TechAndComputer (Aug. 13, 2012) Building owners and designers, and particularly members of the building services industry, are racing to implement intelligent buildings and smart grids, which are widely heralded as a boon in terms of both energy efficiency and facilities management. But many are overlooking the potential risk of malicious attacks on these highly networked control systems.

Share This: **See Also:** **Matter & Energy**

- Construction
- Energy Technology
- Civil Engineering

Computers & Math

- Software
- Computer Programming
- Artificial Intelligence

Reference

- Computer insecurity
- Cyber security standards
- Traffic engineering (transportation)
- Malware

Writing in the latest issue of the journal *Intelligent Buildings International*, David Fisk of the Laing O'Rourke Centre for Systems Engineering and Innovation at Imperial College London warns that, as we have seen with the humble PC, the basic building blocks of intelligent buildings -- the process controllers that make up the distributed building management system (BMS) -- can be infected by malware, often through a 'backdoor' left ajar on a trusted network.

David Fisk notes that: "… the basic system -- for example, the bare minimum standby generators -- should normally be independent of the intelligent-building software (much as a warship still carries a sextant should the GPS be jammed)." And he warns:

"This is not current practice as far as can be discerned from existing ASHRAE and CIBSE standards."

Fisk's article, 'Cyber security, building automation, and the intelligent building' begins with a

short history of the rise in intelligent control -- from the 1960s, when the only real threat was an irate engineer armed with a hammer, through the movement away from bespoke hardware and software to proprietary software such as the ubiquitous Windows system during the 1980s, to the post-9/11 emergence of the anonymous cyber-aggressor.

The middle section of the article then presents a review of a more recent attack, now known as Stuxnet, which demonstrated the wide-ranging havoc that could be caused by malicious software infecting plant controllers. This section also explains how such attacks now present a threat to the 'smart grid' and other open systems.

Finally, the article discusses how risks may be assessed and mitigated, using a hypothetical attack on the heating, ventilation and air-conditioning (HVAC) systems of a super-casino to illustrate the urgent need for the building systems design community to re-think traditional security strategies. As a minimum, building services professionals should deploy a 'whole-system design approach' and owners should plan for periods during which 'intelligence' is not available.

Story Source:

The above story is reprinted from materials provided by **Taylor & Francis** , via AlphaGalileo.

Note: Materials may be edited for content and length. For further information, please contact the source cited above.

Journal Reference:

1. David Fisk. **Cyber security, building automation, and the intelligent building**. *Intellige*

nt Buildings International
, 2012; : 1 DOI:
10.1080/17508975.2012.695277

Note: If no author is given, the source is cited instead.