SMartER Power Grid

Dhananjay Phatak, Nilanjan Banerjee, and Ryan Robucci
CSEE Dept. UMBC, phatak@umbc.edu

Position paper submitted on 31st October 2013 for evaluation to be included in the Dec. 2013 NSF workshop on "Energy-Cyber-Physical" Systems

(A) *The real, fundamental and physical reasons for which today's electric-power-grid must be upgraded*

The commonly purported need for and/or advantages of the so called "smart-grid" (including the often over-rated efficiency obtained by "demand sensitive pricing") are tenuous at best and fall apart under genuine scientific scrutiny. [1]. We therefore start with a brief explanation of the fundamental, non-trivial, physical reasons for which the current electrical power distribution grid needs to be upgraded [1].

In the long run we must live only by sustainable sources of energy (hydro-electric, wind, sun-light); since all other forms of energy, such as fossil fuels, nuclear fission etc. are not replenishable and will eventually run out. The sustainable forms of energy are inherently geographically distributed, and often follow diurnal cycles. For example on a bright and clear summer day, in the pre-dawn hours in California, large amounts of electricity could flow from East Coast while a similar bulk transfer may be needed in the reverse direction after the sun has set in the East but is still shining in Arizona and California. There is a need to aggregate the distributed generation capacity (ex: in all the houses in a region) and then transport the electricity elsewhere. In other words future grid needs to be truly bi-directional all the way to the last/smallest level (that of rooftop panels on top of a house) and have the ability to distribute `OR AGGREGATE` energy as needed, *on-the-fly*.

In contrast, today's grid has been designed to push energy only one way: from central generating stations to end customers. It is therefore not adequate for the omni-directional energy transport needs of the future.

Moreover, the local conditions (ex: sunny or cloudy, windy or not, ambient temperature, etc.) must be sensed in order to assess how much electricity can be produced locally, and what fraction needs to come from central generation stations. In other words, at least some minimal amount of sensing of local conditions and the ability to communicate some data with peers also needs to be included in the future grid.

(B) *Our Novel Cross Domain idea : Leverage the grid as a separate physical path to enhance security*

We have demonstrated that with minimal changes, a smart-grid-like infrastructure can be leveraged to furnish provably strong location authentication certificates on demand, from a Power-Grid Location Server [1, 2, 3], which is extremely important in many scenarios, especially in real-time SCADA control. Obviously, it would be highly desirable to verify that a critical command (for example, to raise or lower the fuel rods in a nuclear reactor) did actually originate at a pre-designated safe place (such as the control room of the nuclear reactor) and was approved by a human operator at that location. Our methods achieve both these goals [1, 2, 3], in essence creating the first class of "killer applications", viz., safeguarding all SCADA controls against remote subversion attempts (for details, see [1, 2, 3]).

Location authentications are also important when critical components (such as routers, DNS servers, etc.) in the control-plane of the Internet exchange routing or other actionable information; in election scenarios to make sure that the election machines were turned-on only on the day of the election, only in the precinct and only for the actual hours the polling stations were supposed to be open. In general strong location authentication can enable "reliable chains of custody".

Another useful application is location-based access control. The DoD could require that the user prove

that they are located at a pre-designated safe location (via a location certificate obtained from the Power-grid location server). Unless the certificate is furnished, access to sensitive documents can be denied. This would prevent an adversary from remotely downloading sensitive secrets (China supposedly stole a whole lot of secrets by remotely penetrating DoD systems and downloading documents including designs of some nuclear weapons, and most recently the design parameters of the Joint Strike Fighter from computers of the contractor Lockheed-Martin).

Another application might be where the DoD requires that the cloud-services or data-storage providers must not archive sensitive data at offshore sites; that data must reside on storage devices within the US and the location certificates from electric power grid location server can be used to verify compliance.

The second class of "killer applications" is anti-theft tracking. If electric cars is the future then the entire grid can serve as an anti theft infrastructure. It is clear that the same concept can be extended to tracking any device that needs electric power. For example, a laptop can be configured (partly in hardware) in such a way that during the boot, it sends a message to a grid-location tracking server, via the plug, electric meter and the (last hop) electric conductors of the power distribution network. A grid-location tracking server then checks whether the meter (and therefore the plug that relayed the message) is at one of the prior designated "allowable/safe" places, and sends a "you are blessed to run" or "you are connected at an unexpected place, not authorized to run in normal mode" message back across the power-plug. Unless a clearance message is received, and verified; the device (laptop) can be configured to ask for more passwords and/or security questions or boot with limited access/functionality or in the extreme case, erase the entire disc and shut itself down (depending upon the level of paranoia). Note that operating on batteries for a long time (to avoid the use of electric plugs because plugging-in the device can disclose the location as outlined above) is itself a cause for suspicion in most cases (unless the laptop is being used in severe outdoors environments or experiments). Therefore the configuration can be easily modified to go into protective mode if the "blessings" from the grid-location-tracking server are not received after say every 10 or in general some "n" cycles of sleeping and awakening or rebooting.

Likewise one could set passwords on lights before leaving for a long trip (to deny thieves the usage of lights), or in general put a limit on the amount of power a plug will deliver.

For extremely critical appliances (for example the centrifuges in nuclear purification plants) the power plugs could be programmed so that the devices they are supplying have to "ask for a permission" before they can draw unusually high amounts of power from the plug. There is a chance that such controls might have prevented STUXnet from doing the physical damage that it did by spinning the centrifuges erratically and out of control thereby physically destroying them.

A third class of killer applications is to also relay emergency messages via the electric conductors. In addition to whatever methods are being used by home-monitoring services, they could also send emergency signaling messages via the last hop electric conductors. The more the number of paths the emergency messages go through the better. An event affecting the entire community might be signaled for instance by flickering the lights and or displays (if any that are on) at a rapid frequency to grab the attention of someone playing a video game in their favorite virtual reality setting, perhaps in a well isolated sound-proof room, signaling to them that they should check the news, or look outside, there might be a tornado approaching or that their house is likely to get flooded in the next 10 minutes, or that there has been an earthquake...
This is a variant of an old idea: during world war II, British electric utilities used to drop the frequency of the AC current to signal an impending air-raid.

In [1, 2, 3] all possible issues such as "why not GPS"? what about other existing authentication methods? are fully addressed in detail. In particular, our methods can be incorporated as an additional independent factor in any existing multi-factor authentication scheme; there is no need to abandon existing methods that work well. Moreover, the cost of upgrades is subsumed under the "SMart Grid" initiative anyway. Therefore the utility companies can immediately create permanent new streams of revenue by offering security services and applications (outlined above) across the electric conductors in the last hop of the

utility grid and the end-user electric meters; at almost zero direct infrastructure upgrade costs.

In summary our novel cross-domain idea is to use the conductors in the last hop of the electrical distribution network as physically separate path over which only security tokens and control messages are exchanged. Note that electrical conductors cannot compete with optical fibers for high bandwidth delivery of consolidated Video/Phone/Data services over the Internet that most ISP's offer today, simply because they were not designed to carry data, they were designed to carry electric current.

However, they have sufficient bandwidth to carry only security tokens and/or control and emergency messages. As a matter of fact, starting from about 2005 or 2006, the city of Manasses in Virginia was providing Broadband over Powerline (BPL) service to its customers, i.e., for some fixed dollar amount per month, people in Manasses could get their Internet service (about 1-10 Megabits/second) through their Electric Conductors; instead of (formerly Coaxial) Cable-based ISPs (most the Coaxial cables have been replaced with Optical-Fibers by now). The reason we mention this fact is to prove that BPL delivery has been done before, the technology is mature. In fact the BPL standard was finalized by the IEEE in 2011, just about a couple of years ago.

It is a blessing in disguise that that effort (in Virginia) failed and that BPL service has been discontinued since 2008; because there is no point in competing with optical fibers for regular internet/TV/Video data delivery. That would be a misuse of the (relatively) small but precious bandwidth that the electric conductors offer.

There is a golden opportunity to re-create an Internet-like infrastructure across/over the electric grid distribution network from scratch. This time there is added opportunity to not repeat the mistakes of the Internet. In particular, Security must be considered from the get-go in every step and protocol implemented in such a network. We strongly recommend that this network remain as separate as possible from the Internet, in order to avoid importing all the junk and problems associated with the Internet.

Note that after the optical-fiber from the ISP, the electric power conductors make-up the 2nd highest-bandwidth pipe/path which is physically-separate (from the default data-path provided by ISPs) and also reaches almost all end users. Its (relatively) small but precious bandwidth should not be squandered away; either in a futile competition with optical-fiber data pipes; or by allowing arbitrary Internet traffic. Rather that bandwidth should be used only to exchange security tokens and control message to enhance the security of all electronic communications at large.

References

[1] D. S. Phatak, "Smarter electric grid viewgraphs," Sept. 2012.
URL: http://www.cs.umbc.edu/~phatak/cybersec/grid-viewgraphs-sept-2012.pdf.

[2] A. T. Sherman, D. Phatak, V. G. Relan, and B. Sonawane, "Location authentication, tracking, and emergency signaling through power line communication: Designs and protocols for new out-of-band strategies," *Cryptologia*, vol. 36, no. 2, pp. 129–148, 2012.

[3] D. S. Phatak, "System, method, and apparata for secure communications using an electrical grid network," May 28 2010. US Patent App. 12/790,285, First set claims has been approved as of November 2013, and a Patent is expected to be issued in the near future.