SMart^{ER} Power Grid

Viewgraphs presented at the National Energy-Cyber-Physical Systems Workshop organized by the the NSF (@Arlington)

16th December 2013

Dhananjay S. Phatak

phatak@umbc.edu

Disclaimer

- The adjective "**SMart*ER***" could be (mis)interpreted to infer that our methods and systems are simply a rehash of the usual or conventional topics that are implied by the (cliched) term "Smart Grid"

- We unveil completely independent cross-domain ideas about how the grid operators can immediately create **permanent revenue streams ($$$)** by using their conductors to provide **"Cyber Security"** services.

SMartER Power Grid Exec Summary : it can Defeat All Remotely Executed Subversion-attacks and more..

1) **Defeat All Remotly Executed Subversion-attempts (DARES) :** Novel cross-domain solution that ***solves*** the problem **of protecting critical infrastructure** from remote attacks ; even if computers that control components of the infrastructure are remotely subverted.

   + Smart power connections to mitigate threats like the STUXnet.

2) **The second wide class of applications** : tracking and theft-reporting (electric cars, laptops, … more generally any device that needs electricity)

3) **Third wide class of applications** : Reliable Chains of Custody (verifying the proper operation of election machines, ensuring that sensitive cloud data is physically stored only at pre-designated safe locations and not in foreign countries ….), Digital Rights Management/licence control

4) **Fourth wide class of applications**: PLES : Power-Line Emergency Signaling

- Sounds too good to be true ? read on & contact phatak@umbc.edu

Main Idea

- We propose using electric conductors in the last-hop of the power-grid together with the electric power meter at the end-user premises to implement additional/side-channel(s) to enhance security (via physical path diversity in multi-path/multi-factor authentication).
- Whatever works currently should be left alone; location authentication via power-lines/meter essentially provides additional dimension/factor that can be added to existing multi-factor authentication schemes

Why Power-lines ?

1. Physically distinct path to end-user premises
   - imp; given the dwindling diversity of data-paths
2. Electric©City essential => high coverage
3. **Fully Bidirectional channel (unlike GPS)**
   - provides finer resolution than GPS in many cases
   - GPS may be obstructed or unavailable
4. Denial of Service (DOS) attack harder: needs
   - physical path break => cannot be done remotely
5. Can use unlimited amount of power => can
   - use long keys for strong crypto + unlike mobile devices (phone, GPS ..) no size/wt, battery limits

advantages++

6. Can withstand **+ Report** power outages
   - (with battery backup) [this itself could be a killer-app]
7. US power grid: isolated from grids in china, russia..
   - physically separate => harder to penetrate
8. Provably Strong location binding
   - portable device (phone, GPS…) can be stolen
   - In contrast a **power meter cannot be "stolen"**, it must be located at a fixed place designated by the utility company & **its presence at that place can be tracked**
9. Legal precedent: utility-bill is accepted as
   - proof of legal residence => location certificates issued by power-grid-server are likely to be acceptable to all

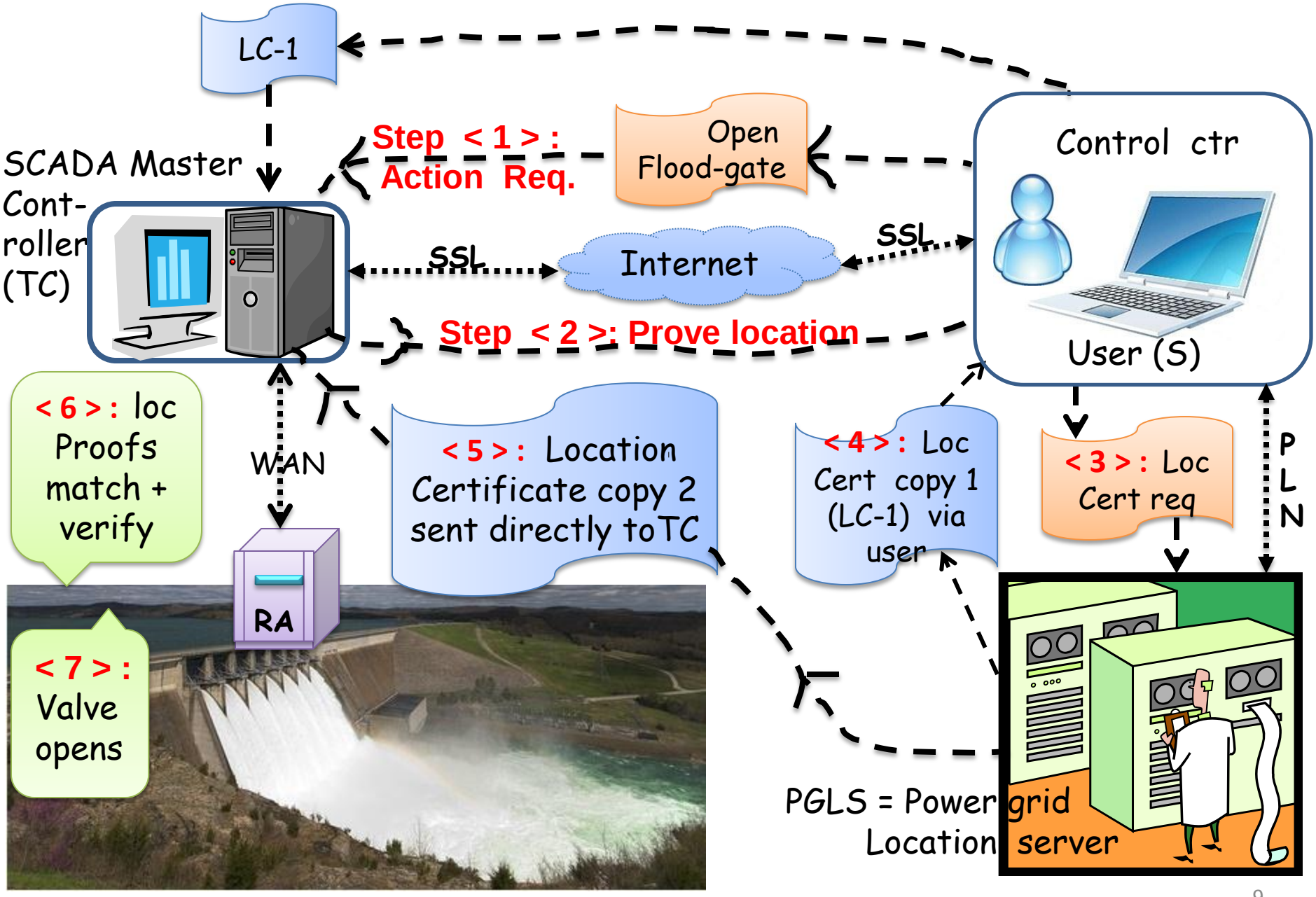
$$++

10. Flexible: use it by itself or as an add-on
    - Independent factor/dimension in a multi-factor authentication scheme
    - can be adapted depending upon the criticality of application. ex: real-time SCADA control vs. location based access to docs/data(bases)
11. THE most important benefit is the fact that **Infrastructure creation cost ≈ 0**
    - can be piggybacked onto, (i.e., absorbed into) the upgrades to the grid that are slated to take place under the “Smart Grid” initiative.

Business case : Killer apps class 1: **Protecting Critical Infrastructure**

- Strong real-time Location binding => real-time access control based on location.
- our methods can **verify that the source of a (trans)action request is at a (pre)-designated ``safe location''** (such as a grid-control room or a hydroelectric dam control center etc).
- our method can **also verify that there is a human in the loop**, i.e., the (trans)action was indeed approved by a human

Location based SCADA access control



RA = Remote Actuator, TC = (Trans) Action Controller, PLN = Power Line Network

Steps illustrated in the diagram

- **Step 1:** user (ex: an operator in a control room) issues a command for a trans-action (ex: open flood gate) over the regular communication channel (we call it the "in-band" communication channel)
- **Step 2:** TC (trans-action controller) issues a challenge to the command issuer: prove that you are located at a pre designated / safe location authorized to issue the command. Proof ≡ location certificate from a Power Grid Location Server (PGLS). Loc. cert valid only for the trans-action requested and pending; & includes the trans-action parameters.
- **Step 3:** operator sends a request for location Certificate (LC) via the powerline-network (including the HAD = Human Authorization Detector, Electric Meter, Nearest curbside transformer or substation upstream from the electric meter.

- PLN necessarily includes an **out-of-band communication channel**
- If all credentials/tokens/nonces/keys can be verified; the PGLS is certain that the bits were physically sent by the meter.
- **Steps 4 and 5:** PGLS creates at least 2 copies of the location certificate; sends one copy in the reverse direction along the forward path and another copy directly to the TC via the regular in-band channel
- **Step 6:** TC verifies that both copies match or are consistent w.r.t. each other and the original trans-action requested

- **Step 7:** Only after this verification the actual trans-action is allowed to execute (in the example in the diagram the TC instructs the Remote Actuator (RA) to open the flood-gate)

PLN ≡

S ⟷ HAD ⟷ Electric Meter ⟷ Last-Hop-Server ⟶ PGLS

Pressing the HAD switch(es) generates unique token/nonce sequence that is known to the Meter (they both share cryptographic seeds/secrets that are created at install-time)

Electric meter (EM) relays encrypted messages to/from the Last-Hop-Server (LHS) via the electric conductors in the last hop.

Our last-hop-server (LHS) picks up the message and sends it to the PGLS

Robust + fool-proof

- Don't mess with the power grid any more than necessary
  - our design PHYSICALLY PREVENTS the use of power grid paths further up-stream beyond the last-hop (to minimize interference with the utility)
- Location Certificate: 2 copies via separate paths

- At the TC : Unless the two copies match the (trans)action is *not* allowed.

Thwarts all remote attacks even if "S" is hacked

mitigation of STUXnet & other threats

- Smart electric plug/outlet : require a passwd before it gives power (ex; to deny the usage of lights/electricity to burglars)

- More generally: power connections supplying electricity to critical components (like, the centrifuges in the **STUXnet** example) could be programmed to supply power within strict limits + in a pre-set temporal pattern
- Most modern controls use electrical devices..

Independent monitoring of critical systems

- If too much power is being used
  - for example: to over-drive the centrifuges
- or the actual/observed power usage pattern seems to deviate substantially from the expected/normal power usage pattern
  - Ex: when the centrifuges were repeatedly spun very fast and then slowed down drastically until they broke down.

then the “smart” power outlet/connection can raise an alarm or shut the system down…

Business case: Killer App class 2

- **Entire grid can be leveraged as a tracking and anti-theft infrastructure**
  - electric cars can be tracked if stolen
  - How long can a lap-top be kept away from a power plug ? It must be charged at some point.

    the laptop can be configured as follows: during boot, unless it (the laptop) receives a "you are blessed to run" message sent by a tracker entity across the electric conductors via the electric plug, the laptop goes into safe mode or shuts itself down …

Killer App class 3: Reliable custody chains, DRM

- Tracking => Reliable custody chains
  - Election machines … even … shipping containers
- DoD could verify (via Power-Grid location certificate) that cloud service providers are storing sensitive data on devices that are physically located within the U.S.

- DRM/software Licence control: s/w vendors could find the location where their s/w is being run (via a Location Certificate)

Killer App 4: Emergency messaging

- home-monitoring systems (Brinks, ADT..) send messages to authorities (police, fire-stations etc) if some event is detected.
- In addition to whatever communication mechanisms they use today, the same msg can also be sent via electric conductors.
- Sending urgent message via multiple paths increases the chance that it will get through.
  - Emergency signaling goes back to WWII UK : to signal an air-raid, drop AC frequency

Unique advantages in emergency signaling

- **wide area Emergency signaling via power-grid:** Warnings of approaching tornadoes, tsunamis, flash floods, forest/wild-fires ….. Can also be delivered via power-grid in addition to all other current methods.

- Ex: switch the lights/display-screens etc. in the target area on/off at a pre-determined rapid flicker rate to signal emergency.
  - **Even if a web-junkie is comfortably ensconced in his/her basement; completely engrossed in their favorite virtual world/universe/games with visors and ear-phones put-on; flickering the lights/displays might grab their attention…**

Potentially large future app class 5

- In the near future, Identity translation and verification transactions will explode in number (someone will be translating and verifying identities 24/7/365)….
  - Ok 24/7/365.2425… (must have at least 1 joke….)
- That volume will dwarf the volume of transactions handled by visa/master-cards; in fact all credit card companies put together.
- Who is poised to gobble up all that business?

ISP's = Evil Empire ??

- ISP's: they own the single highest b/w data path (typically an optical fiber) to user homes
- To prevent monopoly, for anti-trust reasons, some other entities (apart form the ISPs) should also share the action/revenue/profits

- **power companies need to grasp this ASAP**
  - The earlier they get their nose under that tent; the greater the chance that we shall be able to avoid monopolistic stranglehold by the ISP's

Power line = 2nd highest b/w path to end users

- Electric conductors cannot compete with the bandwidth that optical-fibers can provide
  - designed to carry power efficiently, not data
- It is therefore futile to compete with the ISP's for voice/video/data delivery and Internet connectivity
  - An attempt was made: in Manasses Virginia, Internet connectivity @10 Mbps b/w (bandwidth) was made available via the electric conductors
  - However, after 2 or 3 years, that experiment failed (no demand) and was discontinued in 2008

Best use of that small but precious b/w ??

- failure of BPL (Broadband over Power Lines) experiment in Virginia = a blessing-in-disguise because it is futile to compete with optical fibers for data delivery
  - Tantamount to squandering the relatively small but precious b/w offered by electric conductors.

- That small but precious bandwidth is best utilized by reserving it only for exchanging security related (authentication) tokens; & control and emergency messages

Rare Golden opportunity to re-create Internet-like infrastructure from scratch !!

- IEEE has finalized the BPL standard very recently, in 2011 (to the best of our knowledge)
- BPL can potentially deliver substantially larger bandwidth if required, esp. over small distances (in the last hop)
- Networking technology is fairly mature by now: Internet experiment/experience has shown what works well and what does not.
  - All that wisdom/experience should be leveraged at every step in the creation of **SMart**^{ER} grid

Avoid the mistakes in the Internet design

- **Security as an after-thought = disaster**
  - Smart Grid: poised to repeat the same mistakes made in the Internet, web (security = late add on)
- We can and must do better than "best effort delivery": guarantee time-bound delivery
  - For example in the LANs, random access protocols (like Ethernet) must be replaced by much better protocols (such as for example the adaptive tree walk protocol) with strict control to avoid Denial of Service attacks in the Last-hop-networks.

Don’t simply give up, try harder

- QoS Issues
- DoS and DDoS resilience
- …..
- repeating the “software is inherently highly complex” mantra to get out of all liability ??
  - It is utterly shocking to see that we are willing to put ``critical infrastructure” at risk, in pursuit of cheap off-the-shelf solutions.
  - It should be feasible to build “provably secure” systems from the hardware up …… we must insist on it (otherwise it may never happen)

Our conclusions/recommendations

- Strongly urge NIST: Don't squander the small, precious b/w of power grid by falling for the headlong rush to connect the Power Grid to the Internet.
- In fact, to the contrary, maintain the strongest possible separation between the Grid and the Internet

- A judicious use of the b/w of electric conductors can substantially enhance the security of electronic communications at large, making the world a safer, better place

Epilogue: why do we need Smart Grid?

- Reasons given for the need of a smart-grid include:
  - Demand sensitive pricing which drives efficiency up …
  - more user control in a real-time power market
  - Introduce competition (just because …..?)
- above reasons are tenuous at best & fall apart under genuine scientific scrutiny:

  A utility engineer recently said: “Suppose everybody buys electric cars that need charging every day (or night). Even if the charging were to be done in a manner that completely avoids fluctuations in power demand; there is not enough capacity to deliver that much energy/day to all houses”

Climbing the wrong tree???

- Utility Engineer's recent comment continued :
  - "The capacity (# of conductors?) would need to be at least doubled. We are ignoring this infrastructure problem at our own peril… focusing instead on trendy catch-phrases like ``market mechanisms''; which in reality might not make sense when applied to the generation and distribution of electricity …"

Is there a **real fundamental/physical** reason?

- **YES !!**
  - For long term survivability…. In the long run; must live on solar(light)/wind/tidal = **sustainable** forms of energy
  - these sources are inherently distributed in nature.
  - To efficiently harness these resources, the electric grid must be bi-directional , today's grid is designed to push power only one-way: from a central generator to users
  - also need to predict demand => sensing local conditions

Interested in commercialization

- publications
- **US Patent app filed in May 2010**
- **First patent issued in January 2014**
- **Several more patents to follow…**
- **a free ride on the "Smart Grid" initiative**
- Looking for partner(s) to build & market