ChargePrint: A Framework for Internet-Scale Discovery and Security Analysis of EV Charging Management Systems

Network and Distributed System Security Symposium (NDSS)

Tony Nasr[*], Sadegh Torabi[†], Elias Bou-Harb[‡], Claude Fachkha[§], Chadi Assi[*]

[*]Concordia University, Montreal, QC, Canada

[†]George Mason University, Fairfax, VA, USA

[‡]University of Texas at San Antonio, San Antonio, USA

[§]University of Dubai, UAE

Presented by:

SADEGH TORABI, Ph.D.

Assistant Professor & Cybersecurity Researcher

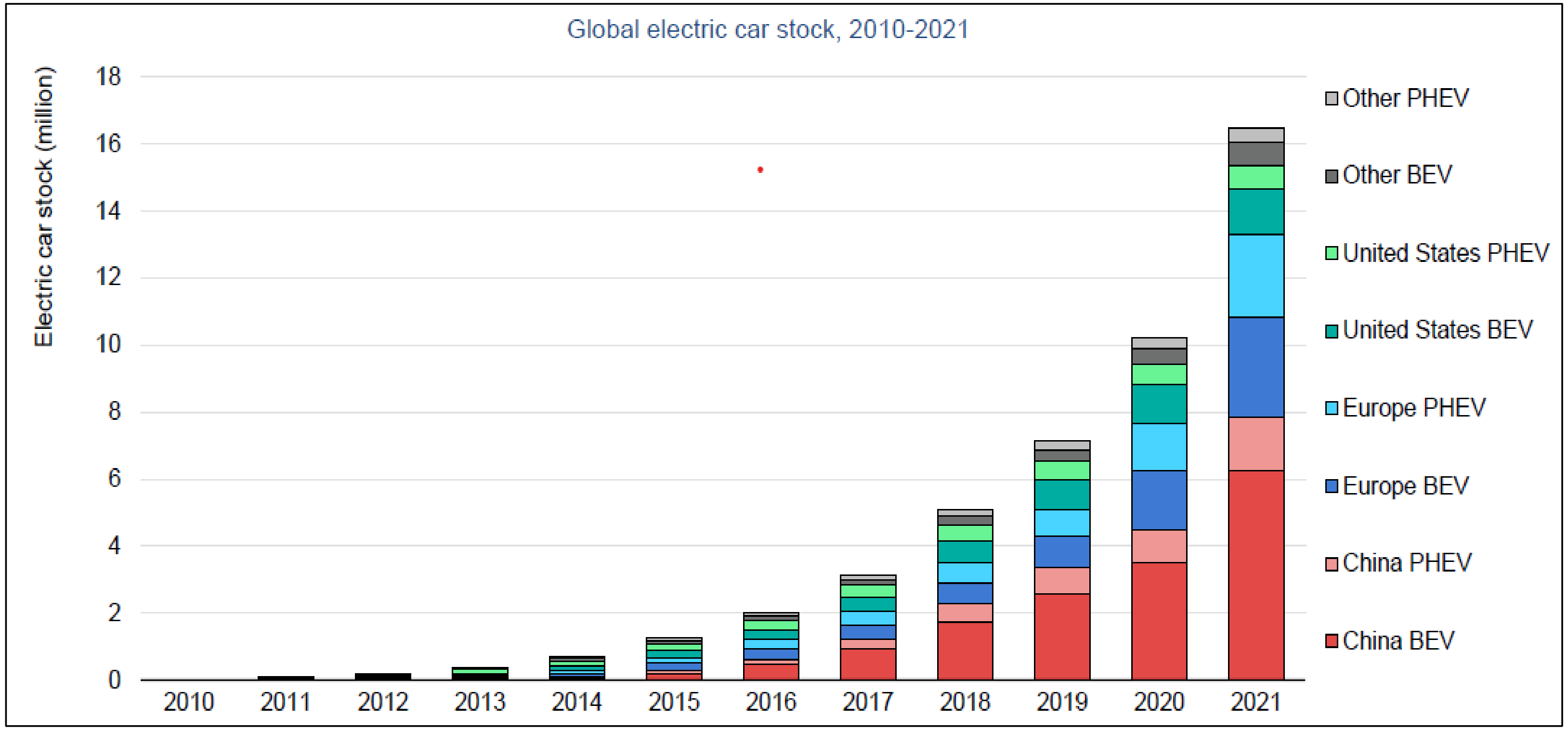
Center for Secure Information Systems (CSIS)

George Mason University, Fairfax, VA, USA

storabi@gmu.edu

Increasing Number of Electric Vehicles (EVs)

- By 2021, number of EVs tripled as compared to the previous 3 years (16.5 M)
- 10.3 M electric cars were sold worldwide in 2022
- 13.6 M EVs expected to be sold globally by the end of 2023
- The rapid adoption of EVs has led to increased charging demands



Expansion of the EV Charging Infrastructure

- Expanding the EV charging infrastructure to keep up with the demand
- The USDOT and USDOE investing $5 Billion to build 500,000 charging stations nationwide [1]
- Similar trends in Canada [1], Europe, and Asia

[1] https://highways.dot.gov/newsroom/president-biden-usdot-and-usdoe-announce-5-billion-over-five-years-national-ev-charging
[2] https://www.nrcan.gc.ca/energy-efficiency/transportation-alternative-fuels/zero-emission-vehicle-infrastructure-program/21876

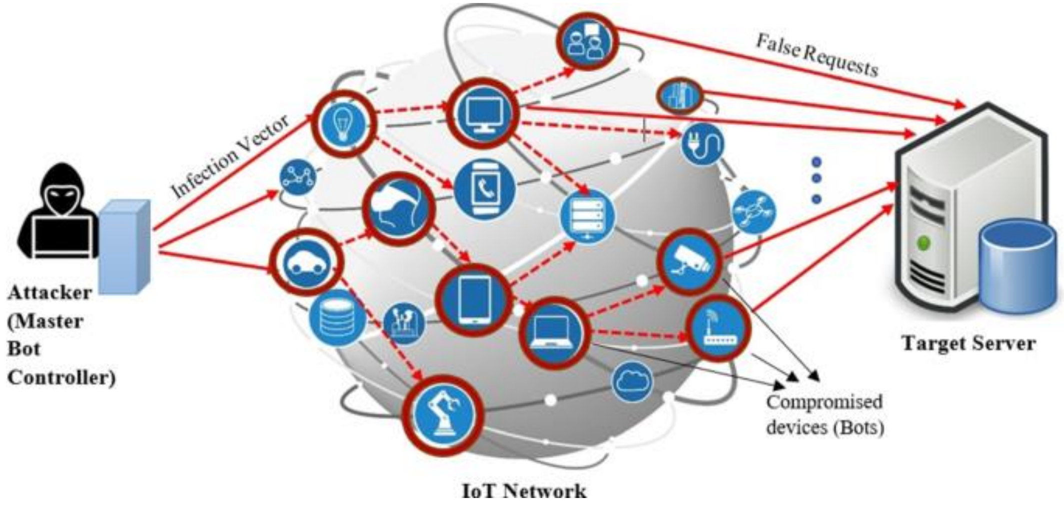
Problem

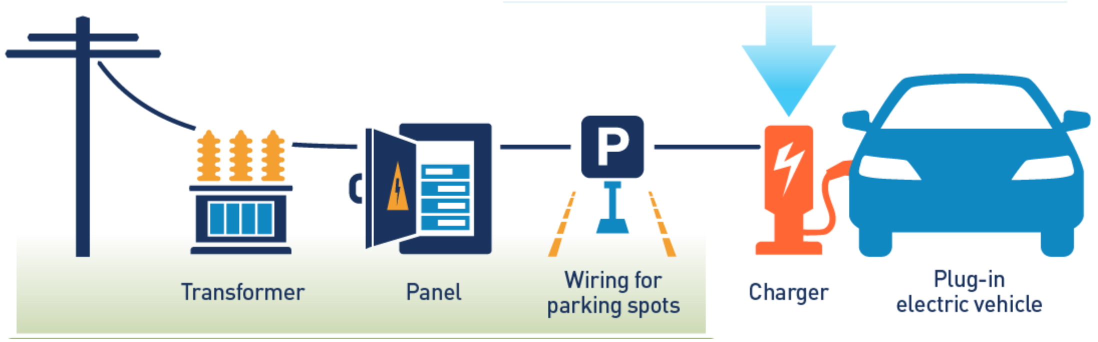
- The EV ecosystem is vulnerable to cyber attacks/exploitations
- Malware, default/weak credentials, vulnerable firmware/protocols
- Lack of knowledge about the security posture of existing EVCS against remote cyber attacks

Why should we be concerned?

- Protect the devices/services
- Compromised IoT/CPS as attack enablers
- Increasing number of insecure EVCS
  - more complex software/firmware, computationally powerful systems
  - connected to critical infrastructure
- Vulnerable EVCS as a new attack vector
  - EV users, operators, and the power grid

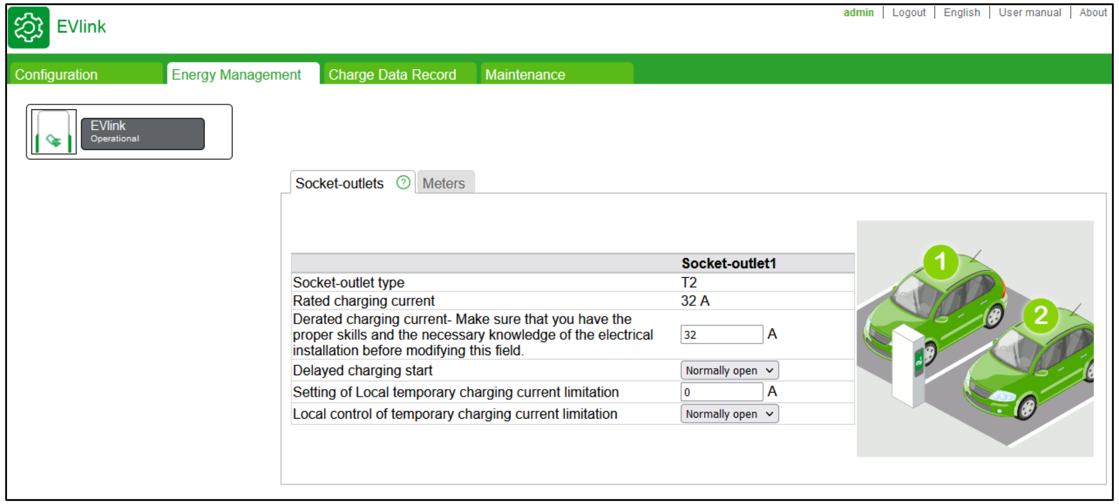
Distributed Scanning and DoS



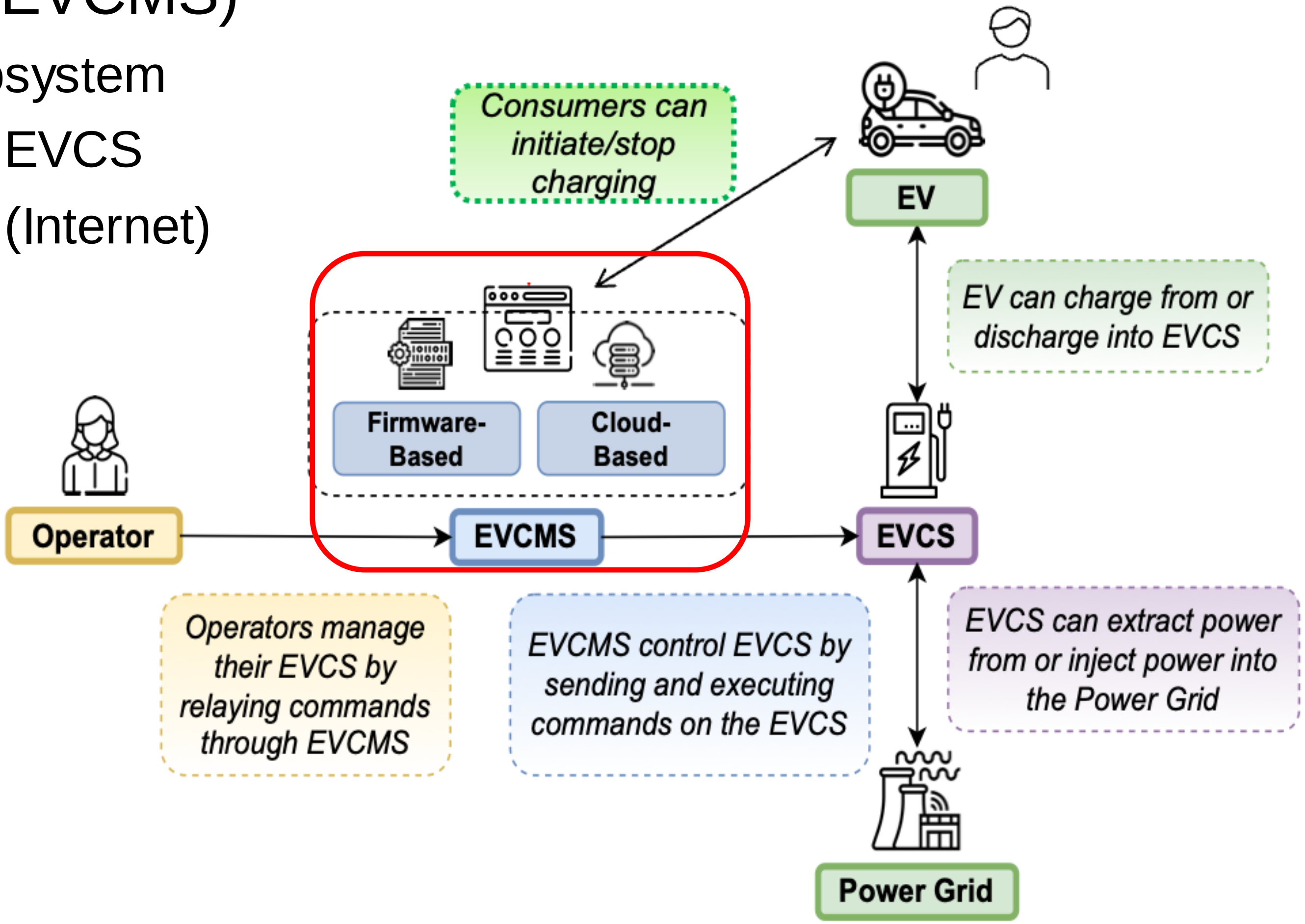


The EV Charging Ecosystem

- A CPS with various stakeholders
- EV charging management systems (EVCMS)
  - A core component in the EV charging ecosystem
  - Collection of software that instrument the EVCS
  - Remote control/management capabilities (Internet)

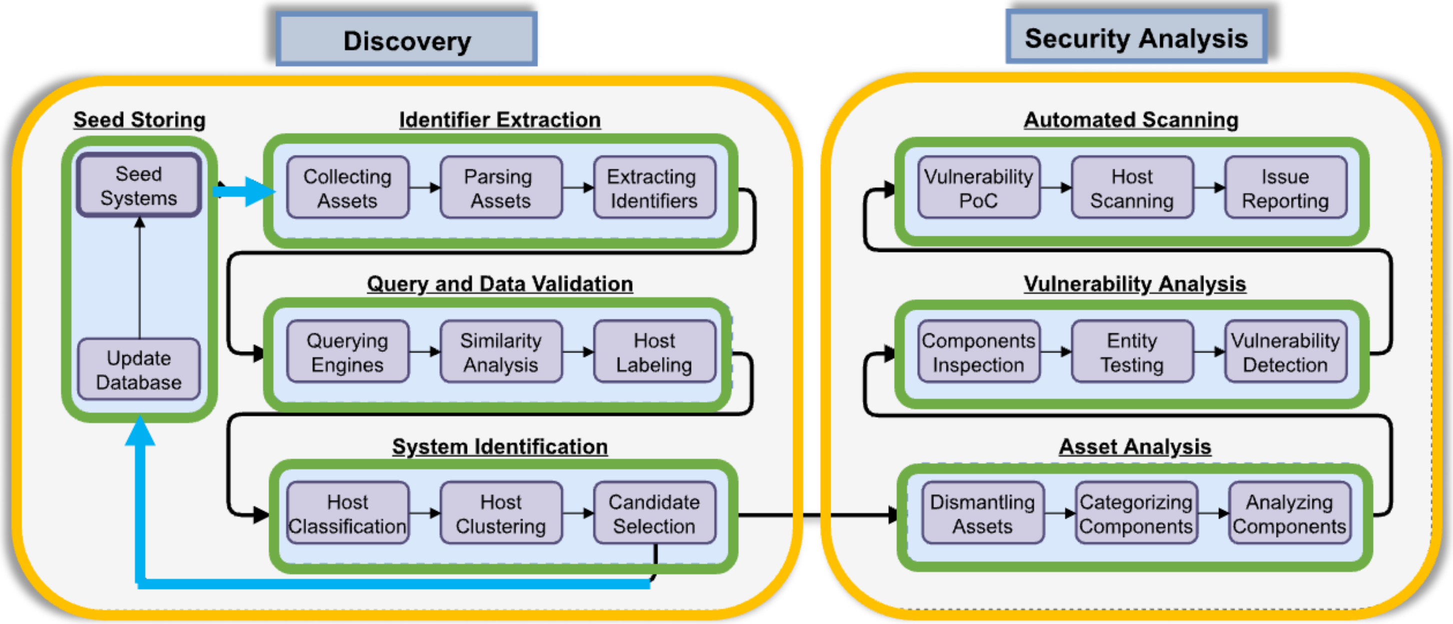


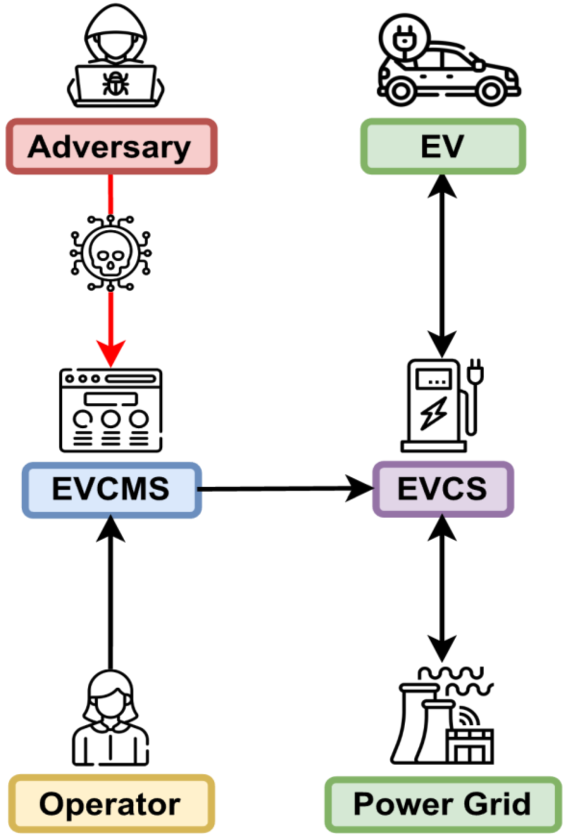
	Socket-outlet1
Socket-outlet type	T2
Rated charging current	32 A
Derated charging current- Make sure that you have the proper skills and the necessary knowledge of the electrical installation before modifying this field.	32 A
Delayed charging start	Normally open
Setting of Local temporary charging current limitation	0 A
Local control of temporary charging current limitation	Normally open



Threat Model

- An adversary wants to exploit vulnerabilities of EVCMS
  - Gains control over the EVCS and performs remote attacks against stakeholders
- Investigate the security posture of the deployed EVCMS in the wild
- Lack of empirical data about the deployed EVCS
- Approach: online EVCMS discovery and security analysis



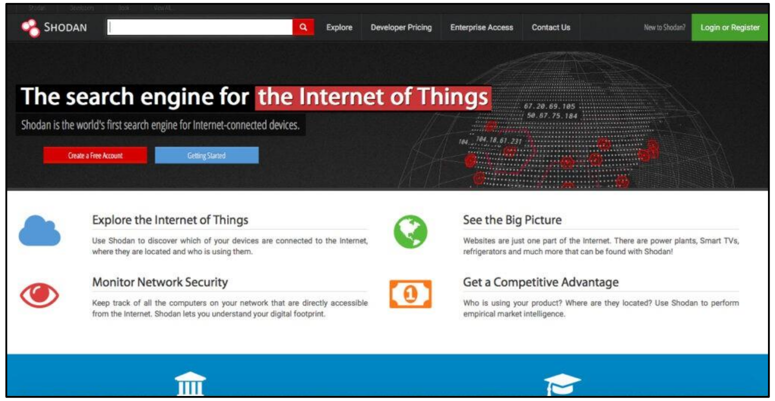


Device Discovery Using Online Device Search Engines

- Device search engines (e.g., Shodan.io)

- Mainly rely on banner analysis
  - limited banner information associated with EVCMS
  - lack of standardization in implementation of EVCMS
  - lack of EV-specific rules/tags/identifiers to use with search tools

- Limited number of discovered EVCS



Question:

How can we leverage existing search engines to extend the EVCMS discovery/fingerprinting results ?

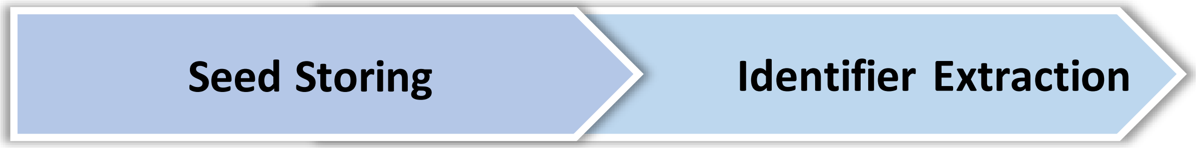
Proposed Approach: Iterative Device Discovery

Seed Storing

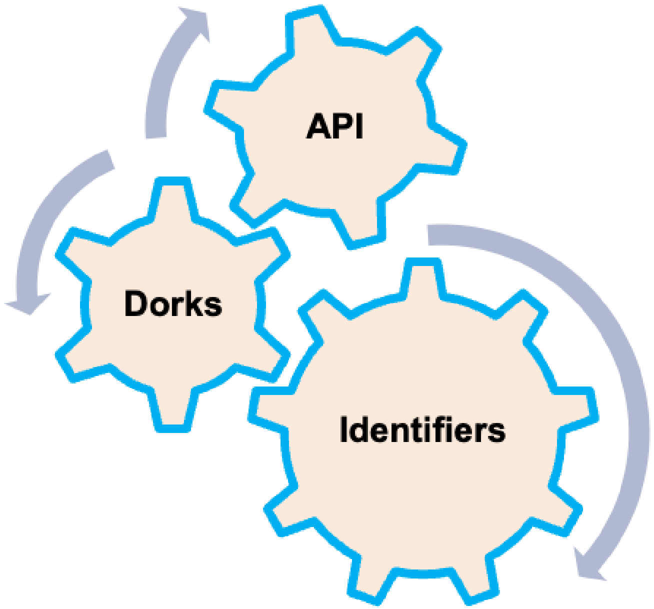
SHODAN ZoomEye censys FOFA

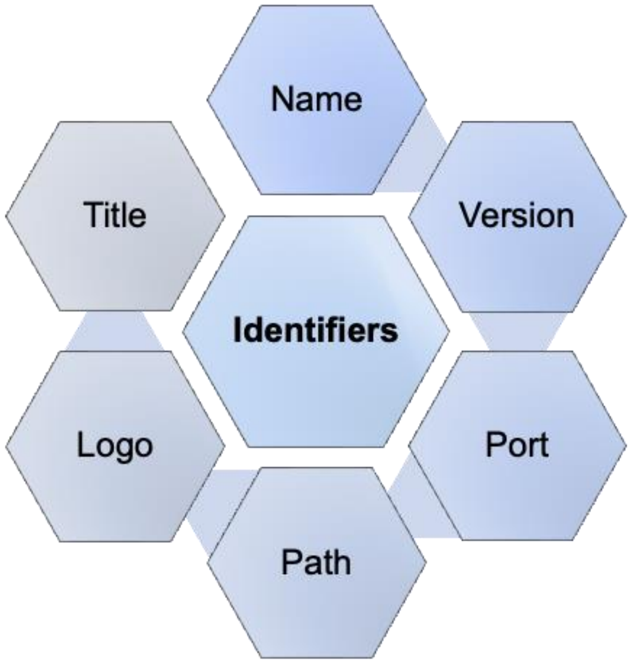
- Leverage 4 well-know device search engines (Shodan, Censys, Fofa, Zoomeye)
- Initial search and lookup using EV-related keywords
- Build a database of EVCMS seeds

Proposed Approach: Iterative Device Discovery



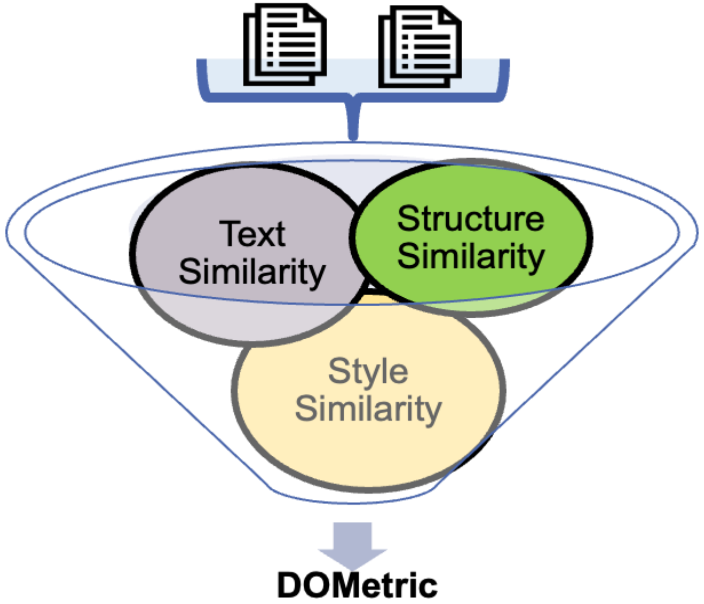
- Collect/parse assets from firmware, web instances, and vendor websites
- Extract identifiers from filesystem items, DOM elements, and EVCS-related strings





Proposed Approach: Iterative Device Discovery

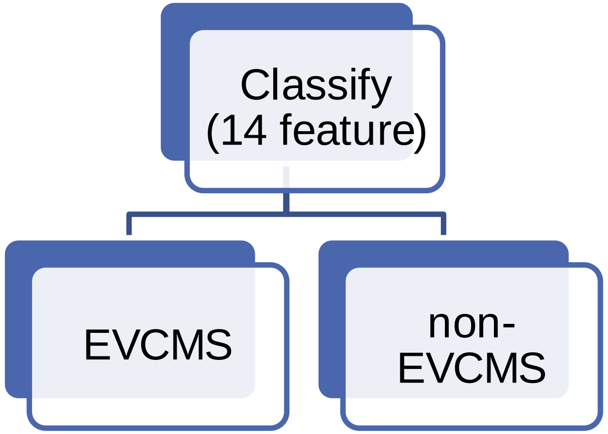
- Query the search engines using the new identifiers → new hosts
- Parsing the EVCMS portals' HTML page to extract their structure, style, and text content
- Introduce the DOMetric by calculating structure, text, and style similarities

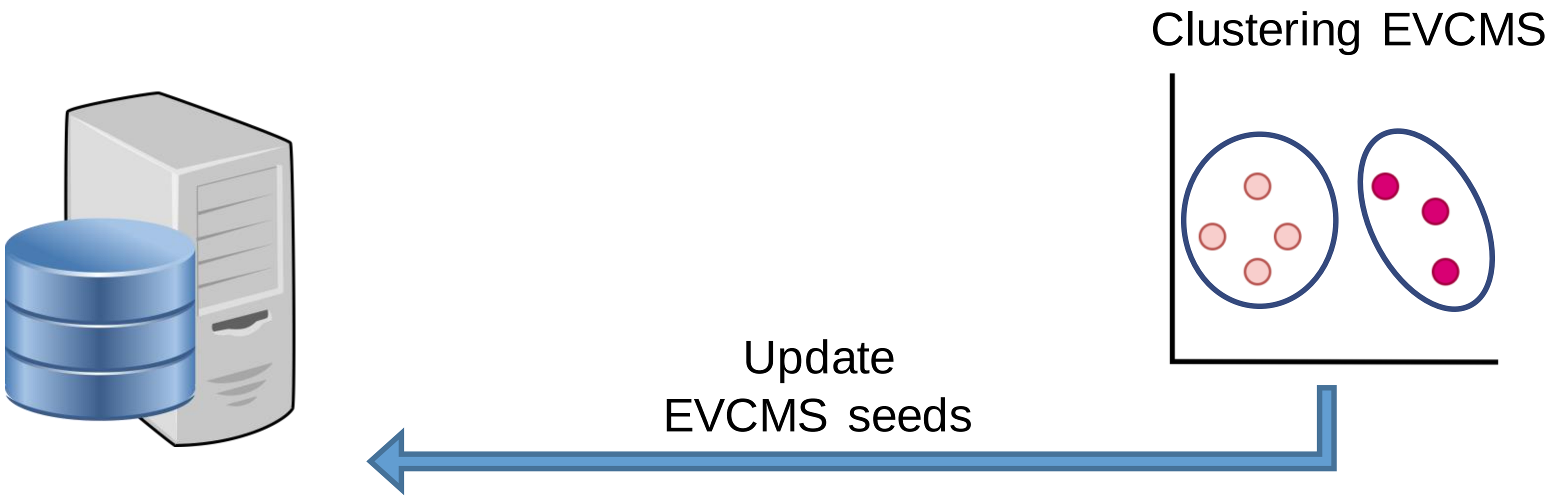


Proposed Approach: Iterative Device Discovery

Seed Storing → **Identifier Extraction** → **Query and Data Validation** → **System Identification**

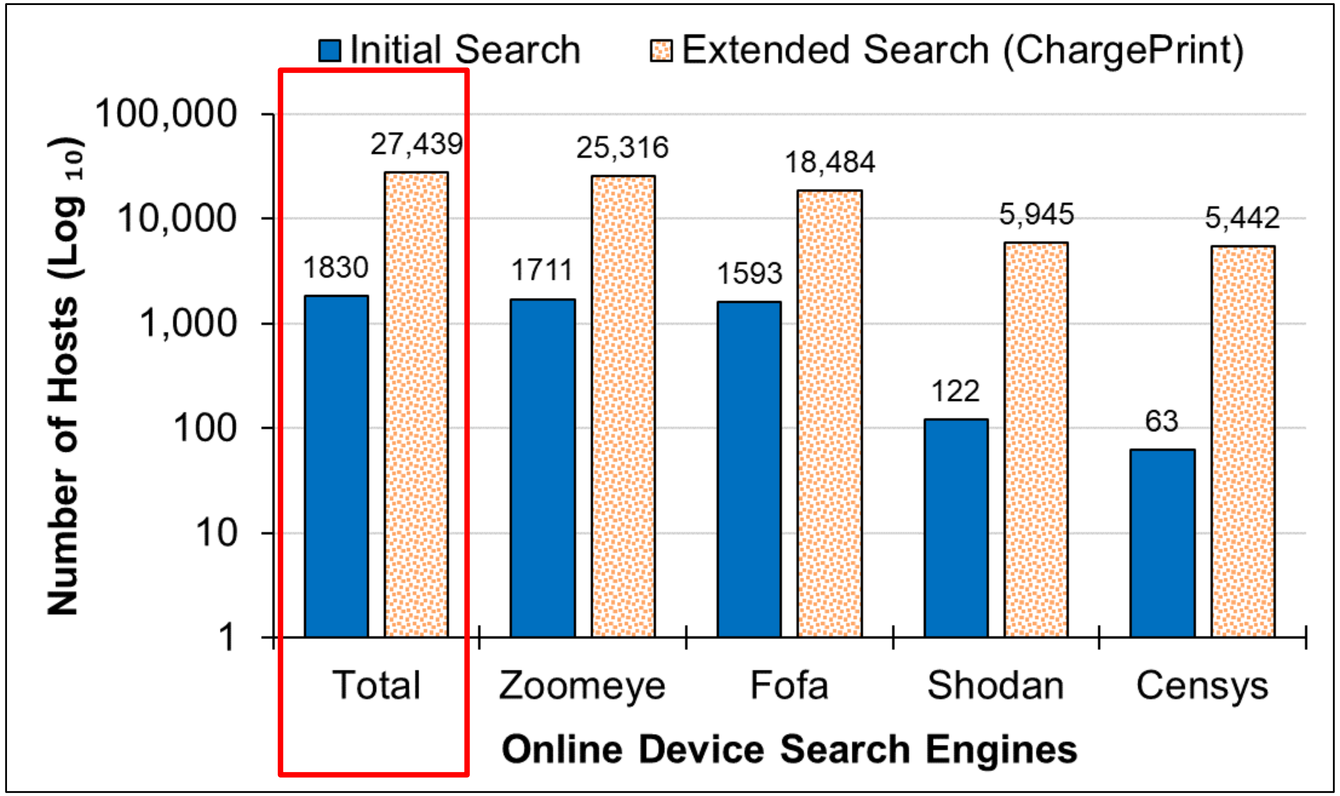
- Separate EVCMS hosts from generic hosts (Binary classifier with 14-EVCMS features)
- Cluster EVCMS hosts using DOMetric (threshold=0.9)
- Select candidate EVCMS (multiple version and more representative identifiers)





EVCSMS Discovery Results

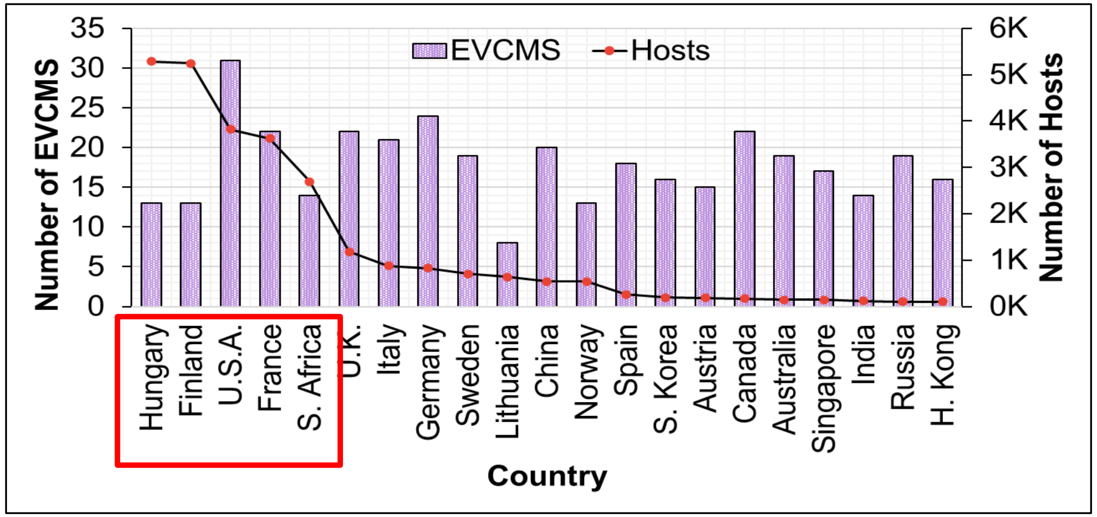
- Initial Search (1,800 EVCMS hosts, 9 products)
- Zoomeye & Fofa produced more hosts
- Extended Search (ChargePrint)

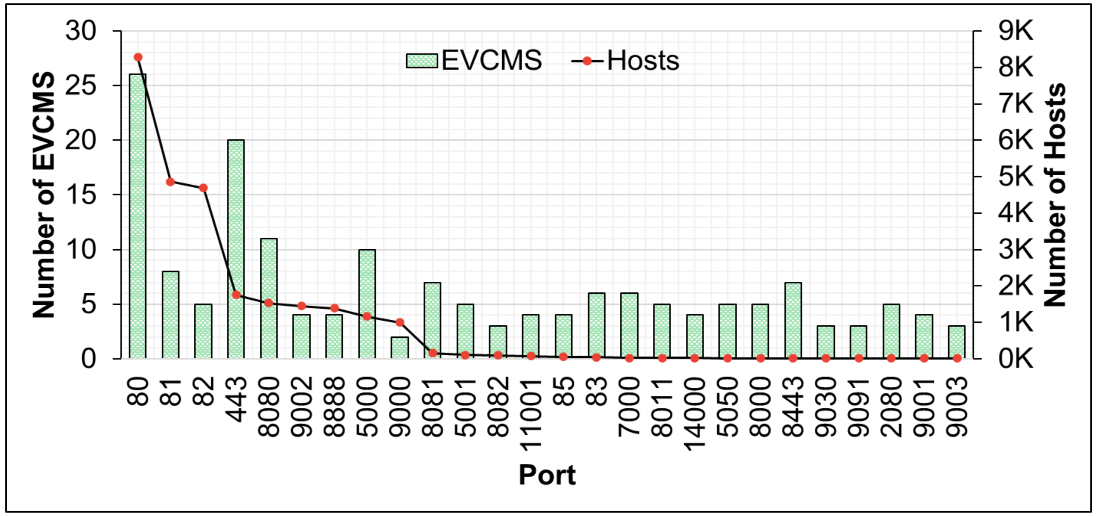


- Significantly improved results
  - Discovered 27,439 EVCMS hosts
  - 20x Zoomeye
  - 10x Fofa
  - 40x Shodan & Censys
- 44 EVCMS products (35 New)
  - initial seed of 9 EVCMS products

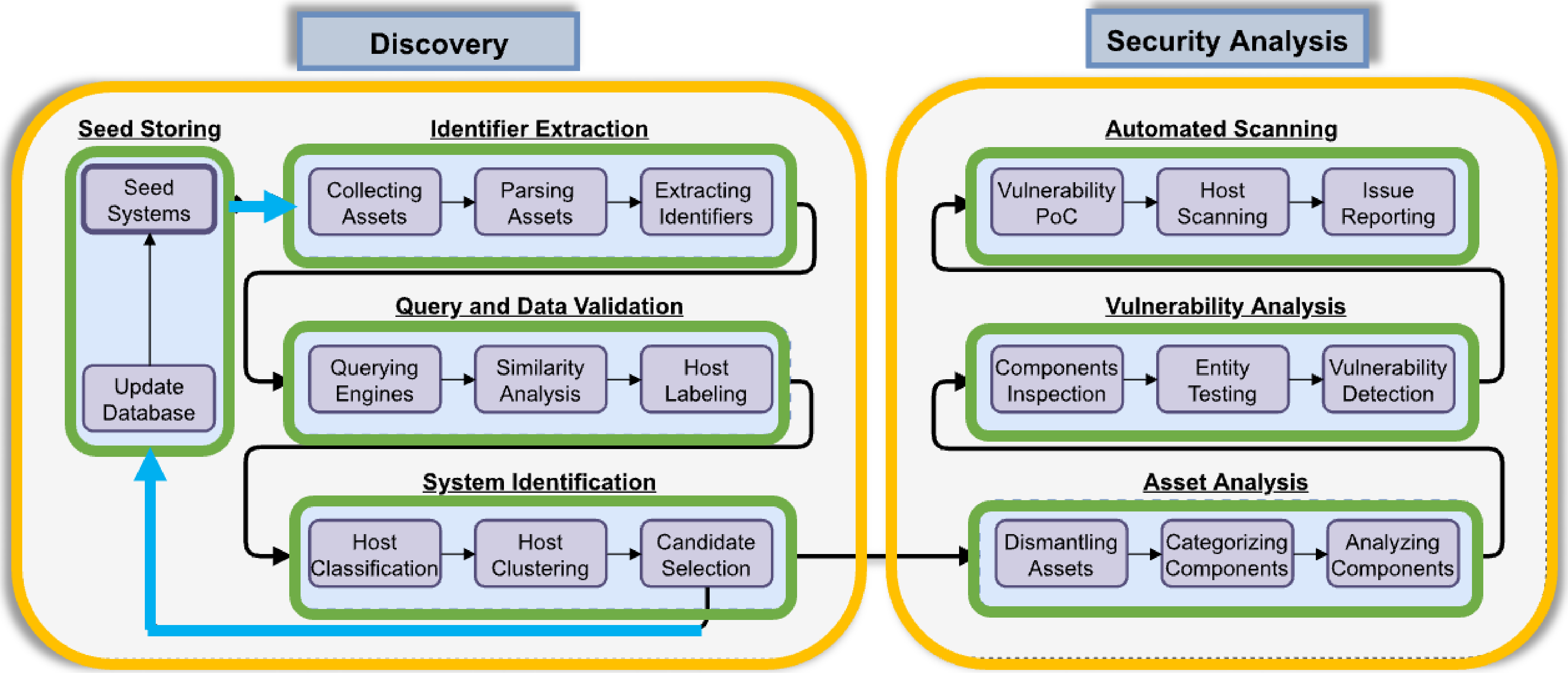
Observations

- Geographical Distribution
  - Host instances distributed across 21 countries
  - 78% were in 5 countries (due to initial seeds)
- Ports and Services
  - EVCMS hosts utilized 26 ports
  - Common ports for web services (e.g., 80 & 8080)
  - Other services: SSH (22), alternative web (82)
- Some EVCMS products use specific port combinations that can be used for targeted discovery





Proposed Approach: Security Analysis



Proposed Approach: Security Analysis

- Security analysis of the candidate EVCMS

Asset Analysis

- Dissect the collected assets & identified compiled, non-compiled, and endpoints
- Perform white-box analysis on binaries and scripts, and black-box analysis on endpoints

Vulnerability Analysis

- Trace execution flow to identify flaws & find vulnerable entry points and cleansing weaknesses
- Leverage common tools to find sensitive functionalities, intercept traffic and find insertion points
- Utilize custom testing procedures to detect classes of vulnerabilities

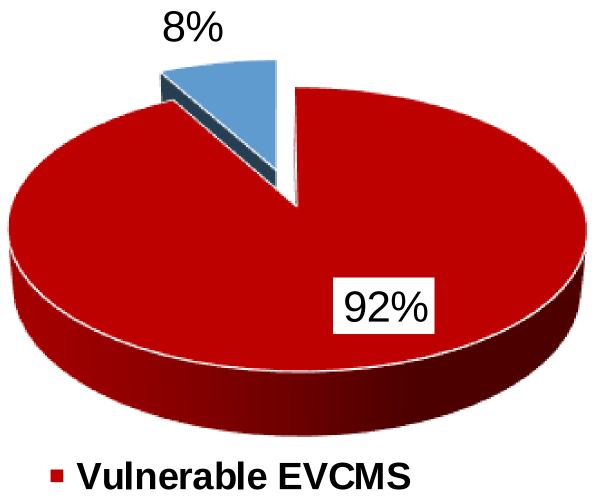
Automated Scanning

- Analyze candidate EVCMS and craft PoC for every vulnerability
- Perform a targeted scan by sending a precise number of requests and parsing the responses for indicators
- Use side-channel techniques to infer vulnerabilities by leveraging version strings and banner correlation

Quantifying the Security Posture of EVCMS

- The majority (92%) of the EVCMS were vulnerable

- About 25,000 EVCMS host instances



ENSTO

EATON
Powering Business Worldwide

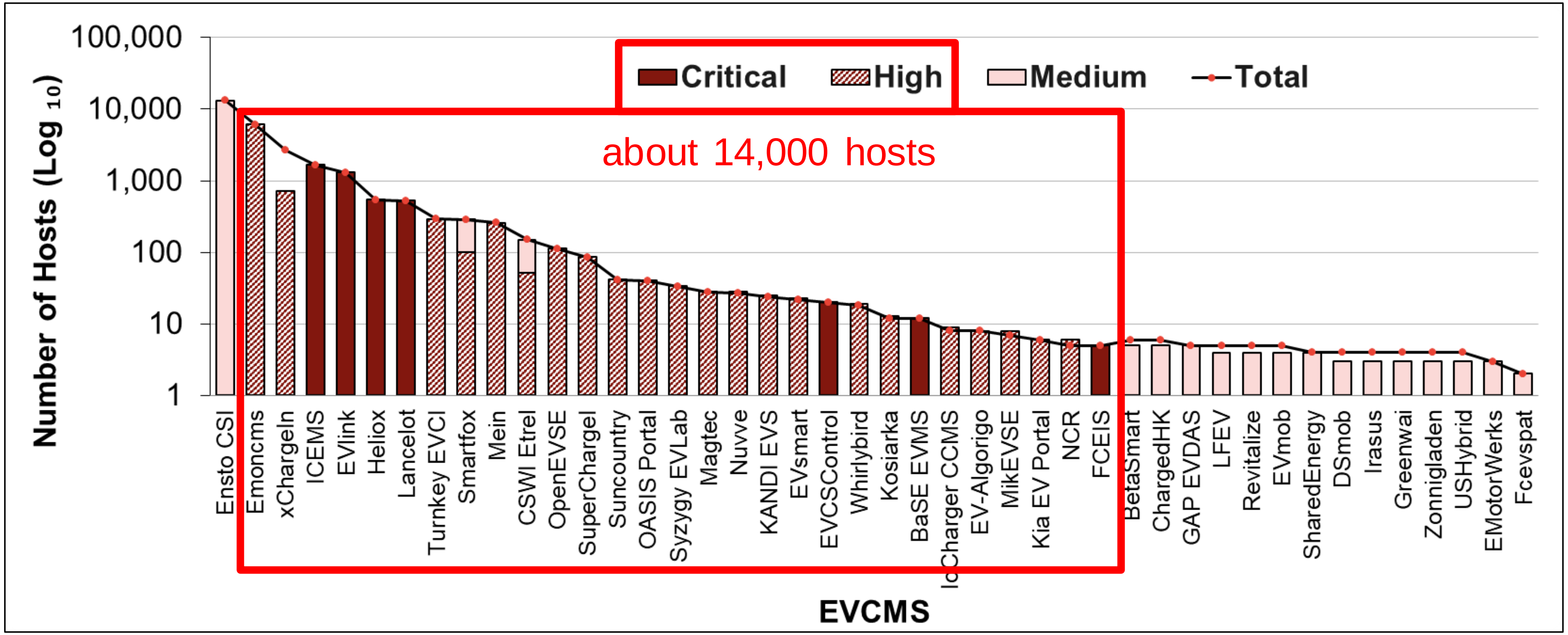
heliox

Life Is On | Schneider Electric

CHARGELAB

Quantifying the Security Posture of EVCMS

- 120 remotely exploitable vulnerabilities
- Some may lead to compromising and controlling the EVCS
- 13 classes of CWE vulnerabilities (critical, high, and medium severities)
- 29/44 EVCMS products are vulnerable to Critical/High Vulnerabilities



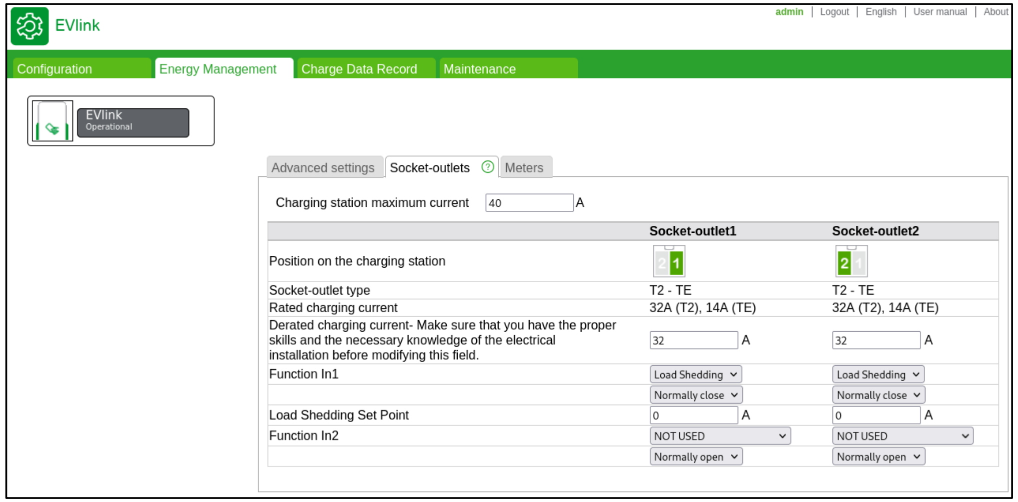
Quantifying the Security Posture of EVCMS

- 5 Critical-Severity vulnerabilities (e.g., SQLi):
  - Affect 7 EVCMS (4,431 host instances)
  - extract databases, access configurations, …
- 4 High-Severity vulnerabilities (e.g., XSS):
  - Affect 22 EVCMS (9,750 host instances)
  - hijack accounts, manipulate settings, …
- 4 Medium-Severity vulnerabilities:
  - Affect 30 EVCMS (17,831 host instances)
  - view settings, access functionalities, …

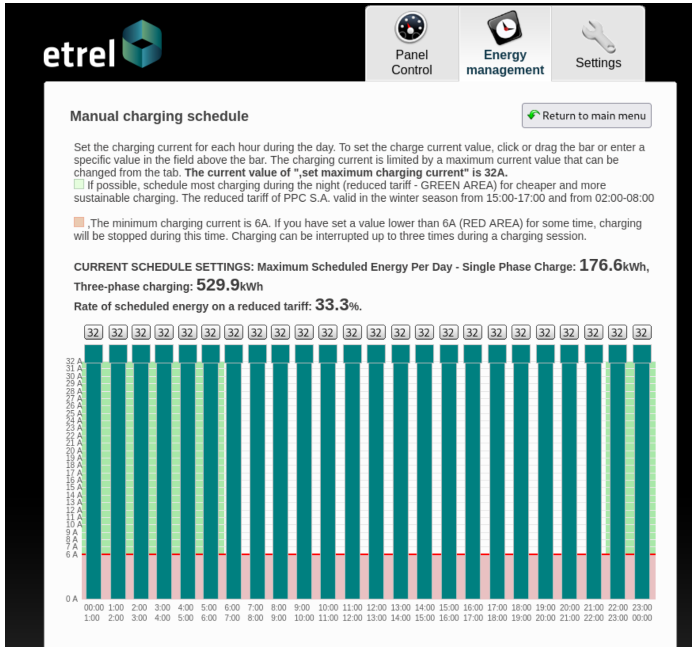
Severity	CWE	Vulnerability	# Issues	# EVCMS	# Hosts
Critical	89	SQLi	4	4	1,684
	611	XXE	5	5	1,290
	798	Hard-Coded Cred.	6	6	900
	918	SSRF	7	3	1,457
	1236	CSVi	1	1	1,203
High	79	XSS	29	19	7,754
	352	CSRF	12	9	7,789
	942	CORS Misconfig.	2	2	3,731
	942	FCDP Misconfig.	2	2	1,205
Medium	200	Info. Exposure	17	17	13,787
	306	Missing Auth.	3	3	1,005
	425	Forced Browsing	2	2	1,402
	799	No Rate Limit	30	30	17,500

Attack Implication

- Attacks Against the EVCS
  - Manipulate the charging process and configurations
  - Downgrade or modify the firmware
  - Create botnet of EVCS as network proxies
  - Lock the EVCS or disable features



- Attacks Against the Users/Operators
  - Obtain personally identifiable information, charging records, and log data
  - Leak electronic billing data

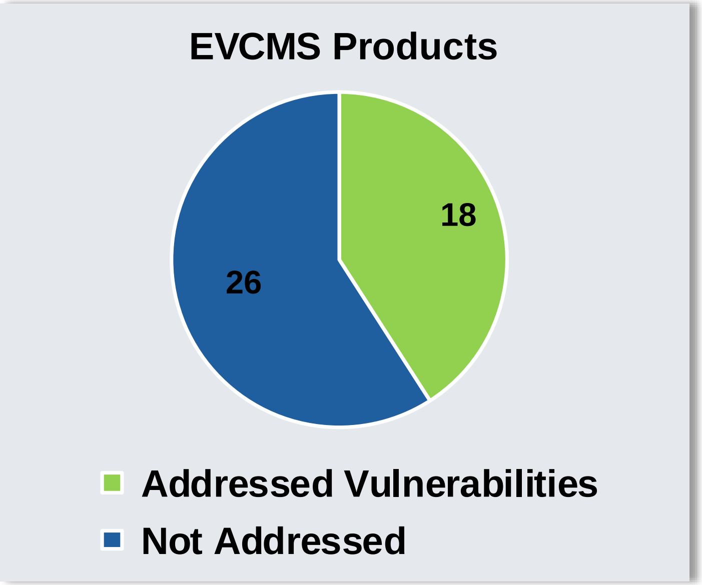


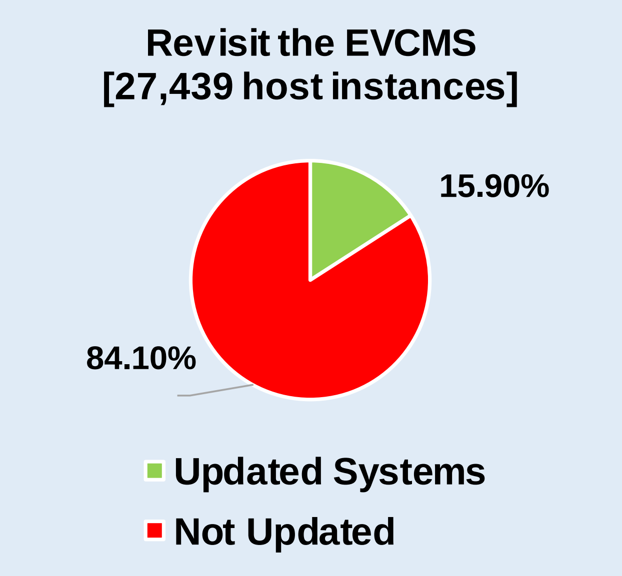
- Attacks Against the Power Grid
  - Control the charging process of a large number of EVCS
  - Conduct frequency instability attacks (cascading failures in the grid)

Vulnerability Disclosure and Mitigation

- Established a Coordinated Vulnerability Disclosure (CVD) process [1]
  - Communicated the vulnerabilities to the developers
  - Provided over 6 months prior to publishing to allow patching
- Acknowledged Zero-Days by several manufacturers
  - more than 20 assigned CVE-IDs
- Patch Follow-Up:

CVE-2021-22706	CVE-2021-22730
CVE-2021-22721	CVE-2021-22773
CVE-2021-22722	CVE-2021-22774
CVE-2021-22723	CVE-2021-22818
CVE-2021-22724	CVE-2021-22819
CVE-2021-22725	CVE-2021-22820
CVE-2021-22726	CVE-2021-22821
CVE-2021-22727	CVE-2021-22822
CVE-2021-22728	CVE-2022-22807
CVE-2021-22729	CVE-2022-22808





[1] https://www.cisa.gov/coordinated-vulnerability-disclosure-process

Main Takeaways

- Explored the security posture of EV charging ecosystem by introducing the EVCMS as a new attack surface
- Proposed an effective approach to address the limitations of existing device search engines and significantly improved EVCMS discovery/fingerprinting
- Shed light on the insecurity of EVCMS at scale (uncovering 120 zero-days)
- Contributed to the security of the EV charging ecosystem by communicating our findings to system developers (successful patching of products)

- Future Work:
  - Improve the accuracy and efficiency of the device discovery and security analysis
  - Aim towards building a real-time EVCMS discovery and analysis platform

Thank You

SADEGH TORABI, Ph.D.
Cybersecurity Researcher & Postdoctoral Fellow
Center for Secure Information Systems (CSIS)
George Mason University, Fairfax, VA, USA
storabi@gmu.edu

ChargePrint: A Framework for Internet-Scale Discovery and Security Analysis of EV Charging Management Systems

Tony Nasr*, Sadegh Torabi†, Elias Bou-Harb‡, Claude Fachkha§, Chadi Assi*
*Concordia University, Montreal, QC, Canada
†George Mason University, Fairfax, VA, USA
‡University of Texas at San Antonio, San Antonio, USA
§University of Dubai, UAE

Backup Slides

Proposed Approach (Iterative Device Discovery)

Seed Storing → **Identifier Extraction** → **Query and Data Validation** → **System Identification**

Seed Storing

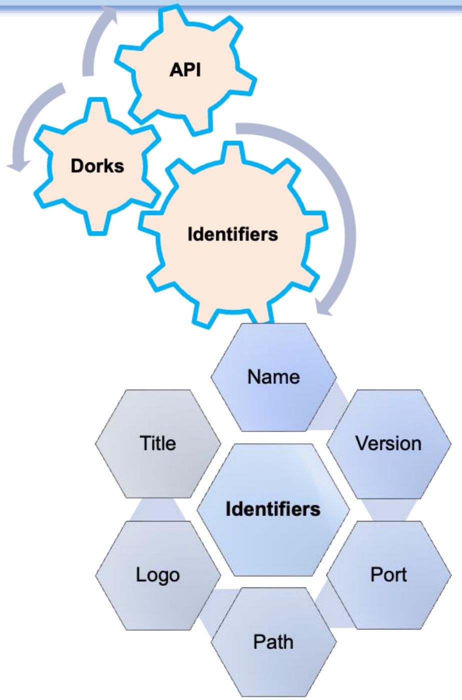
SHODAN, ZoomEye, censys, FOFA

Initial search and lookup using EV-related keywords

Identifier Extraction

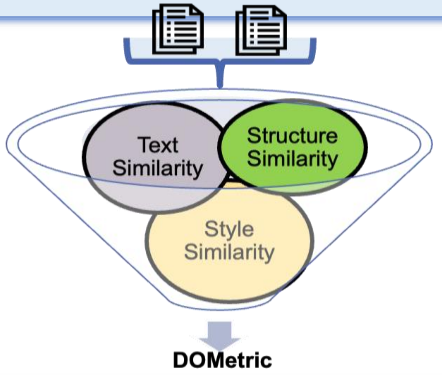
Collect/parse assets from firmware, web instances & vendor websites

Extract identifiers from filesystems items, DOM elements, & EVCS-related strings



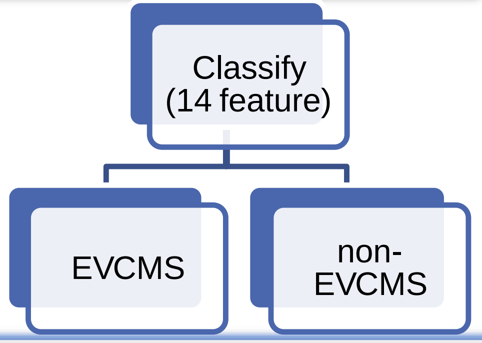
Query and Data Validation

Query search engines using new identifiers & calculate DOMetric



Compare/label discovered hosts using DOMetric (unknown hosts)

System Identification



Employ binary classifier to separate EVCMS hosts from generic devices

Cluster EVCMS host instances using DOMetric & select candidates

Update EVCMS seeds

DOMetric

For **structural similarities** D1(H,C) by performing pair-wise comparison on the sequence of tags in the HTML pages using the Gestalt pattern matching method

$$D_1(H,C) = \frac{2 \times \sum_{i=0}^{max(|S_1|,|S_2|)} |LCS(s_{1i}, s_{2i})|}{|S_1| + |S_2|} \quad (1)$$

For style similarity D2(H,C), we collect embedded style declaration blocks and selectors of common tags from documents' HTML and find the largest number of common declarations between the two documents using Jaccard's index

$$D_2(H,C) = \frac{\sum_{i=0}^{m} \frac{|a_i \cap b_i|}{|a_i \cup b_i|}}{m := min(|A|,|B|)} \quad (2)$$

For **text similarities** (D3) by vectorizing the enclosed text within the tags for the host and use cosine similarity

$$D_3(H,C) = \frac{\sum_{i=0}^{m} \frac{t_{1i} \cdot t_{2i}}{|t_{1i}| \times |t_{2i}|}}{m := min(|T_1|,|T_2|)} \quad (3)$$

$$DOMetric(H,C) = \sum_{i=1}^{3} w.D_i(H,C) \quad (4)$$