WE OFTEN USE THE INTERNET to manage key aspects of our lives — our finances, health, relationships — so the thought of also managing our home’s energy supply online may not seem scary. But as our nation’s outdated power grid goes digital, the implications of opening up yet another area of our lives to the online world has some people worried.

The old power system is being transformed into a “smart grid,” which will integrate renewable energy generated from wind turbines and solar panels housed in homes and businesses into the existing grid. Appliances will communicate with each other to decide when they should run, and any excess energy will be sold back to power companies.

While these new infrastructures will certainly be more efficient, the massive amounts of data exchanged will also increase our vulnerability to security breaches. Information about our daily habits — when we’re home, when we’re on the computer, when our appliances run — might be accessed by a third party. It could be the bored teenaged hacker down the street, or someone or something more sinister.

Another challenge is ensuring participants in this new system play fair and don’t hold back their renewable energy to sell at peak hours and premium prices — thus helping their own bank accounts but hurting everyone else’s.

Bruce McMillin, professor of computer science at Missouri S&T, is working on solutions to these challenges. By using information flow analysis, born in computer science, he is working to develop security measures for these new distributed systems.

“This is a new application of information flow analysis,” he says. “We’re using it to reveal design and implementation issues that would compromise the system’s confidentiality.” In this instance, confidentiality is considered violated when information flows from one domain to another domain (such as inside a house to outside the house).

McMillin is working with the National Science Foundation’s Energy Research Center for Future Renewable Electric Energy Delivery and Management (FREEDM) Systems. Missouri S&T is one of seven universities in the United States and Europe involved in the program. Computer Science students graduate students Ravi Akella, Derek Ditch & Thoshitha Gamage and undergraduate students Stephen Jackson and Thomas Roth are working on projects within the Center. Five members of the S&T electrical and computer engineering faculty are also part of the FREEDM team, including site director Mariesa Crow and co-investigators Badrul Chowdhury, Keith Corzine, Mehdi Ferdowsi and Jonathan Kimball.

“We’re looking to use distributed grid intelligence (DGI) to manage the smart grid,” says McMillin. DGI would allow software to manage a home’s energy usage and would detect, isolate and correct any problems that might occur, while fully coordinating with other systems in the home.

McMillin says smart grid systems couple intelligent cyber action with physical operation, which makes determining the information flow much more complex.

“It’s a fundamentally different security challenge because parts of these renewable technologies are visible to anyone,” he says. “You can see if the sun is shining, if the wind is blowing. There is no absolute secrecy.”

McMillin is applying confidentiality properties such as non-deducibility to this future infrastructure. A system is considered as non-deducibility secure if information does not flow from one protected domain to another, lower-level domain. This ensures that the lower-level user cannot deduce any information about the system. In a non-deducibility secure system, observing that the sun is shining on a solar panel does not tell the observer anything about how the collected energy is used, nor anything about the internal information of the DGI — thus limiting a potential attacker’s information.