Wireless home automation systems reveal more than you would think about user behaviour

July 24 2014

Home automation systems that control domestic lighting, heating, window blinds or door locks offer opportunities for third parties to intrude on the privacy of the inhabitants and gain considerable insight into their behavioural patterns. This is the conclusion reached by IT security expert Christoph Sorge and his research team at Saarland University. Even data transmitted from encrypted systems can provide information useful to potential burglars. Professor Sorge, who holds the juris Professorship in Legal Informatics at Saarland University, and his research group are currently studying ways to make home automation systems more secure. Frederik Möllers from Sorge's team will be presenting the results at the ACM Conference on Security and Privacy in Wireless and Mobile Networks in Oxford on 25 July.

Regulating heating systems to save energy, adjusting lighting levels based on the time of day, watering house plants automatically, and raising or lowering blinds at the required times – the benefits of today's smart home automation systems are numerous and they are becoming increasingly popular with homeowners. However, studies by the research group led by Professor Christoph Sorge have shown that these wireless systems can also pose a security risk. 'Many of the systems do not provide adequate security against unwanted third-party access and therefore threaten the privacy of the inhabitants,' says Sorge, an expert for IT security, data protection and encryption technology at Saarland University. Sorge and his team have examined how susceptible the

systems are to attack.

For the purposes of their study, the researchers took on the role of a malicious attacker. 'Using a simple mini-PC no bigger in size than a packet of cigarettes we eavesdropped on the wireless home automation systems (HASs) of two volunteers and were thus able to determine just how much information a conventional wireless HAS reveals about its user,' explains Sorge. No other information about the users was available to the research group. The result: 'Non-encrypted systems provide large quantities of data to anyone determined enough to access the data, and the attacker requires no prior knowledge about the system, nor about the user being spied on,' says Professor Sorge.

'The data acquired by the attacker can be analysed to extract system commands and status messages, items which reveal a lot about the inhabitants' behaviour and habits. We were able to determine absence times and to identify home ventilation and heating patterns,' explains the expert in legal informatics. The analysis enabled the research group to build up profiles of the inhabitants. Even systems that use encryption technology can supply information to third parties: 'The results indicate that even when encrypted communication is used, the number of messages exchanged is enough to provide information on absence times,' says Sorge. Potential attacks can be directed against the functionality of the system or the privacy of the inhabitants. 'An attacker with malicious intent could use this sort of information to plan a burglary,' says Sorge.

'A great deal still needs to be done to make wireless home automation systems secure. Improved data encryption and concealment technologies would be an important step towards protecting the privacy of HAS users,' explains Professor Sorge. He and his group are currently working on developing technology of this type in collaboration with the University of Paderborn as part of a research project funded by the Federal Ministry of Economics and Energy.

The research work into home automation systems began with a Master's degree thesis by Andreas Hellmann, who was supervised by Professor Sorge while still at the University of Paderborn. With his research group now based at Saarland University, Professor Sorge is currently continuing research in this area with his research assistant Frederik Möllers, who will be presenting the results of their recent study in Oxford on 25 July.

Provided by Saarland University