By Duncan Hodges

Mapping Smart Home Vulnerabilities to Cyber-Enabled Crime

'ALEXA, SECURE MY HOME!' ARE SMART DEVICES IN OUR HOMES INCREASING THE RISK OF TRADITIONAL CRIMES, SUCH AS RESIDENTIAL BURGLARY?

Burglary is a traditional crime occurring in an offline environment that *the majority of the UK public consider causes substantial harm*, with victims often left feeling vulnerable and fearful. Although residential burglary rates have been slowly declining over the last 20 years, there were still nearly *300,000 residential burglaries reported to the police between June 2018 and June 2019*.

As smart home technology becomes more prevalent, our homes are no longer entirely offline spaces, becoming instead complex 'cyber-physical' environments. Our research at Cranfield University has explored the potential for the smart home to 'cyber-enable' traditional crimes, using residential burglary as a case example.

The act of committing burglary involves a complex set of decisions. Generally, *burglars experience three phases of their crime*:

The first phase involves scanning the environment to identify suitable areas to operate in; there is evidence that this is a relatively unconscious act as offenders go about their daily lives.

The second phase is the identification of a target property within the chosen area. During this phase, several dynamic and complex cues interact to support the choice of the target within the area. These include external layout and access cues (for example, properties with easy access to the rear or those hidden from public view); relative affluence cues; cues associated with whether the property is currently occupied; and cues associated with potential security measures – although it is important to note that expert burglars are rarely deterred by such security features.

The final phase of burglary is entry to the property and the search for items of value to the burglar, typically following a systematic route.

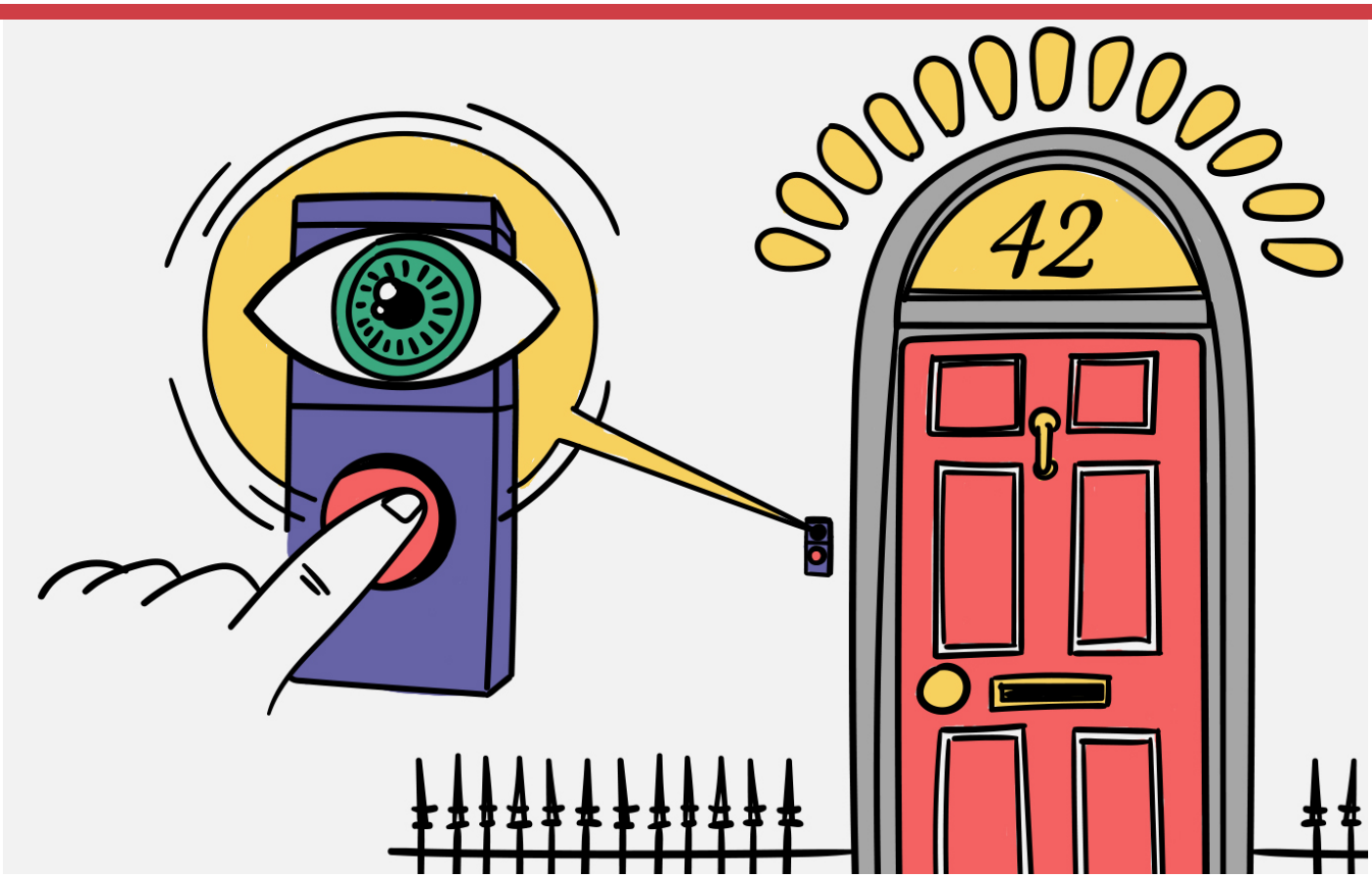
To explore the interactions between the smart home and these phases we created three smart home deployments, incorporating a range of devices to simulate increasing levels of 'smart' complexity:

1. The 'simple' deployment offered the ability to remotely control lights and other simple devices.
2. The 'complex' deployment included controlling a greater number of physical attributes of the space, such as the temperature, while also beginning to observe the environment.
3. The 'complete' deployment represented a smart home incorporating many of the devices that are readily available on the market, including smart locks. These deployments formed the basis for our assessment of the increased risk of burglary.

SMART DOORBELLS AND LOCKS

From our analysis there is, on the whole, unlikely to be any significant effect on residential burglary through deploying smart home technology. However, two devices do have some influence: smart doorbells and smart locks.

These are devices that are particularly noticeable due to their deployment on the exterior of properties and can thus increase the salience of affluence cues – experienced burglars use these cues to identify properties with potentially more high-value items, during the target selection phase.



Smart doorbells could become a strong cue to the relative affluence of properties. But with a relatively low number of smart locks currently deployed in the UK, it is unlikely that even experienced burglars will routinely come across these devices anytime soon.

One common theme in the literature surrounding burglary is that in general, burglars are looking to maximise their familiarity with the property, so the presence of unfamiliar locks, such as smart locks, may actually form a deterrent regarding entry through this particular access point.

There is also a significant body of literature that suggests that there are likely to be alternative vulnerable doors and windows, particularly at the rear of the property, which a burglar is likely to prioritise.

STAYING SMART

While at present we think there is relatively little increase in the risk of residential burglary from the use of smart devices, this may change in the future as burglars adapt to the emerging cyber-physical home.

Using the analysis developed in this research we can identify several potential indicators that burglars are beginning to adapt to these new technologies. The most salient is an increase in group-performed planned burglary since this can better exploit unintended information leakage in the cyber domain.

This form of burglary is typically rare in residential settings at present but is more common in commercial settings. Hence, an increase in the burglary of commercial premises exploiting smart-devices may be a good bellwether for a likely increase in smart devices being exploited in residential burglary.

Criminals rate of adaption to the cyber-physical home will be related not just to the rate of adoption of smart home technology by consumers, but crucially to the ability of households to deploy the technology securely.

READ MORE

This article is part of a series exploring the security of smart home technology. See all outputs from the project here: *www.crestresearch.ac.uk/projects/adoption-and-exploitation-of-smart-home-technology/*