WHAT IS SO DANGEROUS IN SMART GRIDS?

Artem Chaikin

Electricity is rising in price, and the world economy is looking for new ways to improve energy efficiency. In addition to solar and wind stations, everyone around the world is actively building Smart Grids allowing effective energy use. Because they are usually connected to the Internet, there is natural interest in their security level.

Attention! All the vulnerabilities described in this article have been reported to and fixed by the vendors, but they can occur in current systems.

What They are Made of

China invested $4.3 billion in Smart Grids in 2013, and worldwide the investment made was up to $14.9 billion. Pike Research predicts more than $46 billion to be spent on this technology by 2015. This forecast has found support among economists as well as ecologists. Greenpeace, by the way, believes Smart Grids can save our planet.

Smart Grid technology has only just begun to win over proponents from all over the world. Today, in their simplest form Smart Grids are used in residential climate control systems. Such devices allow end users to monitor and manage the use of the wind and solar energy, and to make use of alternative energy sources in their absence. Are Smart Grids unsafe for advanced housekeepers? To answer this question, we need to know what control components such grids consist of.

Fingerprint utilities request a remote host for its family identity. The answer helps to determine an operating system or device modification.

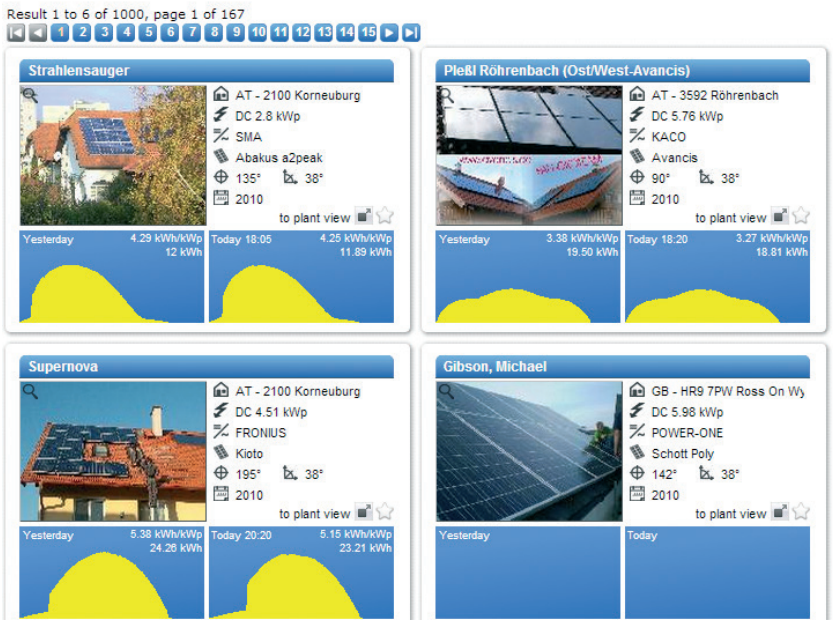
After a small fingerprint research study, we traced the built-in systems served as a basis for Smart Grids of at least nine vendors on the Internet.

While the WindCube family was the most popular, our choice to experiment with another vendor's devices proved to be a smart decision. The vendor provides a controller with numerous advanced features online: PowerPC processor, RTOS, built-in web server, support of FTP, Telnet, SSH, TCP/IP, HTTP, PPP.

In Search of the Smartest

***Dorks** are key words, URLs or their parts that allow using search engines or web scanners to look for a path to a control panel or a page with errors.*

Browsing the Internet for Smart Grid systems based on the controllers selected was relatively easy. Many thanks to the vendor's official website that specified the operating system of the device and guided us on how to study its configuration following the address http://...../ZZZ. We then used inurl to search for information in site subdirectories and Googled the name of OS and ZZZ. Finally, we found several pages with the IP addresses, subnet masks, and serial numbers of certain devices. Within what systems do these microcomputers work?



Solar panels connected to the web server of Solar Sail

One of the pages we obtained uncovered that the platform under research also runs as part of the systems that monitor photovoltaic generators called Solar Sail (we have changed vendor's name). Such generators turned out to be very popular. According to the developer, globally there are more than 200,000 solar power stations and almost 1,000,000 inverters connected to this company's web server.

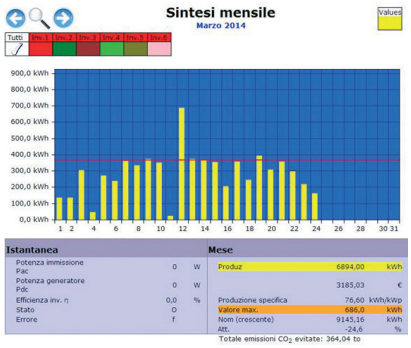
Examining Solar Sail Firmware

Solar Sail firmware cutaway view

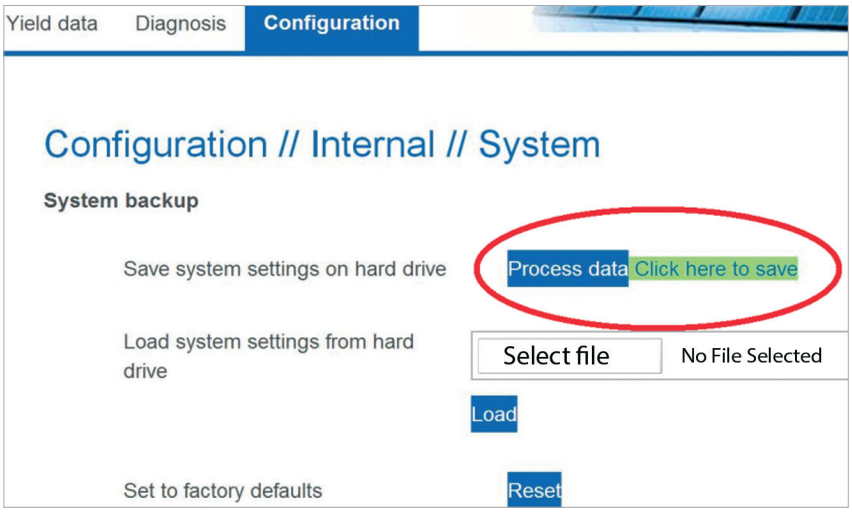
PT Helps Siemens and the Large Hadron Collider

The experts of Positive Technologies demonstrated what they found when analyzing the security of Siemens SIMATIC WinCC Open Architecture, a new SCADA system. This HMI system is used to automate operation of numerous critical facilities, including control over technological processes in the Large Hadron Collider (Switzerland).

SIMATIC WinCC Open Architecture is a part of the Siemens HMI product family employed to create human-machine interfaces and is used in various industries. WinCC OA allowed automating the West-East Pipeline (the world's longest pipeline), the St. Gotthard Tunnel, the Sitina Tunnel in Slovakia, airports in Zurich and Geneva, liquid helium plants, water purifiers and water supply installations.



Power generation data by Solar Sail's Smart Grid systems



Solar Sail control panel

With firmware for Solar Sail systems downloaded, we checked its file structure, looked for Google dorks and configuration scripts that provided system control. Such commands as strings and grep helped to detect the header Solar Sail Client, which spurred us to Google the URL inurl: Solar Sail-Client. As a result, we found numerous systems of individual users and pages with power consumption data for Solar Sail's various Smart Grid systems. However, this type of information would only be interesting to system supervisors.

You Can Go Without Passwords

Having studied Solar Sail's control panels, we found out that approximately 5% of the systems did not require passwords for access to the configuration page. The other 95% did require passwords, but they were of no use. With a query to a configuration script created, we could make the control panel return the configuration backup copy, upload it to our PC, and retrieve the password.

However, we did encounter some problems when trying to decrypt the password, which is always indexed as 222. HEX often resulted in strange things, so we took a different approach: we set an arbitrary password (1234567890) on a non-password protected device, saved it, then downloaded its configuration file, and checked its encryption.

This is also the way to acquire all necessary passwords and their encrypted variants.

Let's Look Further

You've already noticed it wasn't hard to access the configuration page of Solar Sail. The device firmware is available from this page. By the way, Solar Sail's official documentation says firmware updates are password protected. However, only one of the systems required a password, which was easy to guess ("Solar Sail"), and coincided with the login and was unavailable for ordinary users.

What's Tomorrow?

In fact, users of smart houses and mini offices connected to alternative energy sources are beta testers of Smart Grid systems. Developers hardly have any mercy on thrifty owners making gross errors in protection mechanisms. In our case, anyone could pick up a user out of hundreds of thousands of owners of Solar Sail Smart Grids on the Internet, bypass authorization (sometimes it was not even required), install compromised firmware remotely, obtain access to system parameter control and penetrate other system segments. Controlling mechanical systems (disabling inverters, fire, and other unpleasant events) was also possible.

If we continue to move too hastily in making electrical systems more intelligent, the security risks may rise to the level of SCADA systems, and the stories about attackers using computers to disable electricity across an entire city may all be too real in the near future.

```
191;home.
192;username
193;^d5c7d4dbdec5d9c8
194;
195;0
196;0
197;0
210;1
211;1
220;0
221;1
222;^9494949c9c9c9c94949e
230;[Denominazione impianto]
231;[Nome gestore]
```

Configuration file backup copy

IDC Recognized Positive Technologies as Fastest Growing Firm

Positive Technologies has been ranked the world's #1 fastest growing vendor of security and vulnerability management (SVM) solutions by respected market intelligence firm International Data Corporation (IDC). Positive Technologies received this independent confirmation of its rising status in the global security market in IDC's recently released report, Worldwide Security and Vulnerability Management Forecast for 2013-2017.

According to IDC, Positive Technologies grew at a rate of nearly 83% in 2012 while the overall market for SVM solutions grew at a rate of 9.4%.

"The demand for products that allow us to properly assess security and stand firm against new IT threats is one of the engines of our growth on the global market," Yury Maksimov, the CEO of Positive Technologies, commented. "Our ability to deliver a higher standard of results comes from our investments in security research and our hands-on experience detecting vulnerabilities in the networks of global companies."

Among the factors providing for SVM market growth in the nearest future, the experts of IDC name expansion of cloud infrastructures, necessity to protect big data, corporate use of smartphones and tablets, and extensive use of enterprise-level mobile applications.