wardriving the smart grid

:: practical approaches
to attacking utility packet radios ::

shawn moyer
and
nathan keltner

DefCon 00010010

This page intentionally left blank.

This page intentionally left blank, too.

This page wasn't supposed to be blank.
Not sure what happened there. Plz advise.

"The truth is also that a well-placed squirrel can wreak almost as much havoc as a cyber attack on a power grid."

“Doctor” Charles Palmer, Director, Institute for Advanced Security, IBM, June 2010

“We must find this well-placed squirrel, and ensure that it never falls into the hands of our enemies.”

Shawn Moyer, esq, The Internet, June 2010

If you haven't just emerged from a coma, you probably have some idea of the multifaceted attack surface that the inevitable modernization of power transmission and distribution is rapidly introducing.

What you may not be thinking about just yet, though, is the path much of that attack surface travels on... The air around you.

So where do we start? The "Smart Grid" itself is pretty well understood at this point, and I won't bore you by linking to some Wikipedia article or other and describing it.

At the end of the day it's pretty simple: Utilities have been operating more or less in the dark, or at least at a macro-level, for a long time now, with no real idea of load or usage beyond (at best) a neighborhood or substantion level. The price paid for that lack of visibility is clear as well: brownouts and blackouts caused by unexpected or unforeseen changes in load that, while rare, often have a domino effect due to interdependence between utilities. At a less intrusive level, utilities struggle with either overbuying or underbuying capacity, with an unexpected heat wave or a cold snap enough to put planning off the rails.

The basics are pretty straightforward - let's connect utility distribution, delivery, and transmission, let's automate where we can. Let's monitor load, usage, and demand, and adapt our delivery in something closer to real time.

In reality, the notion that in 2010, utilities are still "rolling trucks" to connect and disconnect service and gather usage data is laughably quaint. Imagine an ISP with no QoS, no granular view into real-time usage or load, no bandwidth caps, no weight-based routing protocols, no metered bandwidth. Your cell phone, cable, satellite television, and broadband providers all have near-instant visibility into load, demand, and usage, and have for over a decade.

Is it really so unreasonable to expect electric, gas, and water utilities to want the same just-in-time data, the same accuracy? No, it's not.

Unfortunately, though, it's not quite that simple. Because US utilities are so late to the party, and thanks in no small part to some well-intentioned but missapplied stimulus money,

adoption of grid automation is happening at a breakneck pace, and as with any rapid push of new technology, Mistakes Are Made.

And those mistakes have greater potential consequences than, say, the great Central Colorado Comcast Outage of July 1, 2010, which, while certainly frustrating to the writer of this document due to his inability to stalk nearby strangers on Foursquare, ultimately doesn't quite equate to a real disruption of critical infrastructure.

If we accept that this stuff is inevitable, and that at least the rationale to interconnect all of the grid's naughty bits together makes sense, what's the quickest way to move things forward?

Let's say you've got a few million homes to bring online, a handful of power stations, a few thousand substations, maybe a reactor and a geothermal plant or two (kidding, mostly), and you've got a few million in stimulus money to do it with, which unfortunately has a shelf life of 24 months or so.

Yep, you're probably going wireless. It's quick, it's low-footprint, and all of the vendor whitepapers you read seem to say the right words, "FIPS-140, encrypted, secured transmission, signing certificates", and whatnot. Sure, there are rumblings of standards bodies and requirements definitions, like AMI-Sec and UtiliSec, or even some bazillion-page audit spec from the fossils at NERC. But you need to go live now, you don't have time to wait for committees and subcommittees to ratify some watered-down list of vagaries.

And that vendor whitepaper looks fantastic, it really does. It has flow charts and everything.

[The rest of this paper, with actual kung fu beyond random rambling, will be available at http://www.agurasec.com/WardrivingTheSmartGrid/ on the day of the talk. Also, because I don't think anyone really reads these papers before they go to talks, prove me wrong. Go to that URL, and read the HTML source and we'll know if you saw this beforehand.]