owner's full rights, so guests, children and cleaners can do anything the owner can.	Shared screens get a shared, limited role.	1. Provide a kiosk role with chosen controls only. 2. Require a PIN for security actions on shared screens. 3. Time out admin sessions on shared devices.	E	none	CWE-1220
OPH-RC-6	**Remote Desktop to the Hub.** Owners and installers expose the hub through remote desktop, VNC, SSH or a third-party tunnel with weak credentials, to reach it from work.	Provide a secure remote path so nobody builds their own.	1. Offer an authenticated remote access path in the product. 2. Warn when the hub's admin interface is reachable from the internet. 3. Require MFA on any remote admin path.	E	CAPEC-555	CWE-1188
OPH-RC-5	**Notification Tells the Street.** Lock-screen notifications say 'Front door unlocked', 'Alarm disarmed' or show a camera snapshot to anyone holding or near the phone.	Lock screens show that something happened, not what.	1. Default to generic notification text for security events. 2. Keep camera snapshots off lock screens unless chosen. 3. Encrypt notification payloads end to end.	I	none	CWE-359
OPH-RC-4	**Location All the Time.** The app asks for continuous location for geofencing and sends each member's movements to the cloud and to the rest of the household.	Use the least location, for the shortest time, shown to the fewest people.	1. Use on-device geofence events rather than location history. 2. Keep each member's location visible only to themselves unless they share it. 3. Let each member turn presence off without leaving the household.	I	none	CWE-359

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-RC-3	**Old App Still Accepted.** The cloud accepts every old app version, so flaws fixed in the app stay exploitable by anyone who keeps the old one.	Retire vulnerable client versions.	1. Enforce a minimum app version for security fixes. 2. Version the API and turn off deprecated endpoints. 3. Prompt owners to update before blocking.	E	none	none
OPH-RC-2	**Screenshot Shows the Code.** Camera views, door codes and recovery codes appear in app-switcher snapshots, screen recordings and shared screens.	Hide sensitive screens from capture.	1. Blank sensitive screens in the app switcher. 2. Mark code and camera screens as secure against capture where the platform allows. 3. Show codes only on request, for a short time.	I	CAPEC-648	CWE-359

VA · Voice and Automations

Voice assistants, routines and scenes, rules and scripts, third-party skills and AI agents: the layer that turns words and events into actions on the house without a person pressing a button.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-VA-A †	**Voice Opens the Door.** Voice commands are accepted from anyone in earshot, from the television or from inaudible injection (ultrasound, laser), and some of them unlock doors, disarm alarms or open the garage. *Seen: DolphinAttack (2017); Light Commands (2019)*	Voice is not identity; security actions by voice need a second factor.	1. Keep voice unlock, disarm and open off by default. 2. Require a spoken PIN and voice match, and confirm on a phone. 3. Filter inaudible frequencies and check that commands come from a live speaker.	S, E	none	CWE-290
OPH-VA-K †	**Rule Runs as Owner.** Automations run with the owner's full rights, whoever wrote them, so a household member or integration creates a rule that unlocks the door at three in the morning.	A rule runs with its author's rights, and security actions need the owner's approval.	1. Run each rule under its author's permissions. 2. Require owner approval for rules that unlock, disarm or open. 3. Notify the household when a security rule is created or changed.	E	none	CWE-250

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-VA-Q †	**Agent Talked into It.** An AI home agent acts on instructions hidden in device names, calendar entries, messages or text a camera sees, or reads 'open everything' too literally.	An agent's reach is limited and its security actions are confirmed.	1. Give the agent no lock, alarm or heat-appliance tools without per-action confirmation. 2. Treat device names and other content as data, never as instructions. 3. Log every agent action with the prompt that led to it.	E, T	none	CWE-1427
OPH-VA-J	**Sound-Alike Skill.** A third-party skill or action with a name that sounds like a trusted one captures commands, keeps listening or asks for passwords. *Seen: Skill Squatting (Kumar et al., USENIX Security 2018); Smart Spies (SRLabs, 2019)*	Invocation names are reviewed for confusion, and skills cannot impersonate the assistant.	1. Review new skills for names that sound like existing ones. 2. Stop skills from asking for passwords or keeping the microphone open after they finish. 3. Show which skill handled each request.	S, I	CAPEC-631	none
OPH-VA-10 †	**Spoofed Sensor Triggers a Rule.** A rule uses a spoofable signal (motion, presence, a doorbell press, recognised face) to disarm or unlock, so whoever fakes the signal triggers the security action.	Security actions never rest on a signal an outsider can fake.	1. Exclude untrusted sensors from triggers for security actions. 2. Require a second, independent condition for any disarm or unlock rule. 3. Flag rules that link outside sensors to security actions.	E	none	CWE-807

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-VA-9	**Imported Rule Does More.** A community blueprint, script or shared routine does more than it says, sending data out or unlocking a door under a harmless name.	Show what an imported rule will do before it runs.	1. Show every action and destination of an imported rule before import. 2. Run imported rules with no security actions until the owner approves them. 3. Sign rules from known publishers.	T, E	none	CWE-829
OPH-VA-8	**Rules Fight Each Other.** Two automations work against each other (heating on, window open), or loop until a device is damaged, and one triggered sensor sets off a chain.	Detect conflicts and loops before and while rules run.	1. Check new rules for conflicts with existing ones on the same devices. 2. Stop loops with a limit on actions per device per minute. 3. Show the chain of rules behind each action.	T, D	none	CWE-835
OPH-VA-7	**Presence Faked.** Away mode turns off when the system sees the owner's phone by Wi-Fi or Bluetooth address, so a spoofed address 'comes home' and disarms the house.	Presence from a radio address is a hint, not a person.	1. Do not disarm on network presence alone. 2. Use authenticated presence from the owner's phone. 3. Notify when presence changes the security state.	S	CAPEC-151	CWE-290
OPH-VA-6	**Overheard and Kept.** False wake words record private conversations, which are kept, reviewed by people or sent to contacts. *Seen: Alexa recording sent to a contact (Portland, 2018)*	Recordings are rare, short-lived and visible to the household.	1. Tune wake-word detection to favour missing a command over recording. 2. Delete recordings by default, and ask before human review. 3. Show every recording in the household's history.	I	none	CWE-359

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-VA-5	**Ordered by Voice.** Voice purchases and account changes need nothing but a voice, so children, visitors and the television make them. *Seen: Alexa dollhouse order by a child (Dallas, Jan 2017)*	Voice transactions need a PIN and a confirmation.	1. Ship voice purchasing off or behind a PIN. 2. Confirm purchases and account changes on a phone. 3. Make purchases easy to cancel.	E	none	CWE-308
OPH-VA-4	**Assistant Answers Anyone.** The assistant tells anyone who asks whether the alarm is set, what is in the calendar and who has messaged, and reads notifications aloud.	Personal and security answers need voice match.	1. Require voice match for personal and security questions. 2. Keep security state out of spoken answers by default. 3. Let each member set what the assistant reads aloud.	I	none	CWE-359
OPH-VA-3	**Rule Changed Quietly.** Rules can be edited without anyone being told, so a malicious change stays unnoticed until it runs.	Every rule change is attributed and announced.	1. Record who changed a rule, when and what changed. 2. Notify the household of changes to rules that touch security devices. 3. Keep rule history and allow rollback.	R	none	CWE-778
OPH-VA-2	**Wrong Voice, Wrong Profile.** Voice match mistakes one household member for another, so personal results, purchases or permissions go to the wrong person.	Fall back to the least-privileged profile when unsure.	1. Treat uncertain voice matches as a guest. 2. Let members set which actions need a confident match. 3. Let members review and correct matches.	S	none	none

HH · Household

The people in the house: partners, children, lodgers, guests, cleaners, landlords and installers. A smart home has many users with different interests, and most products model one owner.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-HH-A †	**House Turned Against Its People.** A partner or ex-partner with admin rights uses the cameras, locks, heating and lights to watch, control or frighten the others in the house. *Seen: Smart home devices used in domestic abuse (New York Times, June 2018)*	Everyone who lives in the house can see who controls it, and control cannot be kept in secret.	1. Show every adult resident the full list of users, sessions and linked services. 2. Notify residents when cameras or microphones are viewed and when rules change. 3. Provide a documented way to remove an admin without the admin's cooperation, on proof of residence.	E, I	CAPEC-122	none
OPH-HH-K †	**Ex Keeps the Keys.** Someone who has moved out keeps the account, codes and app access because the devices are bound to their account.	Leaving the house ends access, and the people who stay keep the house.	1. Bind devices to the home, with members, rather than to one person's account. 2. Make removing a member revoke every code, session and token they hold. 3. Let remaining residents take over ownership with proof of residence.	E	none	CWE-282

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-HH-Q	**One Account for Everyone.** The product has one account that the household shares, so there is no attribution, and revoking one person means changing everyone's password.	Every person has their own identity in the home.	1. Support individual member accounts with roles. 2. Make inviting a member easier than sharing the password. 3. Show each action against the person who took it.	S, R	none	CWE-1220
OPH-HH-J	**Landlord Sees Inside.** A landlord or agent installs devices and keeps admin or camera access to the tenant's home, and the tenant is not an admin.	The occupier controls what sees and hears inside their home.	1. Split building control (boiler service, leak alerts) from occupier control (cameras, locks, schedules). 2. Hand occupier control to the tenant at the start of a tenancy. 3. Show the tenant every access the landlord has.	I, E	none	none
OPH-HH-10	**Installer Keeps a Key.** The installer or integrator keeps admin or remote access after handover, and the owner does not know it exists. *Seen: ADT technician accessed customer cameras (disclosed 2020, guilty plea 2021)*	Handover transfers all control and ends the installer's access.	1. Expire installer access at handover unless the owner renews it. 2. List installer access in the app. 3. Require the owner's consent per visit for later access.	E, I	CAPEC-122	none
OPH-HH-9	**Guest Gets Owner Rights.** Inviting a guest grants a role that can add users, view camera history or change rules, and the invitation never expires.	Guests get a narrow role with an end date.	1. Offer guest roles limited to chosen devices and times. 2. Expire guest access by default. 3. Keep camera history and user management out of guest roles.	E	none	CWE-1220

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-HH-8 †	**Child Holds Adult Rights.** Children use the panel, voice or a shared tablet to disarm the alarm, unlock the door or turn on appliances, because the product has no child role.	Roles fit the person: children get the controls a child should have.	1. Provide child roles without security or heat-appliance actions. 2. Apply roles on every interface (voice, panel, app). 3. Let parents review what a child's role can do.	E	none	CWE-1220
OPH-HH-7 †	**Emergency Access Denied.** In an emergency (a fire, a fall, the owner taken ill) responders and family cannot get in or silence the alarm, because there is no break-glass access.	Plan emergency access before the emergency.	1. Provide a break-glass credential held by a named contact or service. 2. Make emergency access logged and notified. 3. Keep a mechanical way in for emergency services.	D	none	none
OPH-HH-6	**Building Controls the Door.** In a shared building, the managing agent's system controls the entrance, flat doors or shared hub, and residents cannot see or limit what it does.	Residents see and control access to their own home.	1. Show residents every credential that opens their door. 2. Separate building-wide access from access to each home. 3. Give residents an audit log of their door.	E, I	none	none
OPH-HH-5	**Family Members Tracked.** Presence and geofencing features show each member's arrivals and departures to everyone else in the household, including people they would not choose to tell.	Each person controls who sees their location.	1. Make presence sharing per person and opt-in. 2. Show members who can see their presence. 3. Let a member stop sharing without others being alerted.	I	none	CWE-359

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-HH-4 †	**Alert Goes to the Absent Owner.** Smoke, CO, leak and alarm alerts go only to the account owner, who may be abroad, and not to the people in the house.	Safety alerts reach the people who can act.	1. Send safety alerts to everyone present and to named contacts. 2. Escalate when the first recipient does not acknowledge. 3. Sound alerts locally whatever the app does.	D	none	none
OPH-HH-3	**Visitors Recorded Without Notice.** Indoor cameras and microphones record nannies, cleaners, guests and tradespeople who were never told.	People in the home know when they are recorded.	1. Provide visible indicators and a guest mode that pauses indoor recording. 2. Prompt owners about notice duties when indoor recording is on. 3. Make recording schedules easy to set around visits.	I	none	none
OPH-HH-2	**Nobody Reviews the Members.** The product never prompts anyone to review users, codes and rights when the household changes, so access only grows.	Access is reviewed when life changes.	1. Prompt a review of members and credentials periodically. 2. Prompt a review when a member has been inactive for a long time. 3. Show unused credentials and offer to remove them.	E	none	none

LC · Lifecycle

Manufacture, onboarding, updates, support, resale and disposal. A house lasts for decades, its devices are supported for a few years, and the house changes hands with the devices still on the walls.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-LC-A †	**Unsigned Update Accepted.** Devices accept firmware that is unsigned, or signed with a key extracted from a device, so anyone on the network or with the device in hand installs their own.	Every update is signed with a key that is on no device, and verified before install.	1. Sign firmware with an asymmetric key held in an HSM. 2. Verify the signature in a secure boot chain rooted in hardware. 3. Reject updates that fail verification and report them.	T, E	CAPEC-186	CWE-494 CWE-347
OPH-LC-K †	**Vendor Turns Off the Servers.** The vendor shuts its cloud, goes bust or sells to an unknown buyer, and the devices stop working, lose their security features or come under someone else's control. *Seen: Revolv shutdown (2016); Insteon shutdown (April 2022)*	Devices keep their core functions, and their owners keep control, without the vendor.	1. Keep core functions local, and publish a local API before end of life. 2. Commit to a notice period and an end-of-life plan. 3. Let owners move devices to another controller (Matter, an open API).	D	none	none
OPH-LC-Q †	**Previous Owner Still Connected.** After a house or device is sold, the previous owner's account still controls the devices and sees the cameras, and the new owner cannot reclaim them without the old one.	Ownership moves with the house, and the old owner's access ends.	1. Provide a reclaim flow based on physical possession and a local reset. 2. Notify and remove the previous owner when a device is reclaimed. 3. Warn sellers to transfer devices as part of the sale.	E, I	none	CWE-282 CWE-283

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-LC-J	**Implant in the Box.** Counterfeit, grey-market or compromised devices arrive with malware preinstalled, and the product cannot tell a genuine unit from a tampered one. *Seen: BadBox Android TV boxes (Human Security, 2023 and 2025)*	Devices prove they are genuine before they are trusted.	1. Use hardware attestation at onboarding. 2. Refuse to onboard units that fail attestation. 3. Publish how to check a device is genuine.	T, E	CAPEC-439	CWE-506
OPH-LC-10	**Rolled Back to a Hole.** An attacker installs an older, validly signed firmware that still has a known flaw.	Firmware never goes backwards past a security fix.	1. Keep an anti-rollback counter in hardware. 2. Raise the security version with every security fix. 3. Refuse older images.	T	none	CWE-1328
OPH-LC-9	**Reset Doesn't Erase.** A factory reset leaves the Wi-Fi password, tokens and recordings in flash, so a resold or discarded device gives up the old home's secrets. *Seen: Wi-Fi password stored in plain text in LIFX bulb flash (LimitedResults, 2019)*	Reset erases every secret and personal record.	1. Encrypt user data under a key that reset destroys. 2. Revoke the device's cloud credentials on reset. 3. Test reset by reading the flash afterwards.	I	CAPEC-675	CWE-1266

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-LC-8	**Support Ends Silently.** Devices stop receiving security updates with no stated end date and no notice, and keep running on the network.	State the support period, and tell owners before it ends.	1. State the minimum security support period on the box and in the app. 2. Notify owners before support ends. 3. Offer to isolate or retire devices after end of support.	E	none	CWE-1104
OPH-LC-7	**Old Library Inside.** Devices ship with old Linux kernels, BusyBox, OpenSSL and vendor SDKs with known flaws, and the vendor cannot tell which products are affected.	Know what is in the device and keep it current.	1. Produce an SBOM for every firmware release. 2. Track advisories against the SBOM and ship fixes within a stated time. 3. Remove components the product does not use.	E	none	CWE-1395
OPH-LC-6 †	**Update Fails Halfway.** A power cut or failed download mid-update bricks the device, or leaves the lock or alarm in an unknown state.	Updates are atomic and leave a working device whatever happens.	1. Use A/B partitions with automatic rollback. 2. Update security devices only when disarmed and attended, or with a safe fallback state. 3. Report update failures to the owner.	D	none	CWE-1419

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-LC-5	**Baked-In Certificate Expires.** A root certificate or device certificate baked into firmware expires, and devices across the fleet stop connecting on the same day. *Seen: DST Root CA X3 expiry (Sept 2021)*	Plan credential expiry and renewal for the device's whole life.	1. Keep root stores updatable. 2. Track the expiry of every certificate in the fleet. 3. Renew before expiry with a tested path.	D	none	CWE-1329
OPH-LC-4	**Account Deleted, Data Kept.** Deleting the account or removing a device leaves recordings, maps and history in the cloud and its backups.	Deletion reaches every copy.	1. Delete user data from primary storage, analytics and backups on schedule. 2. Confirm deletion to the owner. 3. Test deletion end to end.	I	none	CWE-212
OPH-LC-3	**Nowhere to Report a Flaw.** Researchers who find a flaw have no published way to report it, so it is sold or disclosed without a fix.	Publish a vulnerability disclosure policy and act on reports.	1. Publish a contact and policy for vulnerability reports. 2. Acknowledge reports and give timelines. 3. Credit reporters and publish advisories.	E	none	none
OPH-LC-2	**Repair Shop Sees the Home.** Devices sent for repair or replacement carry recordings, maps and credentials that the repairer can read.	Devices leave the home without the home's data.	1. Offer a repair mode that locks user data. 2. Wipe or encrypt user data before a unit is returned. 3. Tell owners what a repairer can access.	I	CAPEC-675	CWE-1266

TR · Structural Hazards

Structural hazards are properties of the connected home as a whole, not single faults. In the game they play as Trumps, in both decks; deal them against the whole design before the suits.

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-TR-1 †	**The House Is the Blast Radius.** A software fault in a smart home becomes a physical event: fire, flood, freeze, a door open to the street. Threat models that score impact by data loss miss it.	Score impact by what happens in the house, not just to the data.	1. Add physical consequences (heat, water, access, life safety) to the impact scale. 2. Trace every remote command to the physical effect it can cause. 3. Keep independent, non-software safety for every hazardous effect.	T, D	none	none
OPH-TR-2	**Every Device Is a Door.** The house is as secure as its least secure connected device: the cheapest plug shares a network and a hub with the alarm and the lock.	Assume the weakest device will be compromised, and limit what it reaches.	1. Inventory every connected device and its trust level. 2. Separate devices by trust on the network and in the hub. 3. Let no device send commands to another without the hub's authorisation.	E	none	none
OPH-TR-3	**The Cloud Holds the Keys.** Local functions and safety features depend on a remote service the household does not control, and that service can fail, change or be compromised.	Decide which functions must work without the cloud, and make them.	1. List the functions that need the cloud. 2. Make safety, access and heating work locally. 3. Test the house with the internet off.	D, E	none	none

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-TR-4	**Outlives Its Support.** A house lasts decades, its devices are supported for a few years, and vendors leave the market, so the house fills with devices nobody patches.	Design for the device's life in the house, not its life in the catalogue.	1. State support periods, and plan for what happens after them. 2. Prefer open, local standards that outlast a vendor. 3. Give owners a way to retire devices safely.	E, D	none	none
OPH-TR-5 †	**Many Hands on the Keys.** A household is not one user: partners, children, guests, lodgers, landlords and installers share it, with interests that differ and change.	Model every person who lives with the system, not just the buyer.	1. List every role in the household, including those who never install the app. 2. Give each role its own identity and limits. 3. Model the household turning against one of its members.	E, R	none	none
OPH-TR-6	**Houses Change Hands.** Devices stay with the bricks and accounts stay with people, so every sale, letting or separation leaves access in the wrong hands.	Make transfer of the house a designed event.	1. Bind devices to the home, with transferable ownership. 2. Provide transfer and reclaim flows based on possession. 3. Remind owners to transfer before moving.	E, I	none	none
OPH-TR-7 †	**Many Homes, One Grid.** Connected energy devices act together on the grid, so a compromise or a bad signal moves the load of thousands of homes at once.	Treat fleets of energy devices as grid infrastructure.	1. Model the fleet's combined effect, not just one home's. 2. Build ramp limits and random delays into each device. 3. Protect fleet control paths as critical infrastructure.	D	none	none

ID	THREAT	MITIGATION PRINCIPLE	DESIGN MEASURES	STRIDE	CAPEC	CWE
OPH-TR-8	**Ecosystems Inherit the Weakest Link.** Bridges, multi-admin controllers and cloud-to-cloud links pass trust between ecosystems, and the strongest system takes on the weakest one's flaws.	Trace trust across every ecosystem link.	1. Map every bridge, linked cloud and shared controller. 2. Carry each device's security level across links. 3. Limit what linked ecosystems can command.	S, E	none	none
OPH-TR-9	**Radio Ignores Walls.** Radio, light and sound reach beyond the property line, so the attacker can be on the street, next door or across the road, with no need to enter.	Treat everyone within range as a possible attacker.	1. Measure the real range of every radio and voice interface. 2. Assume the street can hear, see and transmit. 3. Require a local act for anything range alone should not grant.	S, I	none	none
OPH-TR-10	**The House Keeps a Diary.** Sensors, meters, cameras and logs record when people wake, leave, return and who they are with, and together they say more than any one of them.	Minimise and separate what the house records about its people.	1. Inventory every source of personal data in the house. 2. Keep data local unless a feature needs it elsewhere. 3. Model what combined data reveals, not just each stream.	I	none	none