David Tuttle

Research Fellow
The University of Texas at Austin

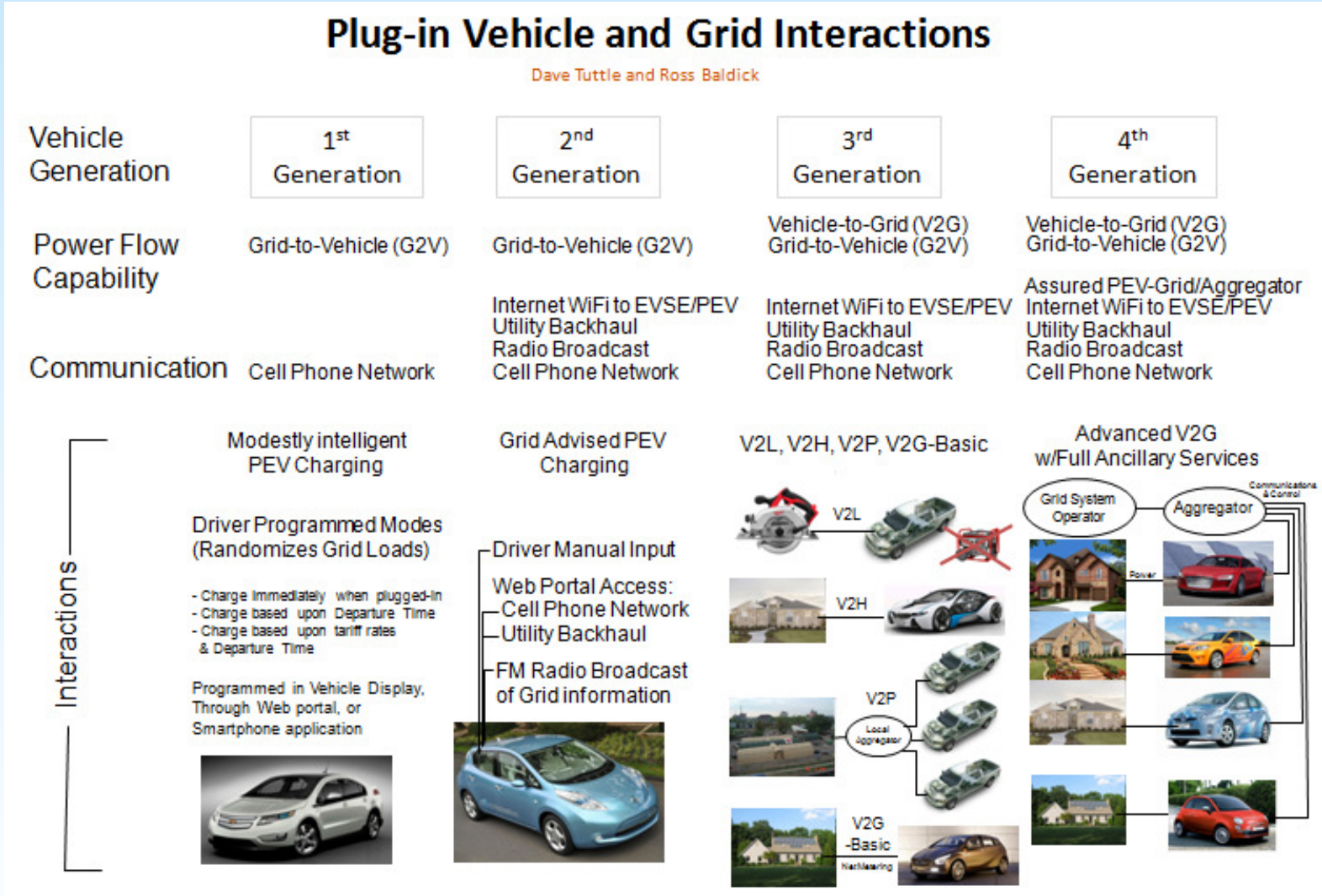
Home Energy Management Systems (HEMS), Home Area Network (HAN), and Plug-In Electric Vehicles (PEV) (updated)

March 27-29, 2012 – Irving, TX

HEMs, HANs & PEVs

- **Different levels of PEV-Grid interactions expose various levels of grid-security risk**
- **Different types of PEVs affect levels of grid-security risk**
- **Security risks on vehicles**
- **The Vehicles**
- **Grid-PEV communication platforms**
- **HEMS/HANs platforms**
- **Security Attacks**
- **Summary**

Security Risks Increase with Greater Sophistication of Grid-PEV Interactions



Type of PEV Affects Charging Behavior & Location

	BEV (Battery Electric Vehicle)	PHEV (Plug-In Hybrid Electric Vehicle)	
		eREV (Series PHEV) With Conventional Range	Parallel PHEV
			
Battery Size	Very Large (24-53kWh)	Large (~16kWh)	Medium (4-12kWh)
Range - Electric+Petrol	Electric only: ~100-250 miles	All Electric for 35 miles then 344 Miles on Petrol (=/> Conventional vehicle)	Electric for 15 miles below 62mph & light acceleration "Blended mode" (=/> Conventional Vehicle)
Charging - Home - Work/Public	Home: Level-2 240V typically needed Work/Public charging needed if distance is beyond range	Home: Standard Wall Outlet sufficient but Level-2 240V can increase electrically driven miles Work/Public charging not necessary but useful	
No Home Charging Available?	Either charge at work/public or not a viable vehicle for this driver	Either charge at work/public or use as a conventional hybrid vehicle	
Key Advantages	No internal combustion engine - Very low maintenance - No tailpipe emissions	No range limitation Operates as BEV, then Hybrid	No range limitation Smallest battery fastest charge

Charging Location Affects Security Risks

BEVs trying to extend range

BEVs using DC Fast Charging

PEV "street parkers" (in the outyears)

Roaming PEVs (mostly BEVs)

BEVs, eREVs/PHEVs (Drivers with Homes)

- Primary charging location for PEVs
- The strength of PEV refueling paradigm
- Many EVSEs may be non-networked

Vehicle Security

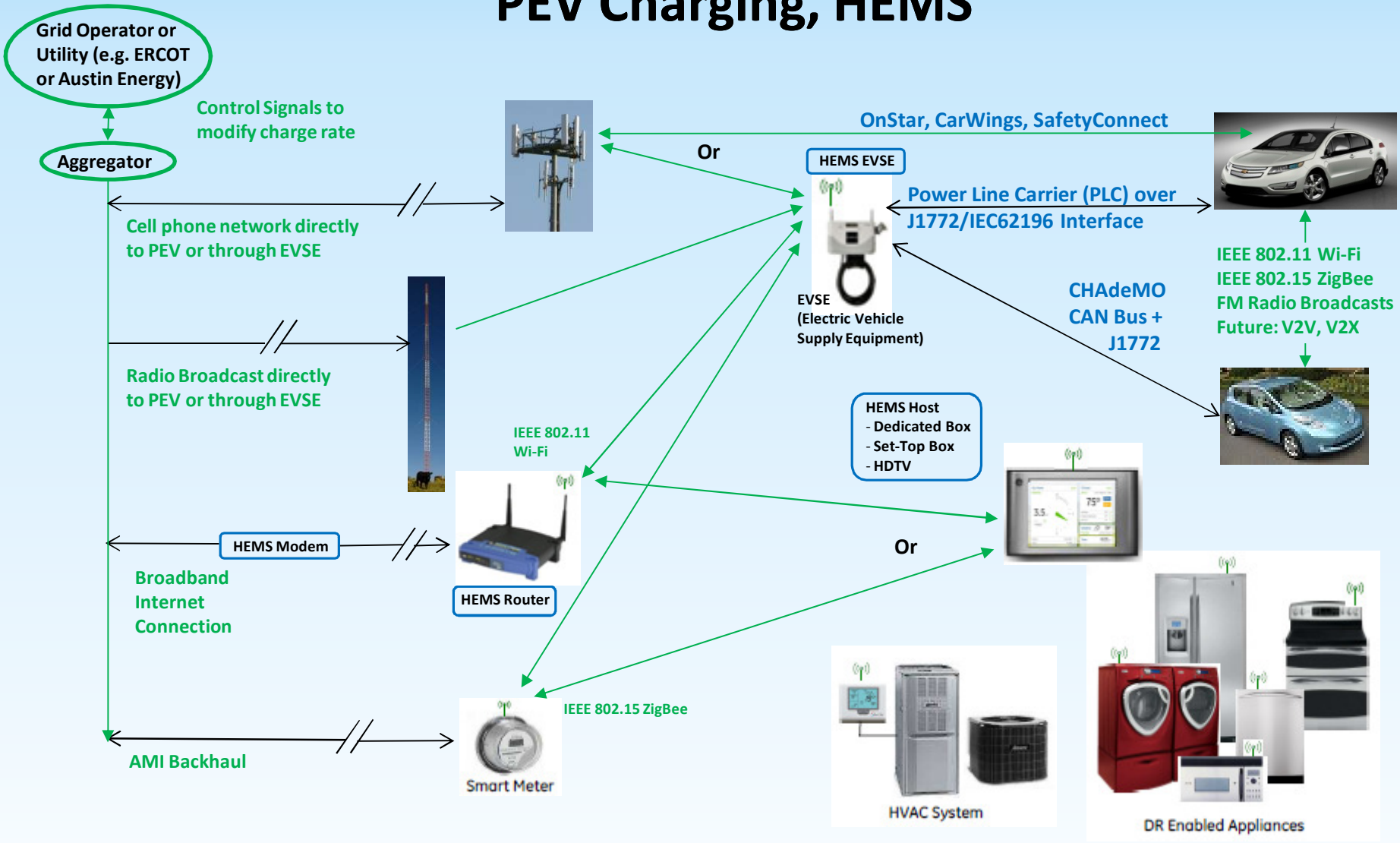
- **Today's conventional vehicles (and PEVs) have multiple communication pathways**
  - OBDII DLC (On-Board Diagnostics Gen 2 Diagnostic Link Connector)
  - Integrated Vehicle Communications: Onstar/CarWings/Safety Connect..etc
  - Aftermarket devices such as PayTeck
  - J1772/CHAdeMO: Plug-In Vehicle charging standard (the only PEV unique pathway)
- **Only one of these pathways is new for PEVs: J1772/CHAdeMO**
  - J1772 does not support general communications between EVSE-PEV at this time
    - Eventually will have PLC on Control Pilot signal
    - Control Pilot signal is private between EVSE & PEV,
      - EVSE may or may not be networked (not needed at residence)
  - CHAdeMO has CAN (Controller Area Network) interface
- **Today's conventional vehicle onboard communications focus: reliability & cost**
  - Security architecture & implementations are weak from some investigations, but…
  - Access is through under-dash OBDII DLC
    - Perpetrator must have access to interior of vehicle
    - Control of only that vehicle
  - Weak security architecture(s) & implementations
    - No authentication, broadcast nature, hardcoded challenge & response

- **PayTeck: disgruntled former employee, 100 cars impacted in Austin, TX**
- **Integrated Vehicle Communications: over Verizon/AT&T, as good as their systems & security**

Summary: PEVs

- **Most PEV charging will likely be at home at night, not public/workplace**
- **If charging is controlled (vs. immediate) in-vehicle programming or w/Vehicle Mfg portal**
- **When "grid advised" charging becomes available, there will be 2 likely pathways:**
  - Integrated cell phone communications (e.g. OnStar, CarWings, Safety Connect..)
  - EVSE to PEV: on J1772 charging cord using PLC (Power Line Carrier) or CHAdeMO using CAN bus
- **Of the 4 pathways, only 1 is new for PEVs:**
  - Control Pilot for J1772, CAN for CHAdeMO
- **Perpetrators can acquire a vehicle & experiment in the comfort of their own lab**
  - Objectives: Ex-filtration of IP, mass panic
- **Vehicles electronics architectures & implementation focus is reliability & cost**
  - Today's conventional vehicles already have a number of latent security exposures, but not consequential to date
  - Koscher, K., et al 2010. Experimental Security Analysis of a Modern Automobile. IEEE Computer Society, http://www.autosec.org/pubs/cars-oakland2010.pdf
  - Checkoway, S., et al, 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. Presented at 20th Advanced Computing Systems Association Conference, http://www.autosec.org/publications.html.

Communication Pathways to Control PEV Charging, HEMS



HEMS,HANs, & Hardware Platform

- **Utilities' concerns: costs & security of large amounts of customer data**
  - Will Utilities actually want to have fine grain DR control beyond the meter inside the home?
  - Simply request amount, percent, duration of DR, receive acknowledgement, confirm
  - Will many utility AMI backhauls have the bandwidth to support DR traffic (vs. meter reading)?
- **HEMS: Application on a variety of hardware platforms to manage customer's devices**
  - Trusted device within home or 3rd party contracted cloud application
  - Within Home: dedicated embedded app, iOS/Android or Linux API app
- **HANs (on customer side of AMI Meter)**
  - SEP2.0, over 802.11 Wi-Fi, 802.15 ZigBee, PLC
- **Hardware platform(s)**
  - Dedicated Box
  - HDTV
  - iHEMS/AppleTV
  - Set-top box
  - Router
  - Plug-In Electric Vehicle's Level-2 EVSE charging station

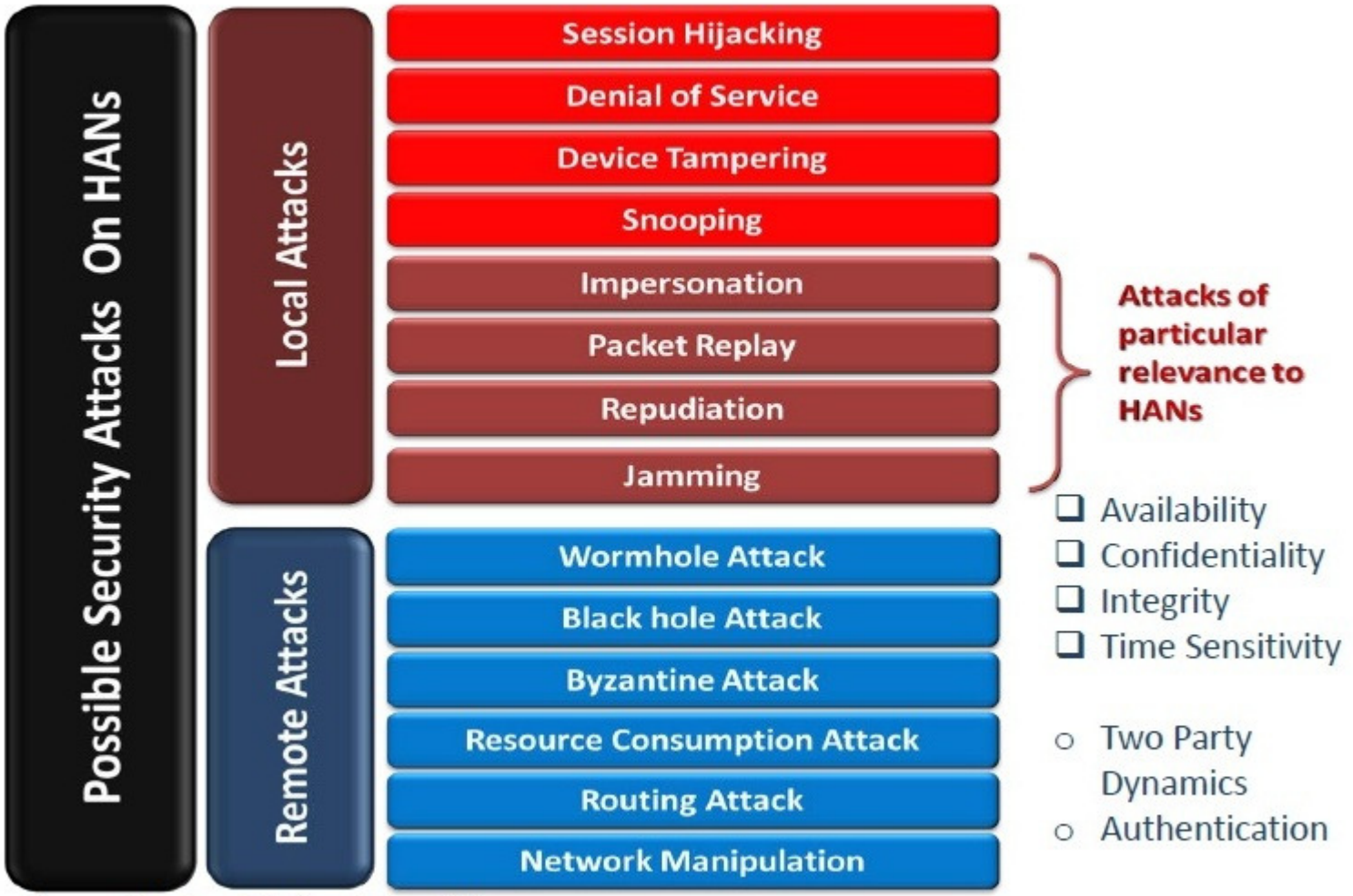
HEMs, HANs & Platforms

- **Utilities less likely to want to control individual devices on customer side of meter**
  - Send request for amount of DR to customer premise HEMS, HEMS acknowledges and confirms
  - Avoids or reduces privacy, communications bandwidth, data management, back office sw, cost concerns
  - AMI backhaul used only for meter reading and DR requests/acknowledgements/confirmations

- **HANs (on customer side of the AMI meter)**
  - Security can track the Wi-Fi, ZigBee, or PLC technologies leveraged
  - Broad intrusion less likely than local intrusions : unclear risk to grid

- **HEMS Likely either dedicated HEMS box or an App on a variety of hardware platforms**
  - iHEMS/AppleHEMS, HEMS app on Android HDTV API
  - Security Risks: exposure of private data on NAS/PC disks or DoS attack

Security Threats to AMI



Source: Namboodiri, Jewell, Aravinthan

Summary

- **The greater the SmartGrid acceptance , the greater the exposure**
  - Electricity use is easy, computing is valuable but too often (very) frustrating
  - How often will customers want to take a simple part of their life and make it PC complex?
    - When meaningful cost, convenience, security, environmental benefits w/o implementation hassles (hence iHEMS)
  - DR likely to focus on big loads like PEVs, HVACs, pool pumps
    - Security through non-access on DLC & defenses of vehicle integrated communications pathways in today's conventional vehicles
      - PEVs will have one additional pathway within 3-5 years
  - Smart Appliances: value from maintenance/service/repair notifications (less from DR)

- **Security threats:**
  - Types & quantity of access points will vary: Low (similar to today's vehicles).. to extreme
  - Will also follow the technologies leveraged (e.g: Wi-Fi, ZigBee)
  - Likely sources: financially motivated, state-sponsored attacks on grid, terrorists bent on creating economic damage or panic, specific targets
  - May have more broad exposure when dominant apps/platforms emerge