Vulnerabilities of Electric Vehicle Battery Packs to Cyber-attacks

Shashank Sripad¹, Sekar Kulandaivel², Vikram Pande¹, Vyas Sekar² & Venkatasubramanian Viswanathan¹

¹Department of Mechanical Engineering, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213.
²Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213.

Electric Vehicles (EV) like all modern vehicles are entirely controlled by electronic devices and networks that expose them to the threat of cyberattacks. Cyber vulnerabilities are magnified with EVs due to unique risks associated with EV battery packs. Current batteries have well-known issues with specific energy, cost and fire-related safety risks. In this study, we develop a systematic framework to assess the impact of cyberattacks on EVs and EV subsystems. While the current focus of automotive cyberattacks is on short-term physical safety, especially in the context of EVs, it is crucial to consider long-term cyberattacks that aim to cause financial losses through accrued impact. Compromised battery management systems such as the control of the voltage regulator could lead to cyberattacks that can either overdischarge or overcharge the pack. Overdischarge could lead to failures such as internal shorts in timescales of under an hour through cyberattacks that utilize energy-intensive EV subsystems like auxiliary components. Attacks that overcharge the pack could shorten the lifetime of a new battery pack to less than a year. Further, this also poses potential physical safety risks via the triggering of thermal (fire) events. Attacks on auxiliary components lead to battery drain, which could be up to 20% per hour. We also develop a heuristic for the stealthiness of a cyberattack to augment traditional threat models for automotive systems. The methodology and the approach presented here will help in building the foundational principles for cybersecurity in the context of electric vehicles: a nascent but critical topic in the coming years.
Modern vehicles consist of a myriad of devices and systems ranging from safety-critical systems that control a vehicle’s brakes to auxiliary components that adjust cooling and wiper speeds. While such components enhance the users’ safety and comfort, they also render the vehicle’s internal networks vulnerable to cyberattacks. When these vulnerabilities are exploited, attackers can gain access to safety-critical systems like the brakes and transmission of the vehicle, as demonstrated by recent work.\textsuperscript{1,2}

Alongside, another notable development in the automotive sector is the transition to electric vehicles (EVs) motivated by efforts to downscale tailpipe emissions.\textsuperscript{3,4} Widespread EV adoption is bottlenecked by limited driving range, battery pack cost, battery lifetime and safety issues associated with Li-ion batteries.\textsuperscript{3,5,6} The battery pack forms a significant fraction of the total cost of the electric vehicle (\textasciitilde20\% of the cost).\textsuperscript{7,8} From the standpoint of automotive cybersecurity, while the primary focus is on immediate safety concerns, EV battery packs introduce several new aspects of vulnerability. It is crucial to explore the cybersecurity aspects of battery packs to inform and improve future work in EV cybersecurity.

One challenge in assessing systems involving batteries is to accurately analyze the complex molecular-
scale processes occurring inside a closed system. A practical battery system stores a fixed amount of energy via reversible electrochemical reactions. During normal operation, several unwanted side reactions also occur, which eventually degrade the battery’s ability to store energy and thus, reduce the lifetime. Further, from a safety standpoint, batteries have a specified set of conditions for safe operation, outside of which there is the risk of thermal events. Cyberattacks may compromise driving range by draining energy through higher loads, reduce lifetime by enhancing side reactions, and compromise safety by pushing the operating conditions to unsafe limits, shown in 1.

The threat model for an EV is centered around an attacker who aims to cause either physical or financial losses through cyberattacks. Modern vehicles, including EVs, contain several devices called Electronic Control Units (ECUs) that are responsible for a majority of vehicle’s functions. These ECUs gather sensor inputs and actuate mechanical components within the vehicle. Recent efforts that have demonstrated the vulnerabilities in automotive networks, have primarily examined vehicles that employ the Controller Area Network (CAN) communication protocol. CAN is the prevailing standard for intra-vehicle communication due to low cost and robustness; however, there are many CAN exploits. An attacker can gain access to the vehicle’s CAN networks via direct physical access or the remote exploitation of an ECU with existing direct access.

**Attack Scenarios:** If an attacker aims to cause financial impact, one attack trajectory could be reducing the lifetime of the battery pack by enhancing the rate of degradation. In terms of physical damage, cyberattacks could increase the risk of thermal runaway where the attacker can overcharge or overdischarge the battery pack through attacks on the battery management systems (BMS) used in conjunction with parasitic loads.

In this work, we develop a physics-driven approach which uses an experimentally validated battery model within a vehicle dynamics model to simulate the operation of an EV. We also explore new concepts like ‘stealthiness of attacks’ and the trade-offs between stealthiness of attack and extent of damage from the attack. Using this framework, we quantify the impact of cyberattacks in different scenarios. We analyze either financial and physical losses incurred through either: (i) permanent damage, defined as a change in the state of system that is irreversible, for example, irreversible capacity loss in a battery pack and (ii) temporary damage, defined as a change in the state of system that is (mostly) reversible, for e.g., reduction in state-of-charge which can be recovered by re-charging.

**Permanent Damage:** As we stated previously, cyberattacks can accelerate cell degradation and shorten the lifetime of the battery pack. Experimental demonstration of degradation is typically indirect as batteries are closed systems and measuring the internal states of the batteries is extremely difficult. Thus, a validated physics-based model that can track the internal states of a battery packs provides a convincing means to demonstrate permanent damage due to cyberattacks.
Among the different mechanisms that cause cell degradation, two main processes of interest are: (i) growth of the solid-electrolyte interphase (SEI) layer at the graphite anode and (ii) lithium plating. The SEI layer grows as a result of solvent reduction at the anode-electrolyte interface and consumes Li$^+$ ions, thereby causing a decrease in the amount of active Li$^+$ ions available and a reduction in capacity. Plating of Lithium at the anode similarly leads to a loss in capacity along with an increase in the risk of internal shorts which could lead to catastrophic safety issues.

The permanent damage due to a cyberattack can be quantified using the rise in the internal resistance of the cell. The rise in the internal resistance is estimated using the increase in the thickness of the SEI layer. The extent of Li-plating is controlled by the electrochemical potential for lithium deposition or the ‘Li-plating potential’. The EV battery pack end-of-life is characterized by degradation in capacity to 80% of the initial capacity. We define the usable 20% of the capacity as the ‘vital capacity’ of the battery pack. A parametric study of the effect of different variables on degradation is compiled in the *Supplementary Information*.

**Compromised Auxiliary Components:** Compromised auxiliary components effectively act as parasitic loads. Quantifying the impact of such attacks requires a close examination of different operating and environmental variables. The variations in each of the state variables like temperature, state-of-charge (SOC), pack size, age of the pack, etc. and the set of variables that defines a given auxiliary component attack workload affects the degradation in vital capacity in a different manner. A parametric analysis of all the variables, exploring the effect of each variable, similar to other studies reveals that the damage to vital capacity increases with the temperature by following the Arrhenius relationship which implies that cyberattacks conducted at higher ambient temperature would cause greater impact. Damage to vital capacity also increases with the State-of-Charge of the battery pack which suggests that attacks on fully charged battery packs would cause more damage. As the age of the pack increases, the damage caused by a fixed load in the same conditions decreases. The damage to vital capacity is seen to be a sub-linear function of the total time of attack, characteristic of a diffusion-limited process. Further, damage to vital capacity increases linearly with an increase in the cumulative energy consumption of the load, a phenomenon which has been covered previous studies on capacity fade.

Following the insights from the parametric analysis, we infer that attacks which comprise of energy intensive auxiliary components when engaged after a new battery pack is fully charged cause the most damage. We design the attack scenarios accordingly. We consider two types of EV users based on charging behavior, either charging at ‘Home’ or charging at ‘Home’ and at ‘Work’. The sample attack workload spans a duration of one hour and is based on the combination of A/C at high power along with Lights, Power-Steering and Wipers. We analyze the cases where these users are located in Oslo, San Francisco, Beijing, Delhi and Phoenix which serve as proxies for the environment state variable of temperature and are chosen to represent a wide range of temperature conditions. In order to analyze the impact of auxiliary component cyberattacks, we use $\Delta R$, a quantity which represents the increase in internal resistance of the cell compared to a
Figure 2: We can study the impact of auxiliary component cyberattacks here, based on the results for simulations equivalent to \(~400\) days. \(\Delta R^*\) represents the increase in the resistance of the cell due to the cyberattack when compared to the baseline scenario. The triangular markers indicate situations where the vehicle is attacked twice in a day. In such cases, the average \(\Delta R^*\) of the two attacks is shown, while the circular markers represent the cases with one attack over the day.

cell which has not been subjected to the attack workloads. \(\Delta R\) essentially provides information on the effectiveness of the cyberattack. We calculate \(\Delta R\) after 400 days for each case using the following relationship,

\[
\Delta R = \frac{R^A_{SEI} - R^B_{SEI}}{R^B_{SEI}},
\]

where \(R_{SEI}\) is the resistance due to the SEI layer, and ‘A’ and ‘B’ represent the attack and baseline scenario. For the quantities reported in (Fig. 2), \(\Delta R^*\) values are obtained by normalizing all the \(\Delta R\) values with the minimum value in a given set which facilitates the comparison of values within the set.

In (Fig. 2), the rise in \(\Delta R^*\) is the most for Oslo, which has the lowest average ambient temperature. While an increase in ambient temperature causes an increase in the thickness of the SEI layer, the resistance due to the formation of SEI layer impedes further growth.\(^3\) This phenomenon leads to the fact that places like Phoenix, where the ambient temperature is high, already feature a substantial SEI layer thickness, thereby minimizing any additional damage to vital capacity due to the attack workload. However, it is worth highlighting that the average resistance due to the SEI film formed is higher in warmer regions compared to colder regions. The two cases of charging, at Home and at Work, do not show any substantial difference, although, if the EV is charged in both locations, then we have two separate time windows for attack.
Figure 3: A compromised battery management system is vulnerable to attacks that override the lower voltage cutoff which can overdischarge the pack. During overdischarge, one of the initial steps is the decomposition of the Li-ion containing SEI layer which is followed by the dissolution of copper ions from the current collectors, with the possibility of internal shorts and other safety events. The estimated time to the onset of copper dissolution occurs during overdischarge is shown above for the cells based on NCA (Ni$_{0.8}$Co$_{0.15}$Al$_{0.05}$O$_2$) cathode and Graphite anode. For components with the power consumption equivalent to lights (∼200 W), the time to onset of copper dissolution is under 2 hours while components with a high power consumption like air-conditioning have a timescale of less than an hour.

Compromised Battery Management Systems, Overdischarge: When a BMS is compromised, an override of the lower cut-off voltage is possible. An attack on an EV with a depleted battery pack and compromised BMS can lead to overdischarge through energy-intensive auxiliary components. In terms of such cyberattacks occurring on an EV with the depleted battery pack, the idea of using wake-up functions as attacks has been demonstrated recently. Such attacks could be followed by auxiliary component attacks discussed in this work, to overdischarge the cells. During overdischarge, the initial stages involve the decomposition of the SEI layer which is composed of Lithium containing compounds and subsequently Copper dissolution from the current collector begins. The dissolved Copper ions eventually lead to deposition of metallic Copper and potential internal shorts. The time for potential failure can be estimated using the time required for the decomposition of the SEI layer during the cyberattack, as shown in (Fig. 3). The cells shown in (Fig. 3) correspond to that of a 100 kWh battery pack based on NCA (Ni$_{0.8}$Co$_{0.15}$Al$_{0.05}$O$_2$) cathode and Graphite anode. The thickness of the SEI layer is a function of the age of the battery pack where 50nm is assumed to be equivalent to a battery pack aged over 2 years, however, the thickness would change with the vehicle operating conditions. We observe that attacks that involve components with an energy consumption rate of over 200W, the timescale for the complete decomposition of the SEI layer and potential failure is under 2 hours. While the consequences of overdischarge in Li-ion batteries depend on the kind of materials used in the cells, the impact could range from the loss of energy through the internal short to thermal and safety events as well.
Figure 4: The impact of cyberattacks on charging systems specifically aimed at overcharging the battery pack is summarized here. (a) The attacks studied here lasts for one hour after charging. We can study the increase in the SEI growth rate and $\Delta R^*$. (b) This increase along with Li-plating translates to capacity fade and could shorten the lifetime to about 200 days at an overcharge voltage of about 0.4V. The reduction in the Li-plating potential due to overcharge in (Fig. 4a), provides a metric to quantify the risk of developing internal shorts due to lithium plating. When the same attacks are performed on older packs, we observe that the $\Delta R^*$ growth rate increases while the Li-plating potential decreases, both of which are detrimental to the state-of-health of the battery pack.

**Compromised Battery Management Systems, Overcharge:** A compromised BMS can modify the upper cut-off voltage. The pack can then be charged at a voltage higher than the normal charging voltage (manufacturer specific upper voltage cutoff) leading to overcharging. Within a constant current-constant voltage protocol, an increase in the charging current would lead to an increased rate of degradation which is an extension of the previously mentioned parametric analysis on the discharge rate of the battery pack. However, overcharging the battery pack leads to various other issues shown in (Fig. 4).

In (Fig. 4a), we observe a super-linear rise in the growth rate of $\Delta R^*$ as the overvoltage per cell increases in a fresh cell. The charging system cyberattack simulated spans a duration of one hour after charging similar to the auxiliary component cyberattacks. However, the consequent damage caused to the battery pack in terms of capacity fade, as shown in (Fig. 4b), is enormous. At a cell overvoltage of 0.4V, we observe that the pack reaches its end-of-life or 100% damage to vital capacity in about 200 days. This could result in significant financial impact as shown in (Fig. 4b) where we estimate the monetary value of the loss of capacity for a 100kWh battery pack assuming the cost of battery packs of about $200/kWh. (Fig. 4a) also shows the decrease in the Li-plating potential which implies that lithium would plate more readily at higher overvoltage. Over time, such attacks could lead to an increased amount of Li-plating which could have safety implications resulting in physical impact including thermal events and fire.

**Temporary Damage:** With compromised auxiliary components, attack workloads can cause a depletion of energy contained in the battery pack, thereby a reduction in available driving range.
Table 1: Stealthiness of attack, a qualitative metric used by attackers to reduce the chance of detection.

<table>
<thead>
<tr>
<th>Auxiliary Component</th>
<th>Stealthiness of Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Parked</td>
</tr>
<tr>
<td>A/C-High</td>
<td>High</td>
</tr>
<tr>
<td>A/C-Low</td>
<td>High</td>
</tr>
<tr>
<td>Power Steering</td>
<td>N/A</td>
</tr>
<tr>
<td>Lights</td>
<td>High</td>
</tr>
<tr>
<td>Fan</td>
<td>High</td>
</tr>
<tr>
<td>Wipers</td>
<td>Medium</td>
</tr>
<tr>
<td>Combinations</td>
<td>High</td>
</tr>
</tbody>
</table>

This damage can be reversed by charging the battery pack. However, such attacks can play into the well-known issue of ‘range anxiety’.

For some vehicles, with battery packs <40 kWh battery packs, up to 20% of the available range could be depleted in under one hour with energy intensive attack workloads which include combinations of auxiliary components as discussed previously. Such attacks which engage several components at the same time will be more energy intensive compared to single components, however, such attacks might be easier to detect for the user which is discussed in the subsequent sections.

**Stealthiness of Attack:** An important constraint on a cyberattack is the likelihood of it getting detected. In the case of auxiliary components, the detection is by the user and hence it is difficult to develop a quantitative metric for the same. However, in order to provide a basic overview of the issue, we develop a qualitative understanding using three scenarios, namely, ‘parked’, ‘stationary’ (at rest within driving operation) and ‘driving’. A summary of the stealth of an attack involving a given auxiliary component is given in (Tab. 1). Such a metric is heuristic but it provides a calibration for the components that are more likely to be targeted based on the attacker’s perspective. An auxiliary component that involves a high stealthiness of attack and is also energy intensive would naturally be targeted often.

**Rowhammer Attack:** Rowhammer style attacks have been demonstrated previously where targeted workloads on memory systems were generated to cause corruptions which can be used to launch further attacks. We observe an analogous case here with battery systems since battery pack is made up of several cells arranged in a matrix involving a series-parallel configuration. This architecture is vulnerable to ‘rowhammer’ attacks since individual strings or cells within battery packs could be targeted through a compromised battery management system and the damage to individual strings or cells is magnified. Each of the cyberattack scenarios we have considered, like attacks on auxiliary components, overcharge, and overdischarge could be orchestrated as rowhammer attacks. We previously discussed the various factors due to which the damage to the battery pack increases with a reduction in pack size for the same workload which is especially relevant to rowhammer attacks. Such attacks could not only shorten the lifetime of the targeted subset of the battery pack but could also lead to issues related to instabilities due to the isolation of strings within the battery pack.
We have discussed the potential physical and financial impact due to cyberattacks on EVs and EV subsystems. We identify simple but effective cyberattacks on auxiliary components that can temporarily drain the battery pack up to 20% per hour. Furthermore, we analyze attacks that could lead to a deterioration in the power capability due to an increase in the cell resistance. We use a metric which is equivalent to the ‘normalized resistance increase’, which can be used to quantify the extent of performance reduction. We find that normalized resistance increase is generally higher for colder regions. We find that cyberattacks on auxiliary components launched after the pack is completely charged (i.e. high state-of-charge) lead to more damage. The cell resistance increase, largely due to the formation of a solid-electrolyte-interphase (SEI) layer, follows a sublinear relationship with time. This results in a new pack being more vulnerable than an aged pack to cyberattacks on auxiliary components. Compromised battery management systems expose the pack to two kinds of attacks, (i) Overdischarge and (ii) Overcharge. Overdischarge attacks which override the lower cutoff voltage of the pack could lead to the complete decomposition of the SEI layer in under two hour thorough auxiliary components with a power rating of over 200W. The decomposition of the SEI is followed by the dissolution of Copper ions which could eventually lead to internal shorts and potential safety events. Cyberattacks launched during charging through the compromise of the voltage regulator could lead to an overcharge of the cells, which in some cases could even lead to physical safety issues (e.g. fire). Further, this could lead to a new pack being depleted to 80% of its initial capacity (end-of-life for an EV battery) in less than a year. Finally, a compromise of the battery management system could lead to novel “rowhammer”-style attacks (attacking a string of cells), which could damage a subset of cells in a short time span. We believe that the results presented here will inform the development of robust detection and prevention systems and provide a rational design approach for electric vehicle automotive security.

Acknowledgements S. S., S. K., V.S. and V. V. gratefully acknowledge support from Technologies for Safe and Efficient Transportation University Transportation Center. V.S. and V. V. gratefully acknowledges support from the Pennsylvania Infrastructure Technology Alliance, a partnership of Carnegie Mellon, Lehigh University and the Commonwealth of Pennsylvania’s Department of Community and Economic Development (DCED).

Competing Interests The authors declare that they have no competing financial interests.

Correspondence Correspondence and requests for materials should be addressed to V.V. (email: venkvis@cmu.edu).

Methods

Battery Pack Simulations. The description of the system of equations for the multiphysics battery model\textsuperscript{14,20} can be found elsewhere. Cells constructed based on this modelling framework are assembled into a battery pack model. The baseline load profile for the vehicle is based on Urban Dynamometer Driving Schedule for 50 miles per day, along with a constant current-constant voltage (CC-CV) charging protocol with a peak power of a level-1 charger. The attack workloads are
implemented within this daily load profile. The daily load profiles are repeated to simulate the operation over a long period. The battery model is a thermally coupled model,20 and the ambient temperature conditions are implemented within the same simulation framework, described in detail in the Supporting Information.

 Supporting Information (SI): Supporting Information contains details of the parametric study for battery degradation and other information on the battery modeling undertaken for the study.

References


Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks on Auxiliary Components

Shashank Sripad\textsuperscript{a}, Sekar Kulandaivel\textsuperscript{b}, Vyas Sekar\textsuperscript{b,1}, and Venkatasubramanian Viswanathan\textsuperscript{a,1}

\textsuperscript{a}Department of Mechanical Engineering, Carnegie Mellon University, Pittsburgh PA 15213; \textsuperscript{b}Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh PA 15213

This manuscript was compiled on February 18, 2018

Modern automobiles are entirely controlled by electronic circuits and programs which undoubtedly exposes them to the threat of cyberattacks. Alongside, there is a potential for massive growth in electric vehicle (EV) adoption. The cyber vulnerabilities are magnified with electric vehicles because of the unique and critical risks that entail most EV batteries. EV battery packs provide ‘limited driving range’ and have ‘finite lifetime’, and there is widespread anxiety regarding range and life. In this study, we develop a systematic framework to model cyberattacks on auxiliary components and identify the consequent impact on EV batteries. We model the possible cyberattacks on auxiliary components by engaging them in various ‘modes’ and analyze the impact on battery packs through a physics-driven experimentally-validated model that accurately captures battery dynamics and degradation. In the short-term, cyberattacks could deplete a battery pack by up to 20% per hour and completely drain the available range. The EV battery pack is most vulnerable to cyberattacks when it is fully charged due to the influence of state-of-charge (SOC) on the battery health. For long-term impact, we explore the location effect of attack and identify that cyberattacks could cause a 3-fold increase in the internal resistance (an indicator of cycle life) in cold regions versus hot regions. We believe that the methodology and the approach presented will help in building the foundational principles for cyber-security in the context of electric vehicles; a very nascent but crucially important topic in the coming years.

The modern automobile has all of its ‘workflows’ controlled by electronic circuits, and the provision of additional features and wireless instruments renders the vehicle vulnerable to a host of cyberattacks. The area of automotive cyber-security has received significant attention over the past few years (1, 2) and demonstrated cases of automotive cyberattacks till date have been primarily focused on the possibility of compromising the functionality and safety of automobiles.(1, 2)

Alongside, another notable development in the automotive sector is the transition towards EVs as a response to tailpipe emissions and global warming.(3, 4) The current global stock of over 2 million EVs and HEVs is evidence for the tremendous progress in EV adoption.(5) However, their adoption is still limited by concerns of limited driving range, lifetime, and safety owing to the limitations and potential risks associated with current Li-ion batteries.(6–8)

Given these two emerging trends, a natural question that emerges is the possibility of cyberattacks in undermining the range, life and safety of EV batteries. The hacking of battery firmware, limited to portable electronics, where the supplanting of routine commands with malicious ones within battery monitoring systems is shown.(9) It is worth highlighting that EV batteries are vastly different from portable electronics in terms of the scale of the systems, conditions of operation, as well as the constituent materials and thus, there exists an enormous gap in understanding the landscape of automotive cybersecurity unique to electric vehicles.

The primary challenges involved in assessing the security concerns of systems involving batteries is due the complex molecular-scale processes occurring inside a closed system. A practical battery system stores a limited amount of energy via reversible electrochemical reactions at each electrode. During normal operation, several unwanted side reactions also occur which eventually degrade the battery’s ability to store energy and thus, reduce the lifetime(10). In addition, any battery system also has a specified set of conditions for safe operation, outside which there is a potential risk of fire due to the flammable electrolytes used in modern batteries (7, 11), an event generally referred to as ‘thermal runaway’ (7). Cyberattacks could compromise the driving range of EVs by targeting the stored energy, the lifetime by enhancing the side reactions, and safety by pushing the operating conditions to unsafe limits.

In this article, we develop a physics-driven approach to systematically analyze cyberattacks on EV batteries. Using this approach, we analyze the potential impact of a cyberattack on the driving range of the EV, and secondly, the impact of battery firmware, limited to portable electronics, where the supplanting of routine commands with malicious ones within battery monitoring systems is shown.(9) It is worth highlighting that EV batteries are vastly different from portable electronics in terms of the scale of the systems, conditions of operation, as well as the constituent materials and thus, there exists an enormous gap in understanding the landscape of automotive cybersecurity unique to electric vehicles.

Significance Statement

Modern automobiles are exposed to a host of cyberattacks and the potential risks that entail such attacks has gained significant attention lately. Alongside, globally, the automotive industry is transitioning towards electric alternatives as a response to the harmful effects of tailpipe emissions. The heart of an electric vehicle, the battery pack, could be the target of such cyberattacks, and the associated risks are both critical and unique. In order to understand and quantify these risks, we need a new paradigm which couples existing automotive cyber-security narratives with the knowledge-base on battery systems, and this study presents the first such model for analysis.

V.S and V.V designed the research, S.S. performed all the battery pack simulations. S.K. and S.S. developed the detectability index. S.S., S.K., V.P., V.S. and V.V. analyzed the results and wrote the paper.

The authors declare no conflict of interest.

\textsuperscript{1}To whom correspondence should be addressed. E-mail: vsekar@andrew.cmu.edu

PNAS | February 18, 2018 | vol. XXX | no. XX | 1–11
on the lifetime of the battery pack. The attack scenarios considered are shown in (Fig. 1), where the attacker is able to gain control of the auxiliary components of the automobile to orchestrate a cyberattack. The different variables that need to be considered for modeling such an attack scenario could be categorized as (i) Environment state variables, (ii) Battery pack state variables, (iii) Attacker’s control dimensions, and (iv) Attacker’s constraints. Throughout this study, we only consider ‘primary’ attacks which can compromise systems within the vehicle. It is worth pointing out that ‘secondary’ attacks which attempt to compromise the infrastructure around EVs like charging stations could also be important. Furthermore, we do not explicitly address the issue of the possibility of fire (7), since a physics-driven understanding of this phenomenon is limited at this stage.

In order to enable this analysis, we systematically compiled the energy consumption pattern of every auxiliary component along with its characteristic power profile. The relevant data for such power profiles is curated from a large number of studies (12–16) where several components in different modes of operation have been analyzed. We believe this dataset will form an important piece for future automotive cybersecurity studies.

The workload of a cyberattack is determined by the instantaneous power consumed and the duration of the attack. In the context of auxiliary components, the cyberattack can engage one or more components in different operating modes for varying periods of time, which forms the control dimensions of the attacker. The workloads cause a quantifiable impact on the functionality of the battery pack and thereby of the vehicle itself. It is worth pointing out that cyberattacks engaging certain components can be easily identified (for e.g. windshield wipers). Further, long term engagement also leads to possible identification (for e.g. air conditioning). Thus, there exists additional constraints on duration of attacks and the choice of components for engaging the attack. We explicitly address this issue by developing a preliminary metric for detectability by systematic categorization of the components.

Results and Discussion

We begin by examining the short-term and long-term impacts of cyberattacks on EV battery packs followed by a discussion on a possible approach to understand the attacker’s constraints.

Short-term Impact. Once the auxiliary components are compromised, the attack workloads cause a depletion of energy contained in the battery pack, thereby a reduction in available driving range. Such an impact would play into the well-known issue of ‘range anxiety’ (17, 18).

For the examination of short-term impact or range reduction, we examine different electric vehicles chosen on the basis of the availability and market share in the United States (19), namely, Leaf manufactured by Nissan Motor Company Ltd., i3 by BMW AG, Model S P100D by Tesla, Inc., and e6 by BYD Auto Co., Ltd. The relevant data on the energy consumption, range, and battery pack characteristics for each of these vehicles can be found in the (SI-Text). For all our battery pack analysis, we use a multiphysics thermally coupled Li-ion battery model (20) based on the AutoLion-ST platform. The details and working of the model can be found in the (Methods Section). We have successfully utilized this platform for realistic pack design in a variety of electric vehicle use-cases. (21–23)

The short-term impact of different attack workloads on each of the aforementioned EVs is shown in (Fig. 2). The workload could comprise of either a single component or multiple components engaged at the same time. The important variable in the context of short-term impact is energy consumption, which determines the range of the vehicle. In terms of battery pack state variables, the pack energy or size determines the range based on the energy consumption per unit distance or electric-mileage of the vehicle. In (Fig. 2), we observe the short-term impact by engaging various components is roughly linear in time with the slope being given by the power consumed by the component(s). As would be expected, the high power components such as air conditioning (A/C, 2.6 kW) and Wipers (1.2 kW) lead to the greatest reduction in range. We observe that EVs with smaller battery pack like the Nissan Leaf (30 kWh) or the BMW i3 (33 kWh) are impacted to a much greater extent with a loss in range of

---

**Fig. 1.** Pictorial illustration of an attack scenario. The illustration enumerates all the variables that need to be considered for analyzing the impact of a cyberattack. The four sets of variables together define the environment, specify and define the state of the battery pack, provide a description of the variables under the attacker’s control, and stipulate the constraints that the attack is subjected to. The attacker employs the control variables with the intention of causing short-term impact in terms of reduction in the range of the vehicle or to cause long-term permanent damage to the battery pack. (The automobile outline illustration is published with permission from Chris Philpot.)
To summarize, short-term impact or range reduction due to short-term range reduction analysis also highlights the risk to hybrid electric vehicles (HEVs) since most HEVs have much smaller battery packs compared to EVs, and consequently would lose most of the electric driving range in a short span of time. As the battery packs age, the capacity and driving range reduces, and consequently the impact of short-term cyberattacks would be greater. The rate of aging for current EV battery packs is typically low and thus, the age of the pack has minimal effect in the context of short-term impact.

To summarize, short-term impact or range reduction due to a given cyberattack workload is more effective on smaller battery packs at a lower state-of-charge. The impact would also be marginally higher for older battery packs. The move towards smaller battery packs for urban commute faces a huge threat from cyberattacks. In addition, in the urban scenario, the typical state-of-charge of EVs is well below full charge and with limited charging infrastructure available per EV, this represents a serious vulnerability.

Long-term Impact. Assessing long-term impact is challenging due to the prohibitive (and often impractical) ‘time-cost’ associated with actual battery testing. Thus, the only realistic approach to tackling this challenge is to build high-fidelity experimentally validated models coupled with high-precision testing for a short period of time.

The primary mechanism responsible for cell degradation is the growth of the solid-electrolyte interphase (SEI) layer at the graphite anode of a Li-ion battery. The layer grows as a result of solvent reduction at the anode-electrolyte interface which consumes Li\(^+\) ions, thereby causing a decrease in the amount of active Li\(^+\) ions available and loss in capacity. A model for the current density of the rate of SEI formation is given by:

$$j_{SEI} = -k_{SEI}c_{SEI} \exp\left(\frac{\alpha F}{RT}(\phi_1 - \phi_2 - \frac{\delta}{k_{SEI}(j_n + j_{SEI})})\right), \quad [1]$$

The details of each of the variables can be found in (SI-Text). In addition to loss in capacity, the thickness of the SEI layer increases the internal resistance or impedance of the cell, thereby leading to a loss in the power capabilities.

We propose that the long-term impact of a cyberattack can be quantified using the increase in thickness of the SEI layer or equivalently by the increase in internal resistance due to the attack. The EV battery pack end-of-life is characterized by degradation in capacity to 80% of the initial capacity. The usable 20% of the capacity can be called the ‘vital capacity’ of the battery pack, and the variations in each of the state variables like temperature, state-of-charge, pack size, pack age, etc. affect the degradation in vital capacity in a different manner. A parametric analysis of all the variables was carried out, shown in (Fig. S1-S4), to explore the effect of each variable on the damage to vital capacity and thereby identify the variables which influence the degradation process to the greatest extent.

The damage to vital capacity as a function of ambient temperature during the cyberattack displays the well-known Arrhenius relationship as seen in (Fig. S1). Attacking a battery pack at higher operating temperatures, or in other words, a
time-of-day when the temperature is higher or in geographical locations where the ambient temperature is higher would lead to a greater damage to vital capacity. Evaluating the effect of temperature along with variations in the state-of-charge of the battery pack can be seen in (Fig. S2), based on which we can conclude that cyber-attacks conducted on fully charged battery packs would have a much greater impact than attacks on depleted packs. The time-window after an EV battery pack is fully charged is when the battery is at its highest state-of-charge, and hence is the point when the EV is most vulnerable. Capacity increases linearly with increase in the cumulative energy consumption and average power, the effect of an increase in the differential of power is minimal. Alternatively, what we see is that the magnitude of the discharge rates induced due to auxiliary components is not large enough to have a significant effect on the damage to vital capacity, consistent with prior experimental predictions of the capacity fade with rate of discharge (30).

Using an attack workload that is more energy intensive or attacking a battery pack that is smaller have an equivalent effect, since the metric needed to assess is the depth-of-discharge (ΔDOD) due to the workload. We would also obtain a linear relationship between the ΔDOD and the damage to vital capacity similar to the one seen in (Fig. S4). It follows that workloads which employ energy intensive components or workloads with multiple components engaged together, would cause a greater impact on the battery pack. Although, the increase in the magnitude of damage due to workloads with higher energy consumption is not significant, as seen in (Fig. S4) from the small slope of the linear relationship. A ‘row-hammer’ attack scenario based on the same concept is that of exerting the attack workload on a few rows of cells within the pack. Under such a scenario the ΔDOD increases linearly with the decrease in number of rows. Such an attack would magnify the damage on the rows of the cells under attack and would accelerate the degradation to end-of-life.

An important question emerges on whether age of the pack plays a role in determining the impact of cyberattack. (Fig. S2) shows a bi-variate analysis between SOC and temperature for battery packs of different age, where we observe that older packs show a lower magnitude damage for the same attack workload. Further, we observe a monotonic decrease in the magnitude of damage with every successive attack for the same attack workload. (Fig. S3) shows this quantitatively, illustrating the damage to vital capacity as a function of the time taken by different attack workloads. This shows that damage to vital capacity is a sub-linear function of the total time of attack and age of the pack, characteristic of a diffusion-limited process.

The effect of the nature of the power profile of a workload can be studied using the metrics of cumulative energy consumption, the average power, and the rate of change in power. In (Fig. S4), we observe that while the damage to vital capacity increases linearly with increase in the cumulative energy consumption and average power, the effect of an increase in the differential of power is minimal. Alternatively, what we see is that the magnitude of the discharge rates induced due to auxiliary components is not large enough to have a significant effect on the damage to vital capacity, consistent with prior experimental predictions of the capacity fade with rate of discharge (30).

Fig. 3. The daily power load on the Model S P100D which shows multiple scenarios. The power load shown in ‘blue’ represents the baseline scenario where we have no cyberattacks, and the ‘red’ represents the attack scenario. The attack is assumed to take place only during the time-window after charging based on the conclusions drawn from the our analyses above. The case where the user charges only at home is illustrated in (a) while (b) is a case where the user charges both at home and at work. The attack scenario in the work-charging case could have two distinct sub-cases where the attack is conducted either at one or both the time-windows after charging.

Fig. 4. We can study the long-term impact of cyberattacks here based on the results of simulating the power loads shown in (Fig. 3) for ~400 days. ΔR* represents the relative increase in the resistance of the cell due to the cyberattack when compared to the baseline scenario. Each geographical location shown is incorporated using the variations in ambient temperature over the year. The triangular markers indicate situations where both time-windows after charging in the work-charging case are exploited to attack and in such cases the average ΔR* of the two attacks is shown in the figure, while the circular markers represent the cases where only one cyberattack. The data used to incorporate the ambient temperature variations can be seen in (Fig. S6).

Based on the parametric study summarized above, we can now describe critical attack workloads that are possible and examine them in real-world scenarios. The combination of components chosen for an attack aimed to cause greater impact would be a combination shown in (Fig. 2) which uses...
high-powered air-conditioning, along with lights, wipers, and the power-steering. The results from the parametric analysis of the state-of-charge suggests that the attack should be conducted after the pack is charged completely, and hence we need to design the attack scenario accordingly. We consider two types of EV users as shown in (Fig. 3), the first is a user who only charges the battery pack at 'Home' and the other is a user who charges at 'Home' and at 'Work'. In the former case we have only instance to attack, while the latter case has two instances for the attack. We analyze the cases where these users are located in Oslo, San Francisco, Beijing, Delhi and Phoenix. These locations are chosen to represent a range of temperatures and including potential locations where there could be substantial EV penetration. We also limit the total time for attack to one hour due to the constraints of detectability, which will be discussed later. Another aspect to note here is the apparent analogy between our current approach to assessing long-term damage from cyberattacks and discussions on damage to EV batteries from the Vehicle-to-Grid (V2G) model(31), but an important distinction between the two situations is that in the latter, the user controls whether or not the EV participates in the V2G model, whereas, in the context of cyberattacks the user has no control. It follows that, the findings from our analysis would have implications on the approaches to assess damage for V2G scenarios as well.

In order to assess the permanent damage caused due to the cyberattack in real-world scenarios shown in (Fig. 3), we propose the use of a normalized quantity, $\Delta R$, which represents the increase in internal resistance of the cell as compared to a cell within a pack which has not been subjected to the attack workloads. $\Delta R$ provides information on the effectiveness of the cyberattack. We calculate $\Delta R$ after 400 days for each case using the following relationship,

$$\Delta R = \frac{R^A_{SEI} - R^B_{SEI}}{R^B_{SEI}}, \quad [2]$$

where $R_{SEI}$ is the resistance due to the SEI layer, and ‘A’ and ‘B’ represent the attack and baseline scenario. For the quantities reported in (Fig. 4), $\Delta R^*$ values are obtained by normalizing all the $\Delta R$ values with the minimum value in a given set.

In (Fig. 4), we observe an interesting result regarding location that the relative increase in internal resistance is the most for Oslo, which has the lowest average ambient temperature. This appears to be in contradiction with earlier analysis that shows that higher temperature leads to higher damage due to the attack workload. While an increase in ambient temperature causes an increase in the thickness of the SEI layer, the resistance due to the formation of SEI layer impedes further growth. This phenomenon leads to the fact that places like Phoenix, where the average temperature is high, already feature a substantial SEI layer thickness, thereby minimizing any additional damage to vital capacity due to the attack workload. It is worth highlighting however, that the average resistance due to the SEI film formed is higher in warmer regions compared to colder regions.(32) Comparing the two scenarios of an attack after charging at home versus at work, there is minimal effect on the damage to vital capacity, since the average temperature between the two cases is nearly the same. This analysis suggests that the extent of damage is highest for colder regions, but largely independent of attack timing. In (Fig. 4) we can also study the second case which is that of two attack sequences, one at Work and the other at Home, which is possible in the Work charging scenario.

**Attack Constraints.** An important limitation on the attack is the ability to be detected and the detection process is a highly probabilistic quantity that depends on many different factors. Here, we propose a simplistic model towards handling this complex issue. We develop a quantity, which we term ‘detectability index’ for each component which is a function of time, that measures the degree to which an attack on that component can be detected. The methodology for calculating the detectability index is based on the evaluation of three primary detectable indices associated with a given auxiliary component, (i) physical actuation, (ii) notification regarding the engagement of component and (iii) the component’s
We began this analysis by considering the enormous thrust to develop approaches to deal with issues of cyber security. In this process, it is vital to understand the importance of accurate, precise, and predictive models of battery systems.

Materials and Methods

The 1D+1D or Pseudo 2D model used to simulate the battery pack operation is discussed here. Other details on the power load of the auxiliary components and the energy consumption of EVs can be found in (SI-Text).

Battery Modeling. These equations used for the battery modeling are summarized by Fang et al.,(36) and Kalupson et al.,(20) using Eqs. (3-7) which describe the 1-D transport model for the species and the charge coupled with a lumped thermal model. The solid phase charge conservation is given by

$$\nabla \cdot (\sigma_{\text{eff}} \nabla \Phi_s) = j_{\text{Li}},$$  

where $\sigma_{\text{eff}}$ is the effective electronic conductivity and $\Phi_s$ is the potential of the solid phase. The electrolyte phase charge conservation is given by

$$\nabla \cdot (k_{\text{eff}}^\text{Li} \nabla \Phi_e) + \nabla \cdot (k_{\text{eff}}^\text{ionic} \nabla \log(c_e)) = -j_{\text{Li}},$$  

where $k_{\text{eff}}^\text{Li}$ is the effective ionic conductivity, $\Phi_e$ is the potential of the electrolyte phase, $k_{\text{eff}}^\text{ionic}$ is the conductivity and $c_e$ is volume averaged Li concentration in the electrolyte phase. The conservation of species in the electrolyte phase is given by

$$\frac{\partial (\xi c_e)}{\partial t} = \nabla \cdot (D_{\text{eff}} \nabla c_e) + \frac{(1 - \xi_0)}{F} \varepsilon_0 j_{\text{Li}},$$  

where $\xi_0$ is the volume fraction, $D_{\text{eff}}$ is the effective diffusion coefficient, $\varepsilon_0$ is the transference number, and $F$ is the Faraday constant. The species conservation in solid phase is given by

$$\frac{\partial c_s}{\partial t} = D_s \frac{\partial}{\partial r} (r^2 \frac{\partial c_s}{\partial r}),$$  

where $c_s$ is the concentration of Li in the solid phase, $D_s$ is the diffusion coefficient in the solid phase, and $r$ represents the radius of the particles of active material. The energy balance is represented as a lumped thermal model given by

$$\frac{\partial (\rho C_p T)}{\partial t} = (q_r + q_i + q_k + q_o) A_{\text{cell}} + h_{\text{conv}} A_e (k\nabla T),$$  

which accounts for $q_r$ reaction heat, $q_i$ the joule heating, $q_k$ the heating due to contact resistance between the current collector and electrode materials, and $q_o$ the entropic heating. The last term represents the heat dissipation, where $h_{\text{conv}}$ is the coefficient of heat dissipation and $A_e$ is the cell external surface area.

Degradation Process. An SEI film growth model is used to quantify the loss of active Li-ions and is modeled in a manner similar to other well-known studies(28).

$$\frac{d\rho_{\text{SEI}}}{dt} = -\frac{j_{\text{SEI}} M_{\text{SEI}}}{2F \rho_{\text{SEI}}},$$  

where $M_{\text{SEI}}$ and $\rho_{\text{SEI}}$ are the molecular weight and the density of the SEI. The resistance due to the SEI is calculated using the effective conductivity of the electrolyte (calculated through the SEI using):

$$R_{\text{SEI}} = \frac{\delta_{\text{SEI}}}{\kappa_{\text{SEI}}},$$  

ACKNOWLEDGMENTS. S. S., S. K., V. S., and V. V. gratefully acknowledge support from Technologies for Safe and Efficient Transportation University Transportation Center. V. S. and V. V. gratefully acknowledges support from the Pennsylvania Infrastructure Technology Alliance, a partnership of Carnegie Mellon, Lehigh University and the Commonwealth of Pennsylvania’s Department of Community and Economic Development (DCED).
References


Supporting Information for Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks on Auxiliary Components

Shashank Sripad et al.

Supporting Information (SI)

**SI Text. Fraction of Range Reduction and the Effect of Temperature:** The energy consumption per unit distance for each EV is collected from the data of the United States Environmental Protection Agency. The ambient temperature has a significant impact on the rated range and the use of auxiliary components like heaters and air-conditioners at low or high ambient temperatures causes an additional loss in range. The SOC is could have an effect on the discharge efficiency of the battery pack and hence would affect the energy consumption. An aged battery pack would have a lower pack energy, and hence a lower overall rated range. For more details on the impact of each of these variables on short-term impact. The loss in range is determined by the energy consumed by the auxiliary components and the energy consumption of the vehicle at the time instant of the attack. In effect, the fraction of range lost or the ratio of range lost due to a cyber attack and the rated range of the vehicle would be independent of the temperature.

**Parametric Analysis:** Throughout this study, we examine capacity fade considering a quantity defined as ‘vital capacity’ which is equivalent to 20% of the initial capacity of the battery pack. For EVs a degradation of 20% of the initial capacity or 100% of the vital capacity marks the end-of-life of the battery pack [29]. In order to examine the effect of each variable, we select a sample cyber attack defined by a specific workload on the pack conducted for a fixed duration of time. In other words, we fix all the attacker’s control dimensions and constraints. We also fix all other battery pack and environment state variables apart from the variable in consideration, and thereby examine permanent damage as a function of the given variable alone. For examining permanent damage, the first variable considered for analysis is the ambient temperature. The damage to vital capacity is observed to be an exponentially increasing function of ambient temperature and follows the Arrhenius relationship. The parametric analysis summarized in (Fig. S1-S4) are the results of battery pack simulations for attack workloads of one hour comprising of A/C, Lights, Power-Steering and Wipers, for 400 attack-charge cycles. The Constant Current Constant Voltage (CC-CV) charging protocol is followed in each of the simulations.

The effect of ambient temperature on the damage to vital capacity is illustrated in (Fig. S1). The damage to vital capacity follows the Arrhenius equation and within the same analysis, on comparing different workload, we can observe the damage to vital capacity increases linearly as a function of the average power of the workload.

The SOC along with temperature are studied to see their influence on the capacity fade for battery packs of different age, namely 0, 1, and 2-year-old packs as visualized in (Fig. S2). We observe that the damage to vital capacity increases with increase in SOC, in other words, if a cyber attack is conducted on a fully-charged battery pack or a battery pack which is placed in a higher ambient temperature, then the resultant impact would be much greater.

On comparing the SOC-Temperature results for packs of different age, we observe an interesting trend that older packs show a much lower damage to vital capacity with the same specified cyber attack. This can be explained from the fact that the SEI layer modeled shows a growth rate which is a sublinear function of time, and hence the capacity fade or damage to vital capacity decreases for a battery which has already aged for a certain duration.

The effect of total time-of-attack on damage to vital capacity can be seen in (Fig. S3), where we see that the damage is a sub-linear relationship of time. The damage to vital capacity also increases linearly with a reduction in the battery pack size. This could be explained as capacity fade being a linear function of the depth-of-discharge, as seen in (Fig. S4) since a smaller battery pack would have a larger depth of discharge for the same auxiliary component or workload considered, and this corroborates the findings of other studies [32].

**Detectability Index:** The constraints of detectability that need to be examined are shown in (Fig. S5), where we specify a detectability index to each component as a function of time. The methodology for calculating the Detectability Index in is based on the evaluation of three primary detectable indices associated with a given auxiliary component, namely, ‘physical actuation’, ‘dashboard notification’, and changes caused in the environment. For example, a component like an AC would entail a degree of physical actuation which can be detected due to the audibility of the fans and compressors, with dashboard notifications which indicate the component has been engaged, and finally cause a change in temperature and humidity over time. The Detectability Index is examined in two scenarios, either when the user is driving or when the EV is at rest. The
Detectability Index limit is assumed to be five in each case examined in (Fig. S5).

**SI Figures.** The results of the parametric analysis for long-term damage where damage is studied as a function of each variable, the methodology followed to calculate the detectability index is compiled below, and a visualization of the ambient temperature data for the long-term damage simulations can be seen here:

![Graph showing % Damage to Vital Capacity vs Ambient Temperature](image1)

**Fig. S1.** Damage to Vital Capacity as a function of ambient temperature for various auxiliary components, where we observe the Arrhenius type relationship. Each attack workload is run for a time duration of one hour and then subjected to charging with the pack SOC of about 0.7.

![Heatmaps showing damage for different ages](image2)

**Fig. S2.** Bi-variate analysis of the Damage as a function of the SOC and ambient temperature conducted for battery packs of different age (0,1,2 years). The attack workloads are fixed for a time duration of one hour and then subjected to charging.
Fig. S3. Damage to vital capacity studied as a function of the total time of attack for various auxiliary components which shows the sub-linear relationship. Each attack workload has a duration of one hour, and the pack is then subject to charging. The initial SOC of the pack is maintained at 0.7. The inset shows the different workloads that have been simulated.

Fig. S4. Damage to vital capacity studied as a function of the energy consumption of the auxiliary components at an ambient temperature of 40°C. The damage is calculated after 20 days of attack where the battery pack is subjected to the attack workloads of one over and charged after. The initial SOC of the pack is maintained at 0.7.
Fig. S5. The basic flowchart for computing the detectability index of various auxiliary components. We see the three categories into which auxiliary components can be classified into, namely, 'Physical Actuation' which includes component like compressors, wipers which involve a moving component. 'Dashboard/Notification' includes all the components which notify the user about the component being engaged, and lastly the 'Environment' includes components that have an impact on the environment like changes in temperature or humidity. The detectability index values for each of the components is shown with the variable used for categorization where we see two values, the first is the case where the EV is parked and the second where the values are italicized shows the driving scenario.

Fig. S6. The temperature variations in different locations over the year used for the long-term damage studies. The ambient temperature data for each location is incorporated as an average over every week, and the effect of these changes in temperature can be seen in the SEI growth which is quantified in the model.