# Envisioning Smart Building Botnets

Steffen Wendzel[1], Viviane Zwanger[1,2], Michael Meier[1,2], Sebastian Szlósarczyk[1,2]

[1]Cyber Defense Research Group, Fraunhofer FKIE
[2]Institute of Computer Science 4, University of Bonn
{wendzel,zwanger,meier,szlos}@cs.uni-bonn.de

**Abstract:** A building automation system (BAS) is the IT equipment within a building that monitors and controls the building (e.g., measuring temperature in a room to configure the heating level within the same room). We discuss the potential and the use of botnets in the context of BAS. Our botnet concept and scenario is novel in the sense that it takes advantage of the phyiscal capabilities of a building and as it has to adapt to a specialized environment being highly deterministic, predictable, simplistic and conservative. These properties make anomalies easy to detect. *Smart building botnets* allow the monitoring and remote control of (critical) building automation infrastructure in public and private facilities, such as airports or hospitals. We discuss why building automation botnets could thus enable attackers to cause various critical damage on whole regions and economies. Hiding the command and control communication is a highly beneficial step to adapt botnets to the BAS environment. We show that this is not necessarily a big hurdle and can be solved using existing covert channel techniques.

## 1 Introduction

This paper combines three research areas, namely building automation research, botnet research, and network covert channels.

*Building automation systems* (BAS) are IT components integrated in and capable of controling and monitoring buildings. BAS aim at improving the energy efficiency of houses, at increasing the comfort and safety for people living or working in a building, and at decreasing a building's operation costs. Therefore, it is necessary to enable a BAS to operate critical equipment like smoke detectors or physical access control components.

*Botnets* have become an essential and indispensable part of todays' criminal infrastructure. Botnets allow for controlling and drawing profit not only from individual computer systems but also through mass infection. The modern criminal botnets have become extremely complex and grown into a robust ecosystem of organized crime with a sophisticated service landscape [GBC+12, CGKP11]. The spectrum of criminal activity ranges from hosting stolen credit card information, selling private data in large chunks as well as utilizing cheap computing power (also used for legitimate purposes), to even directly blackmail victims (i.e. encrypt hundreds of computer systems and extort a ransom from victims).

To criminals, BAS offer a completely new market, with new opportunities of drawing profit on a big scale. Thus, BAS are likely to be discovered for the criminal market and adapted for use within the current botnet infrastructure. However, the adaptation of BAS for the use in botnets requires clearing a few hurdles. Our intention is to show that these hurdles are minimal, offering only an initial barrier and short time window before being tackled by criminals. One of these barriers is, as we will show in the following, the need to hide the information flow of a botnet due to the deterministic and specialized nature of BAS. Among other things this requires the use of modern covert channel techniques.

*Covert channels* were defined by Lampson as channels "*not intended for information transfer at all*" in 1973. The definition of covert channels was extended by the U.S. Department of Defense (DoD) as "*any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy*" [Dep85]. In other words, covert channels are not foreseen by a system's design but due to their existence nevertheless allow a security policy-breaking communication [And08], e.g. between confined processes. Covert channels in networks enable stealthy policy-breaking communication between computers and help adversaries to keep a low profile.

We present the first work combining the three mentioned research areas to highlight the potential of a novel class of botnets, namely *smart building botnets*, i.e. botnets that do not attack common network systems to utilize their computing power and network connection, but BAS instead, aiming to utilize their sensors and actuators to perform physical measurements and actions. Thus, smart building botnets allow the monitoring and control of buildings. According to the botnet's size, entire smart cities or even economies could theoretically become part of a smart building botnet. Moreover, BAS communication does not differ between most buildings as only few BAS protocols are widely used. Critical building infrastructure such as hospitals or airports can thus become part of a smart building botnet as well as private housing facilities.

The benefits for malware developers are manifold. First, malware attackers could monitor events (e.g. movement patterns) in a large number of buildings and could thus create usage profiles of inhabitants, which could be sold later on a black market. Second, miscreants can aim at causing a denial-of-service in a building (e.g. forcing an evacuation by a false fire alarm). Third, in contrast to mobile devices and PC systems, BAS are permanently available, rarely modified, face nearly no security features, are designed for long-term deployment and are rarely patched. This makes them an excellent choice for placing bots. Fourth, buildings can be used to blackmail their inhabitants and owners (e.g. forcing the transfer of money to a bank account to end a disruption on a critical system such as an airport baggage transfer system or lifts in a hospital).

*Roadmap*. The paper is structured as follows. Section 2 covers related work on covert channels, botnet communication, and building automation. Section 3 explains the concept of smart building botnets, their benefits for malware authors, and their technical feasibility. We discuss preventive measures to be taken in order to protect building infrastructure and summarize our findings in Section 4.

## 2 Related Work

We combine three research areas, namely network covert channels, botnets, and BAS. Related work on all three areas is discussed separately.

**Recent Developments in Covert Channel Research:** Yarochkin *et al.* propose *adaptive covert channels* [YDL+08], i.e. covert channels able to adapt their communication techniques to changes in the network environment. For instance, if a covert channel communicates using HTTP and an administrator blocks all HTTP communication after some time, the channel can switch to another protocol, e.g. DNS, to continue its operation.
Other significant developments of the last years are the so-called *control protocols* or *micro protocols* [RM08]. Control protocols consist of small headers placed inside the hidden data transferred through the covert channel. Therefore, most control protocols are placed in unused fields of network headers. Alternative approaches exist, e.g. [MK06] place part of the hidden control data in a watermark.
Control protocols enable various features such as reliable data transfer, session management, peer discovery, dynamic overlay routing, switching of the utilized network protocol, and adaptiveness to changes in the network configuration [WK14].

**Modern Botnet Communications:** Former botnets transferred their command and control (C&C) traffic in a simple manner using network protocols such as IRC. Today, botnets obfuscate and encrypt C&C traffic in order to compound detection and take over. Recently, a Linux malware using a simple network covert channel within SSH connections has been discovered by Symantec [Sym13]. Moreover, a steganographic botnet named *StegoBot* already exists. However, StegoBot is not based on network covert channels and rather hides within social network communication by using image steganography [NHP+11]. Another example for this type of covert channels is the *Feederbot*, described by Dietrich *et al.* [DRF+11] which uses DNS as hidden C&C communication channel. Using social networks for covert channel C&C communication is a rising trend in the criminal landscape, as shown by Kartaltepe *et al.* [KMXS10] who described an example "social" botnet using *Twitter*. These examples underline that the integration of information hiding features into malware has already started.
We see a huge potential for attackers willing to improve the stealthiness of C&C communication using covert channels. Micro protocols can therefore replace existing C&C protocols, as existing micro protocol engineering approaches (cf. [WK14]) do not only optimize the protocol's stealthiness but in addition help to keep the botnet communication feature-rich. Adaptive covert channels can additionally increase the robustness of C&C communications as they can bypass blocked protocols and, in combination with dynamic overlay routing, bypass firewall routers.

**Building Automation (In)Security:** BAS form networks which can be interconnected with other buildings and the Internet (e.g., for remote monitoring purposes) and therefore use different protocols, especially *Building Automation Control and Network* (BACnet), *European Installation Bus* (EIB)/*Konnex* (KNX), and *Local Operating Network* (LON). These protocols feature specific security standards, which have been improved over the time. However, even though security features are available in standards they are commonly not integrated in devices nor used in practice.

Former BAS were designed to work as isolated stand-alone systems with basically no security features. Due to the need to increase BAS' functionality, inter-connectivity, interoperability, and especially Internet access became significant features of BAS. Unfortunately, precisely the inter-connectivity of BAS enables remote attacks. Attacks on BAS can, for instance, focus on getting physical access to a building by exploiting window or door actuators [Hol03], on getting access to an organizational intranet [SZ12], or on disabling a building's functionality via DoS attacks [GKNP06].

Granzer *et al.* presented a hierarchical attack model for BAS in which they distinguish attacks on the BAS network from attacks on the devices themselves. Network attacks comprise the interception of a communication (using a sniffer), the modification of network data (via man-in-the-middle attacks), the interruption of the communication (e.g., denial of service attacks and the redirection of traffic) and fabrication attacks (i.e., the generation of new malicious frames and replay attacks) [GPK10]. As for device attacks, the authors distinguish between software-side attacks (e.g., code injection), side channel attacks (based on timing, power, and fault behavior analysis), and physical attacks (e.g., replacement of devices) [GPK10].

While Granzer *et al.* were the first authors to *mention* side channel attacks, our own previous work describes the existence and use of covert and side channels *within* BAS (cf. [Wen12, WKR12]). Side channels within BAS allow inhouse adversaries to monitor events in the building. For instance, an employee could try to monitor events in floors or areas of a building he has no access to. Covert channels in BAS allow inhouse adversaries to bypass data leakage protection (DLP) and to leak confidential data through the BAS out to the Internet. However, none of these mentioned publications covers the concept of smart building botnets.

## 3 Covert Smart Building Botnets

Existing botnets take over IT systems in order to utilize the performance, storage space, and network connection of these systems to attack target systems or networks (DoS attacks) or to transfer spam messages. Physical devices, like temperature sensors of computers, are not used by today's botnets. If bots attack BAS, two different scenarios may arise. First, the remote accessible component of the BAS (e.g. an embedded Linux system) is attacked and used for already known purposes (e.g. spam transfer). Secondly, the actual capabilities of the BAS are used by the bot software. We focus on the latter case as it represents a novel approach.

### 3.1 Utilization of BAS Equipment for Bots

BAS comprise sensors (e.g. temperature, humidity, or presence sensors) and actuators (e.g. electronic windows, heating, ventilation, air-conditioning, or electronic light switches). These sensors and actuators allow two generic uses for adversaries:

1. *Monitoring of Events in Buildings*: Spyware can determine whether persons are present at a particular location of the building (e.g., based on temperature and heating in rooms as well as by using presence sensors). Intruders can use such information to organize and direct break-ins. Therefore, thefts could, for instance, steal equipment on floor 2 if all persons reside or move around on other floors or in the basement. Moreover, monitoring data such as movement patterns of inhabitants can be leaked to the botmaster using a network covert channel.

2. *Remote Control of Buildings*: Malware can take advantage of the actuators of a building, e.g. heating, air-conditioning, ventilation or elevators. Even for single BAS, miscreants may cause considerable damage using these actuators [Fis12] (e.g., disabling fire alarms before placing a fire in the building [Hol03], activating a fire alarm at an airport to cause chaos [Con08], or deactivating an airport's luggage transport system). Another example would be to cause a DoS at the physical access control systems of an enterprise building to prevent that employees can access their office rooms, what could, in the worst case, result in inactivity of a company.

However, speaking of a *botnet*, new scenarios arise, namely the attack of larger infrastructure distributed over many buildings, smart cities, or, theoretically, even economies or states. If adversaries manage to place a high number of building automation bots in such a smart environment, the possible effects of the discussed scenarios increase, as we illustrate using the following scenarios.

1. The mentioned actuator-based attacks (e.g., attacking physical access control systems) can be multiplied by a botnet, e.g. miscreants may attack multiple airports, train stations, and public or private buildings of an economy simultaneously, i.e. the scale of the attack is extended.

2. In order to increase sales for oil or gas, an oil (gas) company could place bots in the BAS of a region or economy and could slightly but permanently increase the heating, ventilation, and air-conditioning levels at night in as many buildings as possible. This would increase the energy consumption and the need for oil (gas).

3. Hellwig *et al.* show that excessive heating affects people's efficiency and capability to work within buildings [HNB+12]. Smart building botnets could take advantage of this effect by increasing the temperature in trading places (e.g. at the Frankfurt Stock Exchange). This allows for influencing trader's reaction time on the targeted stock exchanges.

4. In [Con08], it has been reported that turning off the heating of a server room can cause a room-wide denial of service due to server failures. Such a scenario can be extended by BAS bots to attack a high number of server rooms (simultaneously).

5. An assailant could try to blackmail inhabitants of a high number of buildings by attacking these buildings. Elders, handicapped and weak people could be locked inside buildings (by closing windows and doors automatically) if they do not transfer an amount of money to a given bank account. While, at first sight, elders appear

as untypical BAS users, the value of BAS integration in their homes is linked to *ambient assisted living* (AAL), i.e. the support of the daily life of inhabitants. AAL allows elders to live longer in their own homes before being forced to move to a nursing home and thus AAL is a growing market.

6. Due to the high number of sensors integrated in modern buildings and their diversity, assailants can aim at collecting as many personal data of inhabitants, employees etc. within a building as possible. For instance, presence sensors, temperature sensors, heating levels and light actuator states indicate the (potential) presence of persons in a given area of a building while the nightly use of light in the bathroom may indicate the illness of an inhabitant. Moreover, the presence of AAL sensors and actuators can indicate serious health problems. Such information can be sold at the black market and, for instance, allow thiefs to prepare intrusions in a way adapted to the movement patterns in a building or to insurance companies for allowing an a priori healthiness check of future insurants.

7. A coordinated smart building botnet could activate a high number of devices (especially white goods and other household appliances) simultaneously in order to create peaks in a region's energy consumption.

However, a direct interaction with the BAS can raise a higher level of attention as direct control information passes public networks and because BAS control information is not hidden. If, on the other hand, BAS control information is hidden in low-attention raising covert channels, the operations can be kept more stealthy.

### 3.2 Botnet Architecture and Feasibility in Practice

The concept of a smart building botnet is visualized in Fig. 1. The botmaster controls a number of BAS using network covert channels and applies the previously introduced techniques (control protocols, adaptive covert channels) to hide his communication. The sensors and actuators of each BAS are under control and monitoring of the particular bot.

Bots are therefore placed directly on the Internet gateways of BAS or on remotely accessible *central control units* (CCUs) used in cheaper home equipment like the *HomeMatic*. An increasing number of these cheap home automation systems become available to end-users and thus increase the number of so-called *smart homes*. With the rising number of smart homes, the number of attackable private houses as well as the effect of bot attacks on BAS increases. Typical CCUs run on embedded systems (e.g. embedded Linux, as in case of HomeMatic) and are, even if set up in a secure way, not patched regularly by private owners.

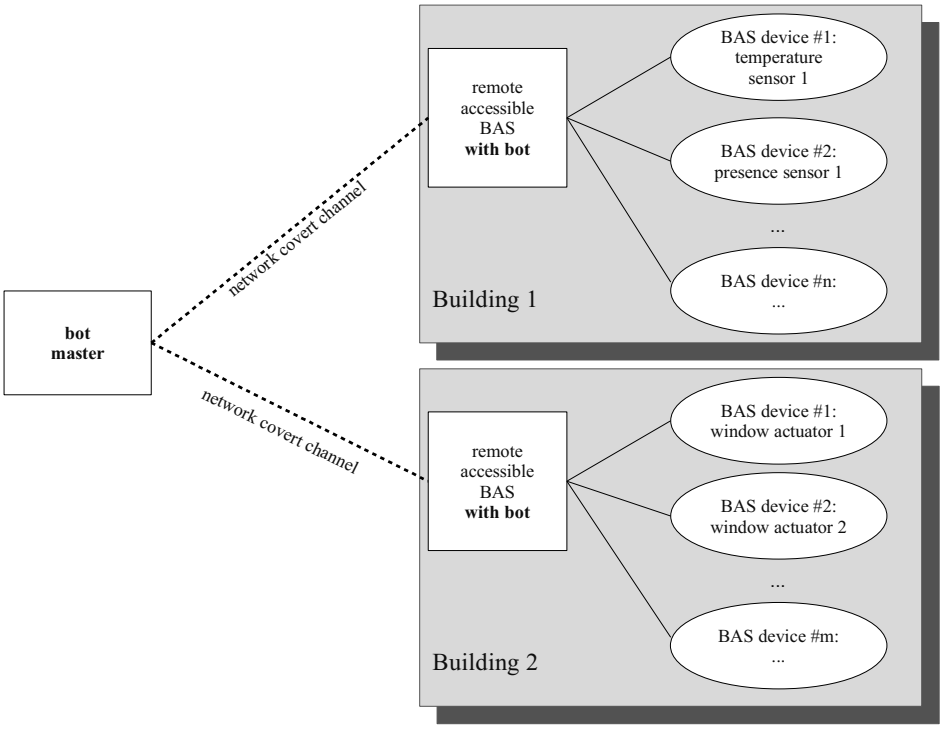


Figure 1: Concept of building automation botnets in combination with covert C&C channels.

A similar problem arises in public and business buildings. Although hardware components are usually of higher quality and robustness, the patching of BAS equipment often is not done by the administration staff. Reasons, why patches are not applied, are the lack of available patches, the limited capabilities of legacy equipment, and the lack of the staff's security awareness.

The infection of BAS installations with bots can be achieved in three ways. First, BAS can be infected by searching vulnerable BAS via the computer search engine *SHODAN* (cf. *www.shodanhq.com*). As shown in the *Industrial Risk Assessment Map* (IRAM), control systems and BAS with Internet connectivity can be found worldwide. In the USA, BAS are available even more often than SCADA systems, PLC systems, HMIs and other automation equipment [MK14]. The IRAM project moreover determined the presence of approximately 14.500 directly online accessible BAS in the USA and approximately 1.300 BAS in Germany. Of the determined remotely accessible BAS installations, 9% are linked to officially known CVE vulnerabilities [MK14].

Secondly, the infection of BAS can be done by hand. Therefore, BAS wardriving, which we presented in [KW13], is considered a means to infiltrate a smart city. In BAS wardriving, adversaries drive through a city in order to determine the presence of wireless BAS. Wireless BAS are popular as their integration in existing buildings is easy and as they are

cheaper than wired BAS. However, BAS wardriving is *slow* since only semi-automated (attackers need to invest time to drive through a city). Moreover, no numbers on the quantity of vulnerable wireless BAS per region are known. Therefore, we consider the second approach as unsuitable for the setup of botnets. In future work, we plan to investigate the feasibility of utilizing GPS-enabled smart phones to discover wireless BAS within a region. Combining the utilization of smart phones with a vulnerability test of BAS would change the second approach from a semi-automated to an automated approach.

A third approach exist in which no bot software must be placed at the target system and in which no network covert channel needs to be applied. Like in the first approach, an attacker searches for directly accessible BAS installations using SHODAN, but then probes whether these BAS directly accept BAS protocol commands. For instance, a BACnet device could be directly connected to the Internet and could thus accept BACnet commands. Such an accessible BACnet device can execute monitoring commands as well as actuator commands and thus, needs no bot software and can be directly controlled by the botmaster. The drawback of the third approach is that it is more likely to raise attention than the covert channel-based first approach.

We consider mixing all three approaches as a useful strategy for malware authors. A smart building botnet might comprise directly controlled BAS (third approach) as well as covertly controlled BAS (first approach). The integration of manually selected BAS (e.g. using BAS wardriving) into a botnet appears only beneficial if the BAS is of significant importance (e.g. an airport may increases the magnitude of a miscreant's attack).

## 4 Discussion and Conclusion

The delineated concept of smart building botnets and their related risks lead to the question of how to react to this upcoming threat. After answering this question, we summarize our work.

### 4.1 Recommendations for next steps to be taken

We believe that the research community should continue to investigate botnets for smart environments and propose further countermeasures to BAS vendors, BAS owners, BAS operators and to the public.

BAS vendors, on the other hand, need to urgently supply their existing BAS equipment with better protection (hardware as well as software, especially for gateway systems). A challenge in this regard is the migration and hardening of legacy BAS. The migration process includes the integration of newer BAS communication protocols linked to better security features.

It is probably not feasible to raise public awareness for BAS threats in a short term, especially not for the concept of smart building botnets. Furthermore, we believe that the

security awareness and responsibilities of BAS operators and BAS owners will be hard to raise. In other words, we must appeal to the research community, to the politics and to the BAS industry for achieving a better protection on behalf of BAS users.

Therefore, academic research, politics and industrial development need to focus two aspects: *i)* creating means for the protection of existing and upcoming BAS; *ii)* creating means for the detection and elimination of bot infections in BAS.

Moreover, the results are required to be delivered in a limited time window: we believe that the organized crime will use any available means to make profit. It is thus only a matter of time before the hurdles of mastering BAS environments are taken to implement smart building botnets. If no further defensive measures are delivered, botnets will gain stable ground in the BAS infrastructure.

### 4.2 Summary

In this paper, we provide an outlook for the extension of current botnet techniques to building automation systems (BAS) by presenting the concept of *smart building botnets*. Smart building botnets utilize the physical capabilities (sensors and actuators) to monitor and remotely control BAS. We reason that such botnets are feasible in practice and linked to various benefits for malware authors.

Our reason for depicting the threat of smart building botnets is to speed up the integration of better protection means by vendors of BAS equipment. We believe that the time window available till such botnets become common practice must be used to enhance the security of existing and upcoming BAS.

Future work will focus on the evaluation of our concept using different BAS technologies as well as on the development of means to protect BAS.

## References

[And08] R. Anderson. *Security Engineering - A Guide to Building Dependable Distributed Systems*. Wiley, 2 edition, 2008.

[CGKP11] J. Caballero, C. Grier, C. Kreibich, and V. Paxson. Measuring Pay-per-Install: The Commoditization of Malware Distribution. In *USENIX Security Symposium*, 2011.

[Con08] R. Condon/ComputerWeekly. New-generation building management systems blow a hole in security, 2008. http://www.computerweekly.com/news/1331080/New-generation-building-management-systems-blow-a-hole-in-security, retrieved: December 2013.

[Dep85] Department of Defense. Trusted Computer System Evaluation Criteria (TCSEC, DoD 5200.28-STD, Orange Book), 1985.

[DRF+11] C. J. Dietrich, C. Rossow, F. C. Freiling, H. Bos, M. v. Steen, and N. Pohlmann. On Botnets that use DNS for Command and Control. In *Proceedings of EC2ND'11*, Gothenburg, Sweden, September 2011.

[Fis12] D. Fisk. Cyber security, building automation, and the intelligent building. *Intelligent Buildings International*, 4(3):169–181, 2012.

[GBC+12] C. Grier, L. Ballard, J. Caballero, N. Chachra, C. J. Dietrich, et al. Manufacturing compromise: the emergence of exploit-as-a-service. In *ACM Conference on Computer and Communications Security*, pages 821–832, 2012.

[GKNP06] W. Granzer, W. Kastner, G. Neugschwandtner, and F. Praus. Security in networked building automation systems. In *Proc. 2006 IEEE International Workshop on Factory Communication Systems*, pages 283–292, 2006.

[GPK10] W. Granzer, F. Praus, and W. Kastner. Security in Building Automation Systems. *IEEE Transactions on Industrial Electronics*, 57(11):3622–3630, November 2010.

[HNB+12] R. T. Hellwig, I. Nöske, S. Brasche, Hj. Gebhardt, I. Levchuk, and W. Bischof. Hitzebeanspruchung und Leistungsfähigkeit in Büroräumen bei erhöhten Außentemperaturen. Abschlussbericht zum Projekt HESO, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, 2012. (in German).

[Hol03] D. G. Holmberg. Enemies at the Gates. *BACnet Today (A Supplement to ASHRAE Journal)*, pages B24–B28, 2003.

[KMXS10] E. J. Kartaltepe, J. A. Morales, S. Xu, and R. S. Sandhu. Social Network-Based Botnet Command-and-Control: Emerging Threats and Countermeasures. In *8th International Conference on Applied Cryptography and Network Security (ACNS)*, volume 6123 of *LNCS*, pages 511–528, 2010.

[KW13] B. Kahler and S. Wendzel. How to own a Building? Wardriving gegen die Gebäudeautomation. In *Beitrge zum 20. DFN Workshop zur Sicherheit in vernetzten Systemen*, pages H1–H13, 2013. (in German).

[MK06] W. Mazurczyk and Z. Kotulski. New security and control protocol for VoIP based on steganography and digital watermarking. *Annales UMCS, Informatica*, AI 5:417–426, 2006.

[MK14] J.-O. Malchow and J. Klick. Erreichbarkeit von digitalen Steuergeräten – ein Lagebild. In *Beitrge zum 21. DFN Workshop zur Sicherheit in vernetzten Systemen*, 2014. (in German, to appear).

[NHP+11] S. Nagaraja, A. Houmansadr, P. Piyawongwisal, V. Singh, P. Agarwal, and N. Borisov. Stegobot: A Covert Social Network Botnet. In *Proceedings of the 13th International Conference on Information Hiding (IH'11)*, pages 299–313, Berlin, Heidelberg, 2011. Springer-Verlag.

[RM08] B. Ray and S. Mishra. A Protocol for Building Secure and Reliable Covert Channel. In *Proc. 6th Annual Conference on Privacy, Security and Trust (PST 2008)*, pages 246–253. IEEE, 2008.

[Sym13] Symantec. Linux Back Door Uses Covert Communication Protocol, 2013. http://www.symantec.com/connect/blogs/linux-back-door-uses-covert-communication-protocol, retrieved: December 2013.

[SZ12] S. Soucek and G. Zucker. Current developments and challenges in building automation. *e & i (Elektrotechnik und Informationstechnik)*, 129(4):278–285, 2012.

[Wen12] S. Wendzel. Covert and Side Channels in Buildings and the Prototype of a Building-aware Active Warden. In *IEEE International Workshop on Security and Forensics in Communication Systems (SFCS 2012)*, pages 6753–6758, 2012.

[WK14] S. Wendzel and J. Keller. Hidden and Under Control: A Survey and Outlook on Covert Channel-internal Control Protocols. *Annals of Telecommunications (ANTE)*, 69(3-4), 2014. (to appear).

[WKR12] S. Wendzel, B. Kahler, and T. Rist. Covert Channels and their Prevention in Building Automation Protocols – A Prototype Exemplified Using BACnet. In *Proc. 2nd Workshop on Security of Systems and Software Resiliency*, pages 731–736. IEEE, 2012.

[YDL+08] F. V. Yarochkin, S.-Y. Dai, C.-H. Lin, et al. Towards Adaptive Covert Communication System. In *Proc. 14th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2008)*, pages 153–159. IEEE Computer Society, 2008.