EV Charging System Standards and Security

Craig Rodine
Member, IEC TC69 and USTAG
Director, Standards – ChargePoint, Inc.

SANS Automotive Cybersecurity Workshop, Chicago, IL
May 8, 2018
Outline

+ Brief survey of the EV charging landscape
+ Ex1: A reasonably secure, operational network
+ Ex2: Recent observations (how not to do it)
+ The quest for security in standards
Survey of EV charging

EV charging *ballpark* metrics

+ Plug-in vehicles* worldwide: ~3 million
  - 765,000+ in US and Canada
  - 1.2+ million registered in 2017
+ Public charging stations (NA): ~35,000
  - Vast majority “L2” = 6-7 kW AC
  - ~8-10% “DC Fast” (L3) = 25-50 kW DC
  - Significant proportion (~80%) on <5 networks
+ Public charging stations (RoW excluding China): ~100,000
  - Approx 25% DC Fast (CCS, CHAdeMO, GBT)
  - Significant proportion (50-70%?) *not* networked
+ Total number of EV charging networks worldwide?
  - ~100; largest few each manage 20,000-40,000 stations

* Global BEV (~67%) and PHEV (~33%) passenger cars, plus light trucks in USA & Canada, and light commercial vehicles in Europe (EVvolumes.com)
Survey of EV charging

Some industry data …

- Monthly Plug-in Vehicle Sales
  - Global
  - 2015, 2016, 2017

- Global Monthly PEV Shares

- Plug-in Sales and % Growth
  - China: +72%
  - Japan: +149%
  - Europe: +38%
  - USA: +27%
  - Other: +126%

© 2018 ChargePoint, Inc.

Rodine SANS Auto Cybersec Workshop
Types of networked stations

+ Public access
  • Broad classification: long-dwell/rapid charge; public/private
  • Application: commercial, municipal, workplace, fleet, highway

+ Workplace
  • Increasing demand (employee benefit, environmental mission)
  • Can be high volume (example: >1,000 stations, many sites)

+ Residential
  • Single and multi-family
    – Most not [yet] networked
    – Utilities may require connectivity

+ Fleet
  • Taxis, busses, trucks (delivery), work vehicles (e.g. ports, utilities, military)
Survey of EV charging

Communication and control standards

EV charging protocols
PWM (SAE/IEC), DIN 70121:2014, ChaDeMo, ISO/IEC 15118, GB/T

Charging Network Management Protocol
(IEC 63110, OCPP, etc.)

Inter-Network Roaming Protocols
(IEC 63119, NEMA 1.2, OCPI, etc.)

The Cloud (Internet)

Product and safety standards
SAE J1772™, IEC 61851-1/-21/-23,
IEC 62196, NEC 70-625, NIST HB44/130,
UL 2202, 2231, 2594

© 2018 ChargePoint, Inc.
Rodine SANS Auto Cybersec Workshop
A secure charging network

A distributed, partitioned network

Customer #1 = Site owner

Customer Admin portal (monitor & manage)

E.g., set pricing policy

proprietary protocol

‘dumb’ (analog) charging control

Customer #2 = EV driver

© 2018 ChargePoint, Inc.
A secure charging network

Security domains

Customer Admin portal (monitor & manage)

Site owner

EV driver

cloud-mobile

E.g., set pricing policy

client-server

intra-cloud

inter-cloud

IEC 63119 (roaming)

IEC 63110

IEC/ISO 15118

IEC 63110

NEMA EVSE 1.2 / new TC69 RFID standard

AC: ‘dumb’ (analog)

DC: DIN (untrustworthy)

© 2018 ChargePoint, Inc.
A secure charging network

POS/AAA with open secure RFID

+ Includes higher-security RFID access
+ Built on trusted ISO standards
  - Open standard: NEMA EVSE 1.2
  - Granular, strong challenge-response
  - Identifies each transaction (swipe)
  - “Leading edge” of end-to-end AAA
+ Engineered for cost-benefit balance
  - Within a broad range of possible solutions
+ Also accepts contactless credit cards
  - Banks, CCs moved to chip&pin, chip&sign
+ Could also support NFC payment
  - Apple Pay, Google Wallet, Samsung Pay

PCI-DSS Certified
Enables familiar behavior and viable business

+ Helps EV drivers get “on board”
  - Resembles other transactions
+ Supports site owner business
  - Enables revenue collection
    - Removes a barrier to adoption
  - Enables flexible pricing
  - Establishes solid trust
+ Supports inter-network roaming
  - Addresses regulatory requirements
  - Helps build a strong ecosystem
Verification and validation

+ PCI DSS 3.2 Certification
  - Comprehensive formal requirements
    - Technical and process
    - Software, hardware, communications, physical integrity, data storage, ...
  - Based in banking industry/community
    - High exact volume, stringent req’ts
    - Regular formal audits (minor versions)
    - Continuous testing and improvements
+ System also verified by a major utility
  - Cyber-physical security requirements
  - Third-party penetration testing
+ Deployed by USGovt (intel, military)
  - Workplace and fleet applications
NEMA EVSE-1.2 Secure RFID standard
General design goals and features

+ Provide a state-of-the-art secure RFID standard for EV charging
+ Agnostic as to EV charging network protocol and business model
  - Supports subscription-based (pre- or post-paid), aggregated term-based, tiered and discounted usage rate plans; pay-per-use, anonymous (e.g. gift card) or attributed (account-based) transactions, etc.
+ Focuses on authentication, doesn’t constrain authorization logic
+ Provides fine-grain accounting of authentication transactions
+ Agnostic as to peer-to-peer or clearinghouse-based roaming models
NEMA EVSE-1.2 Secure RFID standard
High-level description and experience to date

+ An EV-charging-domain-specific application protocol built on widely implemented, strongly proven RFID standards
  - ISO 14443-2/3/4 and ISO 7816-4/5/8
  - These ISO standards are used worldwide for access control
    - In corporations and high-security government agencies
    - In the passports of more than 85 countries
+ Can be implemented in smartcards, tags, and smartphones
+ Now deployed in tens of thousands of tags and charging stations (NA)
+ Has secured tens of millions of charging sessions without known breach
+ Is designed specifically to support e-mobility
  - EV charging roaming aka “network interoperability”
NEMA EVSE-1.2 Secure RFID standard

Technical design goals and features

+ Robust against credential compromise
  - ISO 14443 designed to make cloning and penetration very difficult
  - Counters brute-force, microscopy, power analysis, other types of attack

+ Robust against man-in-the-middle and replay attacks
  - Encodes time and location of each authentication attempt (card swipe)
  - Provides sufficient data to tie authentication to overall transaction
  - Credential can include transaction counter (must sustain >10K x)

+ Allows issuer a choice of cryptographic algorithms and materials
  - To meet security requirements and address cost/implementation tradeoffs
    - To be cost-effective, credentials should use commercial off-the-shelf devices
  - Symmetric and asymmetric cryptosystems are supported

+ High security without exposing secrets to visited networks
  - Strikes a balance between cooperation and competition among EMSPs
  - Isolates compromises to a single network, they don’t propagate
Non-secure EC charging networks

+ Report in December, 2017 showed flaws in implementation
  • From a neutral research institute, presentation at 34C3
  • RFID UID (= account ID) in the clear, no challenge – easily stolen
  • Cloud-station communication not encrypted, easily intercepted
  • ‘De facto’ standard control protocol published, available to all
    – Includes ‘reboot station’ and ‘download new firmware’ functions
    – Demo showed a charging station quickly and thoroughly pwned

+ Described many (most) public charging networks in Europe

+ Screaming out for remedies (article in Der Spiegel)
  • Puts emerging IEC TC69 work in the spotlight …
Is all publicity good publicity?
A brief look at IEC TC69 efforts

- Address levels above charging station
  - IEC 63110: could-station standard
    - To enable multi-vendor networks
    - Strong emphasis on energy mgmt
    - Concerned with site-level integration
      - This is new, leaning towards IoT
  - IEC 63119: cloud-cloud standard
    - To support internetwork roaming
    - Peer-peer or clearinghouse
- Each includes a security TF or focus
  - Analysis and requirements
  - But no coordinated end-to-end analysis
- Proposal: form TC-level System Security WG
### Security in emerging IEC standards (TC69)

#### Draft IEC 63110

**IEC 63110: Management of Electric Vehicles charging and discharging infrastructures**

**General communication interfaces architecture**

- **EVSE-1**
  - **Other interface**
  - **Safety - C&C**
  - **CC & MO**
- **EVSE controller**
- **Loads & sources interfaces**
- **Meter interfaces**
- **DSO, FO, EP Management systems**
- **CSMS**
- **EMS CC interfaces**
- **EMS CC interfaces**
- **?**

**Principle of the diagram:** Two Communication Controllers talk together through Communication Interfaces (last update 07/21/2017)

---

#### + Discrete JWG11 Security Task Force
- **Goals, participation, and process are well defined**
- Based on ISO/IEC 27005 (2011, new edition under development)
  - References ISO/IEC 27001, 27002
- Initial step: risk analysis

#### + Upstream and downstream requirements being discovered
- Federation of security domains?
- Management of crypto materials?
- Data at rest? in device and cloud?

#### + Includes a local “CSMS” entity and communications interface
- For site-based load management
- The first “sideways” requirements
Security in emerging IEC standards (TC69)

Draft IEC 63119

- Well started with system architecture (Part 1)
  - Architecture and framework of multiple parts
  - Use cases, requirements (messages), conformance
- 63110-1 now going to CDV
- Reviewing existing roaming schemes
  - Available specs: NEMA, OCHP, OCPI, ...
- Cybersecurity treatment (in Part 2)
  - NP submitted, approval expected Summer 2018
- Anticipated cybersecurity framework:
  - Extensible “plug-in” authentication (I5)
    - allowing RFID, secure QR codes, NFC, etc.
  - Cloud-cloud (I3) requirements and standards
    - Need to choose best fit among candidates
  - Mobile-cloud (I6) requirements and standards
    - Need to choose best fit among candidates
ETH-IP* (PEV-EVSE) interface introduces a new, potentially nasty EVSE attack surface

Admin uses tool to create pricing policy

Pricing policy is stored in CPI NOS, sent to designated stations

Proxy SA

Open protocol, e.g. IEC 63110

IEEE P2030.5 or ISO 15118

Will the EV become a programmable, negotiating actor?

* ETH-IP = Ethernet/Internet Protocol

© 2018 ChargePoint, Inc.
New functionality in IEC/ISO 15118 Ed2

Note: IEEE P2030.5 enables/envisions similar features

+ Wireless Power Transfer
  • Including Wi-Fi communications
  • For ‘supporting services’ and charging control – all modes (!)

+ Expanded Energy Management functionality
  • Scheduled Mode and Dynamic Mode
  • Target-setting for optimization, support for Grid Codes

+ Bi-Directional Power Transfer
  • Including fast ‘open-loop’ charging control (e.g. for freq reg)
  • A novel energy source with its own requirements

+ Absolute pricing {$, €, ¥, £, ¥, ₩, ₱, …}
  • Required for legal metrology (public-access charging)
  • Brings pricing details ‘in-band’ per established practice (NA)
Missing: an independent, comprehensive, publicly available security analysis.

Missing: harmonization with SAE Trust Anchors and Authentication TF.
Thank You

For further information on this topic, please contact Craig Rodine:

craig.Rodine@chargepoint.com

+1.408.872-7515
System reference model

Figure 4-3
System Reference Model (with Integrated Authentication Device)
Domain-appropriate challenge-response

Figure 5-1
Challenge-Response Authentication Process

NEMA EVSE 1 Secure EVCN RFID standard
More details

NEMA EVSE 1 Secure EVCN RFID standard

Figure 5-2
Cryptogram Generation Process

Figure 5-3
Cryptogram Validation Process