Colorado State University Libraries
Department of Computer Science
Audio/Visual Materials
Transcription of College of Natural Sciences: 2021 Professor Laureate awards and lecture

Item Metadata
Collection: Audio/Visual Materials
Creator: Jan Nerger, speaker; Wilson, Robert, speaker; Indrakshi Ray, speaker
Title: College of Natural Sciences: 2021 Professor Laureate awards and lecture
Date: May 11, 2021
File Name: COMS_ProfLaureateSpr2021.mp4
Transcript Provided By: Adobe Premiere Pro 2026

BEGIN TRANSCRIPTION

00:00:00:00 - 00:00:24:14
Unknown
Welcome, everybody. It is really. It's great to see everybody. I think everyone knows I'm Jan Nerger, but I serve as the dean of the College of Natural Sciences. It's my pleasure to welcome everyone to the 2021 Professor Laureate Awards ceremony and Lecture. As most of you know, the Professor Laureate is the highest academic title that the college awards.

00:00:24:16 - 00:00:54:08
Unknown
It honors faculty who have made truly outstanding contributions to all areas of the land grant mission. So the excuse me areas of research, teaching and mentoring. Outreach and engagement. Professor laureates are faculty who inspire their students. They make extensive contributions to their discipline, and they devote time and energy to service in the not only in the university, but also their profession and the community at large.

00:00:54:10 - 00:01:26:05
Unknown
This afternoon, we are honoring two of our faculty members with the Professor laureate. Let me change the slide here. There they are. Professor Robert Wilson in the Department of Physics, and Professor Indrakshi Ray, Department of Computer science. So what I'd like to do is say a few words about each of our laureates, and then I'll turn it over to Andrew, and she will be giving her a laureate lecture.

00:01:26:07 - 00:01:56:24
Unknown
So Bob Wilson, Bob is a professor in the Department of Physics, and he's the director of CSU's Program of research and Scholarly excellence in high energy physics and particle astrophysics. He earned his B.S. degree at the University of London and his M.S. and Ph.D. from Purdue. He received postdoctoral training at the Stanford Linear Accelerator Center, and he held a faculty appointment at Boston University before he joined our faculty in 1997.

00:01:57:01 - 00:02:23:14
Unknown
He is taught at all levels of the curriculum and has mentored numerous graduate students through the PhD. He receives enviable teaching evaluations year after year. He's considered one of our most engaging instructors, and he's widely known for his use of state of the art technology in his teaching. In terms of his research, Bob has garnered substantial and continuous external funding for his science.

00:02:23:15 - 00:02:53:11
Unknown
He's brought in more than 19. Oh, look, it doesn't show on that slide. It just says greater than $19 million in external funding from the primarily from the US Department of Energy. He has over 500 refereed scientific and technical publications, more than 43,000 citations. He's co-recipient of the 2016 Breakthrough Prize in Fundamental Physics for his work with the T2K collaboration in Japan.

00:02:53:13 - 00:03:24:03
Unknown
He's currently deputy spokesperson of the Icarus collaboration. That's the Fermilab collaboration of more than 150 scientists, engineers and technical staff from over 23 different institutions. He was also founding member and institution board chair of the 200 institution International Deep Underground Neutrino Experiment, or what we refer to as the Dune collaboration. And again, that has over 100 1100 scientists from over 30 countries.

00:03:24:05 - 00:03:51:21
Unknown
I think you'll agree with me that Bob Wilson clearly worthy of the laureate distinction. So I congratulate you, Bob, and ask if you would like to say a few words. Just say thank you very much. Means a lot to be recognized by my peers in the college, and especially when I look at other professor laureates. Being amongst that number is really an arm.

00:03:51:21 - 00:04:07:01
Unknown
And so I look forward to sharing some of my research with you in a fall. Laureate lecture. Yeah. Thank you. Bob. I think we should all applaud, even though he can't hear us.

00:04:07:03 - 00:04:25:00
Unknown
I'm hoping that when you give your lecture in the fall, we are actually sitting maybe over in the student center. I, I dreams of a university that we can actually go to in person. So let me continue.

00:04:25:02 - 00:04:56:22
Unknown
With our second professor laureate in Doctor Indrakshi Ray in is a professor in the computer science department. She's the director of Colorado Center for cybersecurity at CSU. She's also the site director of

the NSF Industry University Cooperative Research Center for Cybersecurity, Analytics and Automation. She obtained her PhD in information technology from George Mason University, and she joined our faculty as an assistant professor in 2001.

00:04:56:24 - 00:05:26:17
Unknown
Doctor raise an outstanding teacher, and she's mentored more than 15 PhD, 13 M.S., M.S., and 17 undergraduate students in her lab. Her nomination letter refers to her teaching style as a guide on the side, rather than sage on the stage. She sees the role of the teacher as one who steers students into seeking out information from a variety of sources, sort of churning and synthesizing that into knowledge that can last a lifetime.

00:05:26:19 - 00:06:06:03
Unknown
She's taught at all levels of the curriculum. She's been particularly engaged in increasing the representation of women and minorities in computer science, and research interests include software assurance, data analytics, and security. She's published approximately 200 technical papers and refereed journals and conference proceedings. And she's received substantial financial support from agencies including the Air Force Research Laboratory, Air Force Office of Scientific Research, the Naia and NSF, and the US Department of Agriculture, as well as from industries in the US, Norway, and Japan.

00:06:06:05 - 00:06:35:11
Unknown
She serves on several editorial boards, including the IEEE Transactions on Services Computing, the International Journal of Information Security, Computer Standards and Interfaces, and the Arts, IEEE Security and privacy. As part of the Laureate Award, each Professor Laureate delivers a lecture on a subject of his or her choice. Indrakshi is going to deliver her lecture now as soon as I give her the screen.

00:06:35:14 - 00:07:03:19
Unknown
And Doctor Wilson Bob will deliver his lecture in the fall. The title of Indrakshi's lecture is Cybersecurity of Embedded Networks in Heavy Vehicles. I'll stop sharing my slides right now and turn the rest of the hour over to our professor laureate doctor Indrakshi Ray. Congratulations. And.

00:07:03:21 - 00:07:33:10
Unknown
Thank you. Jan, it's. Here is my award. And with the camera, I don't think you can see it well. So it's an honor to be awarded the professor laureate from the College of Natural Sciences, Colorado State University. It has been quite a journey for the past 20 years. I would like to thank the faculty and the staff of the Computer Science department at Colorado State University for being with me throughout the journey.

00:07:33:12 - 00:08:06:07
Unknown

Special thank you to my mentor, Doctor Adele Howe, who is no longer here with us, as well as to my collaborator, Doctor Robert France. A special thanks to my chair, Doctor Daryl Whitley, who has believed in me and supported me throughout most of this process. And to my current chair, Doctor Craig Craig Partridge. Also thanks to Dinagat for, you know, encouraging us and, you know, keeping an open door policy where we can approach her.

00:08:06:09 - 00:08:49:22
Unknown
And a very special thanks to my, you know, friend, collaborator and colleague, doctor. Gosh, whenever there is some rain, you know, he comes and holds them over my head. And, lastly, but not the least, you know, I would like to thank my husband and collaborator and competitor doctor. And with that, I'll start my professor laureate lecture.

00:08:49:24 - 00:08:57:22
Unknown
So today I'm going to talk about cybersecurity of embedded networks in heavy vehicles.

00:08:57:24 - 00:09:06:17
Unknown
Whoops.

00:09:06:18 - 00:09:20:11
Unknown
Sorry about that. Yeah.

00:09:20:13 - 00:09:34:13
Unknown
Just want to just kicked it just now you know.

00:09:34:15 - 00:10:02:11
Unknown
So the Department of Transportation classifies vehicles on the basis of their weight. Heavy vehicles are some of the heavy vehicles you see in this picture. They are vehicles, you know, which are over 26,000 pounds. And for the interest of this lecture, I won't refer to them as heavy vehicles. But, you know, truck, for the sake of simplicity, a few facts about trucks.

00:10:02:13 - 00:10:42:02
Unknown
So trucks carry almost 70% of all US freight by weight. Each year, 800,000 trucks carry hazardous material in any given day. In the United States, a semi truck with a full trailer weighs 80,000 pounds or more. Trucks traveling at 65mph traveled three football fields before coming to a full stop. In 2018, heavy trucks were involved in 121,000 crashes leading to personal injuries, of which there were over 5000 fatalities.

00:10:42:04 - 00:11:15:20
Unknown

And this is not even taking into account cybersecurity incidents. Now, if a cyber security incident were to happen and trucks were stopped, if trucks stopped in day one, we'll have food shortages. Hospitals will run out of medical supplies. Manufacturing comes to a halt if trucks stopped for three days. Then on day three, gas stations run out of fuel, food shortages escalate.

00:11:15:22 - 00:11:51:10
Unknown
Medical waste and hazardous hazardous materials release toxins and jumps into the atmosphere. Public services halted. This means there is no no ambulance, no police, no fire, even in the case of emergencies, if trucks were taken off the road for two weeks, clean water supply nearly exhausted. Hospitals will be without oxygen. So I hope I've been able to impress upon you that trucks constitute a nation's critical infrastructure.

00:11:51:12 - 00:11:58:18
Unknown
So the question is, can we launch cyber attacks on trucks?

00:11:58:20 - 00:12:40:12
Unknown
So let's look at automotive cybersecurity incidents for the past 20 years. So as you can see, the number of cybersecurity incidents have gradually increased. Even if you compare the incidents from 2016 and 2019, the number of cybersecurity incidents in the automotive sector has increased 605%. And the scary part is 82% of these are remote attacks. So which means that they don't need physical access to your vehicles to understand why this may happen.

00:12:40:17 - 00:13:13:21
Unknown
Let's look at the internal structure of modern day automobiles. So almost all the aspects of modern day automobiles are controlled through embedded computers, known as electronic control units, that are connected through various networks. The most important of the networks is the controller area network or the can network for short. So the ECUs communicate with each other by sending signals through the network.

00:13:13:23 - 00:13:49:09
Unknown
The question is how do we interpret these signals. So the cars they use their proprietary and protocol in order to understand the signals. So Tesla will have its own protocol, will have its own protocol in order to interpret the signals and understand the message they are sending. Trucks, on the other hand, have a very open design. They have ECUs manufactured by different companies or OEMs, and so that the different issues can talk with each other.

00:13:49:11 - 00:14:27:17
Unknown
The Society of Automotive Engineer requires that all the issues communicate with each other through an open, standardized protocol, which

is known as the J. 1939 protocol and this J. 1939 protocol are used in heavy vehicles. They are also used in medium weight vehicles that way over 1400 0 pounds in agricultural equipments, in locomotive engines, in marine vessels. So they are pretty much ubiquitous.

00:14:27:19 - 00:14:57:10
Unknown
So now coming back to trucks and cars. So car versus truck which is more vulnerable. So in color you can intercept the messages that are passing between the ECUs. But there's a lot of reverse engineering effort you need to invest in order to understand what what messages are being passed. Cars. Trucks, on the other hand, use a standardized J 1939 protocol.

00:14:57:12 - 00:15:26:15
Unknown
And this, the interpretation of the messages, you know, we all understand the structure and we know how to interpret these messages. So by virtue of using the open standards, if you can intercept the messages that the issues are sending or to each other in a truck, you can very easily interpret those messages. So the next thing is that if there is a single vulnerability in this protocol in the J.

00:15:26:16 - 00:16:10:04
Unknown
1939 protocol, this is scalable. This will be present across all OEMs, across all makes and models. So it is pretty severe. The third thing is that networks on trucks are more readily physically accessible through the trailer frames. So in short, you can inject crafted messages into the network and cause the vehicle to behave. Dangerously, trucks install third party telematics systems and fleet management solutions, which can be compromised, and they provide another source for attacks.

00:16:10:06 - 00:16:51:03
Unknown
The final thing is that trucking industry use are more motivated to use modern applications, such as advanced safety systems, driving automation systems, and these applications again increase the attack surface. In short, trucks are more vulnerable to attacks than cars. So now the question is how do we how do we carry out attacks on on these trucks? The most simplest way is somehow, if you can inject some message into the internal network of the track or alter a message in this network, that that's the easiest way.

00:16:51:04 - 00:17:17:15
Unknown
And now the question is how do we do that? So you have these different ECUs that are manufactured by OEMs. And it is entirely possible for these ECUs to have malware or Trojan through which, you know, they can inject malicious message into the network. The network is also accessible through the OBD to ports, which is originally designed for diagnostic purposes.

00:17:17:21 - 00:17:50:00

Unknown
But you can attach something to these Obd2 ports and inject malicious message into the network. And also you can attack you can send malicious message through the by compromising the telematics unit and unit. So it is not at all hard to compromise the network of the of the truck and send maliciously crafted messages. So with this just to summarize.

00:17:50:02 - 00:18:16:21
Unknown
So the trucks use a protocol which is the J. 1939 protocol that and which is an open standard. And important messages are and data are communicated communicated across the ECUs using this protocol. This protocol is implemented on top of the can. There is no security features designed at any layer. And we have a pretty large attack surface.

00:18:17:02 - 00:18:48:06
Unknown
You can physically access the trucks network or you can through remotely. You can also access the trucks network and launch attacks. So with this background, we, thought of, you know, that whether, you know, actual execution attack can be executed on trucks. So in order to understand this, let's look a little bit deeper. So this is the heavy vehicle in general network architecture.

00:18:48:07 - 00:19:15:10
Unknown
At the lower level you have the physical can network that are transmitting, the bits and on top of which sits the J. 1939 protocol. So this tells you how the message must be interpreted. At the heart of the 1939 protocol is the J. 1939 Protocol Data Unit. So this is the unit along which the messages are transmitted.

00:19:15:14 - 00:19:58:12
Unknown
And there is a identifier part which is 29 bits long. And there is a data part which can vary between 0 to 8 bytes. So the can network is a broadcast bus a medium. And the issues can all transmit maybe at the same time. So the priority bits decide that the of the priority of the messages. So essentially that this means that, you know, if two messages are of differing priorities are transmitted on the bus at the same time, the higher priority message will be transmitted and received before the Lord priority message.

00:19:58:14 - 00:20:25:15
Unknown
So example of a high priority message might be the transmission sending the torque control message to the engine. An example of a low priority message might be the vehicle, road speed that is being sent, which is not very time sensitive. So the next component is the parameter group number or the number. So the messages all have types.

00:20:25:18 - 00:20:51:23
Unknown

So the number tells you the type of that message. And and then we have the source address. This gives you the the source address of the issue that is transmitting this message. And then we have the data components which can be to eight bytes long. And just to give you an example. So the parameter group number you know sort of groups of messages.

00:20:51:23 - 00:21:20:04
Unknown
And there might be a group called the engine temperature. So the corresponding data bytes will have you know will carry the values of these parameters. So what is the engine coolant temperature. What is the full temperature. What is the engine oil temperature. So all these information are in these data bytes that are being transmitted. So there are different kinds of messages that are being transmitted between these issues.

00:21:20:06 - 00:21:55:24
Unknown
Some are periodic periodic messages. And these periodic messages are transmitted periodically at fixed frequencies. And it could be important messages giving the state of the vehicle. Then you can have an event based message. When something some event happens then these messages get transmitted. Messages can also be conditional, which means that, you know, when certain parameter value parameter reaches a particular value, then these messages are transmitted.

00:21:56:01 - 00:22:32:23
Unknown
And then you can have on request. Messages that are transmitted on requesting a, on request. Receiving a request. And typically the messages are broadcast which means that, you know, the ECU is sending the message which can be received by any means and any issue. But sometimes there are destination specific and and sometimes like one issue, might request some specific information from another ECU.

00:22:33:00 - 00:23:00:12
Unknown
So the ECU that is requesting some information from another issue, we call that the requester issue and the issue that is responding. We call that a responded issue. And when the response message cannot be sent in one byte or in the on within eight bytes, then these two issues engage in what is known as a multi packet transfer protocol.

00:23:00:14 - 00:23:32:21
Unknown
So in this the ECU basically sends a request. And this says that you know I need some information from you. The responder sends back a reply with a request to send message. And in this reply it sends important information. For example it will tell the responder issue that the information about I'm about to send you is this many bytes long and it transmits many such important information.

00:23:33:00 - 00:24:02:14
Unknown

So on receiving this information, the requested issue allocates the buffer space and does other housekeeping job. And when it is done it sends clear to send message. And when the responder issue when it receives this clear to send message, it now sends its data bytes, all the information and the requester issue receives the responses and sends an end of message acknowledgment.

00:24:02:16 - 00:24:37:18
Unknown
So for computer scientists, this is not a very complicated protocol at all. And we started taking a look at this protocol and see. And there is no cyber security built in in any way inside the truck. And we try to see that, you know, whether we can, you know, play with this protocol and launch some attacks. So we, we had obtained the a very eager, simple, eager grant through which we came up with a very rudimentary test bed.

00:24:37:24 - 00:25:14:19
Unknown
And in the test bed we had an engine control module which had an engine and which and also a retarder engine, which is found in heavy vehicles and a brake system controller. And we added to big boned blacks. And all of this are connected on the can network. And the big bone blacks, they are you know, they have custom built, heavy vehicle communication protocol transceiver units through which they can send the Jayne send and receive J 1939 messages.

00:25:14:21 - 00:25:57:13
Unknown
And these these ones behaved as the attacker. And so they were impersonating different types of issues. So we made them impersonate the engine one. We made them impersonate the brake controller and also impersonate the of board diagnostic tool. And with that we try to launch the a denial of service attack using the Multi Packet Transfer Protocol. So this attacker kept on bombarding this engine with you know the Multi Packet Transfer Protocol.

00:25:57:15 - 00:26:24:16
Unknown
And as a result of that what we saw was that the we monitored the traffic on the bus and the traffic from the engine as well as the retarder they reduced. There was a significant reduction in the volume of the traffic that were being sent by the engine, both high priority as well as low priority, as well as those from the retarder engine.

00:26:24:18 - 00:26:53:19
Unknown
There was an increase in the brake traffic. And now, in order to understand what was happening, I. So we have this issue one which was the engine, and we have the issue two which was the malicious attacker. And then we had a nice issue which we referred to as issue three. So initially nothing was happening. And the issue one was, you know, regularly transmitting periodic messages.

00:26:53:21 - 00:27:24:08

Unknown
And then the malicious attacker sends a request message to the engine. And this request message requires the engine to execute a multi, a multi packet transfer protocol. And the issue one was behaving, you know, still sending its periodic messages. And you know it was receiving more request. And it was also able to respond. And this went on happening for some time.

00:27:24:10 - 00:27:59:11
Unknown
And finally the echo two bombarded the engine one with such request. And after a while this engine failed to respond to requests such request. And it failed to send periodic messages as well. And then a genuine issue sent a genuine request. Unfortunately, the engine was not able to respond to that either. So in short, we were able to launch a denial of service attack on this protocol.

00:27:59:14 - 00:28:28:14
Unknown
So we carried out some such similar protocols on our very simple testbed, and we published a paper in a security conference. And the following year we were invited to the Cybertruck Challenge conference in 2017. And we were able to launch some of these attacks on 2017 trucks, you know, manufactured by the commercial sector for the purpose of NDA.

00:28:28:19 - 00:28:59:08
Unknown
I can't disclose you the name, and we were able to launch some of these attacks. And seeing that the Society of Automotive Engineers had to kind of, you know, revise its specification for the J. 1939 protocol. So in some sense, we feel that, you know, this work has had some impact in the real world. So now that we've been able to demonstrate attacks on heavy vehicles, the next question is how do we attacks?

00:28:59:10 - 00:29:30:17
Unknown
So there are two challenges for detecting such attacks. One is that real time attack detection techniques are needed because the vehicle is operational. It's running. So we need to detect the attacks in real time and take some corrective measure. And the other thing is we need to distinguish between security events and safety critical events. So the oftentimes, you know, there are heartbreaking and other kinds of safety critical events happening in the vehicle.

00:29:30:21 - 00:30:00:19
Unknown
So we need to distinguish between safety and security. So to understand this, what we did was we tried looking at the messages that were being sent by on the network. And some of these, we have different kinds of messages. And some of these messages were carrying data inside. And these data gave you the state information of the vehicle.

00:30:00:21 - 00:30:37:14
Unknown

And we call such messages report. And so this shows 1515 seconds of drive cycle. And we tried to capture the important reports. And so there were six important reports happening. And we tried to order them. And so there were 63 times report one immediately followed report zero. 76 times report to immediately followed report one. And we drew what is known as a report precedence graph.

00:30:37:16 - 00:31:07:22
Unknown
So we drew this report precedence graph from, you know, actual drive cycles. And we executed some, high RPN command injection. Messages to the engine. So what we did was we injected, some malicious message into the bus at different periods of the drive cycle, the start, medium and end of the drive cycles at different frequencies and for different durations.

00:31:07:24 - 00:31:45:23
Unknown
And we observed the report precedence graph. And if you can compare the two graphs, you will see that there is a lot of randomness in the in the graph where message injection took place. And so we tried to quantify this randomness using some metrics. And the two metrics that we used. One was natural normalized graph flux capacity, which essentially is a measure of the number of average number of units measure centered around the number of edges leaving, entering and leaving a node.

00:31:46:00 - 00:32:20:07
Unknown
And we also look at edge distribution, skewness, and with these two measures. And we sampled the sample it every one second and drew a report precedence graph. We built a report precedence graph every second. And the reason for choosing the sample is sampling rate is one second, because most of the important vehicle vehicle parameters are transmitted at a frequency that is much less than one seconds.

00:32:20:09 - 00:32:54:13
Unknown
And so we drew the graph and we computed the, these two randomness measure the NGF C and the as, as distribution weight skewness. And we computed those measures and we basically compared them with 30 of the past values. And we chose a confidence interval and detected, you know, whether there was an outlier or not. And we tried this on two data sets that can work can work.

00:32:54:13 - 00:33:27:12
Unknown
And the Peterbilt data sets and our results are were very promising in the 80 to 90% confidence level. We were able to detect most of these attacks. Having said that, the biggest question is that, you know, can we detect such attacks in real time? And what we found was the major time is the the number of nodes in such the report precedence graph.

00:33:27:14 - 00:33:59:12
Unknown

And when we looked at the number of reports in the entire drive cycle, we had at most 45 reports and 25 reports for 400 and 10s and 74 seconds, respectively. So for one second, the number of reports will be far fewer. So this makes us feel optimistic that, you know, such an intrusion detection system will be able to meet the real time requirements of the of attack detection.

00:33:59:14 - 00:34:31:17
Unknown
So now that, you know, attacks can be detected, you know, how can we, you know, provide visualization aid to the heavy vehicle operator so that they can take some corrective measures in some real time. So a number of reports are being generated at very fast frequency. And clearly, you know, cognitively, human beings are not designed to process so much information that is being generated at such high speeds.

00:34:31:19 - 00:35:00:24
Unknown
So the important thing is we have to make the vehicle operator aware of some critical states in the system that we are reaching, and the critical states are not coming from just one message, but they are coming from, multiple such messages. So one such example is say clutch damage. So in one of the report. So this value 190 is basically tells you it's the RPM.

00:35:01:01 - 00:35:31:03
Unknown
So in one message you get the value of the high RPM. So the the value of the RPM should be between 3000 and 8000. And in a separate message that is, you know, transmitted by a different ECU by the transmission, the the gear value must be between 0 to 50. So when these two events happen, you know, in close succession, then we know that a clutch damage has occurred.

00:35:31:05 - 00:35:59:12
Unknown
So here what we were trying to see is that look at some security critical and safety critical states and give warnings in real time to the vehicle operator. So we were looking at the engine break, disable disable attack. And this attack happens when the parameter 518 has a value of 0.0. And when this parameter 84 has a value between 0 to 30.

00:35:59:14 - 00:36:27:10
Unknown
And then we were looking at the sudden high acceleration demand attack. When this parameter 91 has this value, this set of values, or when, this parameter 559 has a value of one, and when the parameter 84 has a value between 0 to 40. And so messages are coming. So at t one, you know, this message comes and we see that the parameter 518 has this value zero.

00:36:27:12 - 00:36:55:11
Unknown
So which tells me that this parameter has been affected. S1 and S2 are both still in the non-active stage. Because S1 requires both these parameters to be affected in order to become active. Now in time t2, this

message comes and now this parameter 84. You know, has affected this one because a value 15 lies between 0 and 30.

00:36:55:17 - 00:37:30:23
Unknown
And it has also affected this one because 15 is between 0 and 40. So now both the parameters required for enabling state S1 have appeared. And so S1 goes into the active state S2 is still not active at time t three. The parameter 518 gets a new value of one, which basically resets this value. So S1 again goes into the non not active state, and S2 is also in the not active state at a time.

00:37:31:02 - 00:38:00:13
Unknown
T4. This message comes and now you know these two parameters get affected. And so now S2 goes into the active state. So we built basically a system that does such detection. And we are providing visualization aid to the vehicle operator. So the gray value means that you know both S1 and S2 are inactive. In the next state S1 becomes activated.

00:38:00:13 - 00:38:33:03
Unknown
That is indicated by this red color. And in the following state both are inactive. But this is just to indicate that S1 was activated in the previous state. So the blue color signifies that. So we built a system which does this detection. And essentially the complexity of the system depends on the number of states that you are trying to detect and the number of parameters associated associated with those states and the range of values that they can take.

00:38:33:05 - 00:39:15:17
Unknown
So this is our work on state visualization. So very recently we have been working with the statistics department on predictive analytics. And here what we are trying to understand is that number of different parameters are being transmitted at the same time. Is there a correlation or a causation between these different parameters. And here there are two questions that we are trying to essentially ask that if we know a parameter is passed value, can we predict its current value.

00:39:15:19 - 00:39:48:05
Unknown
So that is the first question that we are trying to ask. And in this we used you know, we looked at boost pressure prediction and we looked at statistical approaches as well as one neuro neural network approaches approach. The blue solid line shows the actual value of the parameter and the dotted line, the orange and the green and the red dotted lines are the other statistical approaches.

00:39:48:05 - 00:40:22:04
Unknown
And the purple line is basically the neural network approach. And we find the statistical methods that we use will repeat linear interpolation and cubic interpolation. We find that the static, static technique, the

statistical technique works well in regions where there is low variability, but in regions of high variability we see these peaks and valleys. The neural network we use, the LSTM method works the works best.

00:40:22:06 - 00:40:50:05
Unknown
And so in sense for certain parameters we can see that, you know taking their past values we can predict some of the future values. So the next question is that that suppose a sensor were to be compromised. Can we use other sensor values values or other parameter values to predict the value of a sensor. And for that again we stick with the boost pressure.

00:40:50:08 - 00:41:23:05
Unknown
And it turns out that the past values of all these other five parameters are a better indicator of the future value of the boost pressure than boost pressure itself. And here we have a graph which actually explains that. So this solid blue line is the actual value. And this orange line is basically a is a value that we are computing, taking into account the parameter values of these other five parameters.

00:41:23:07 - 00:41:50:11
Unknown
So this result is also very encouraging. So if some sensor were to be compromised we can use other values to extrapolate it. So all of this appears to be promising. And we also fully understand that, you know, this is not going to work for all parameters, only for certain parameters. And we are right now investigating what we can do with that.

00:41:50:13 - 00:42:18:24
Unknown
So our few, our future directions are in the area of heavy vehicle security are as follows. We are working on predictive analytics together with the statisticians at Colorado State University. And and seeing, you know, which parameters can be predicted and you know, how how the different techniques are faring. So that is one work we are currently engaging in.

00:42:19:01 - 00:43:05:08
Unknown
The other one is trucks have a very flat network in. And what I mean by that is very easily you can inject malicious message into the network and cause, a truck to, you know, behave weirdly. Now, if we can segment the network into components so that even if we were to inject message and, and have, you know, gateways or British bridges across these components, that way, you know, the effect of injecting malicious message is more localized and does not impact the major components and the safety of the vehicle.

00:43:05:11 - 00:43:40:07
Unknown
That is another, area that we are currently investigating. We are also looking at intrusion detection systems of a and here we are looking at both analytical approaches as well as machine learning approaches to

doing intrusion detection. And we are also focusing on cyber resiliency of heavy vehicles. We believe that, you know, not not all attacks can be prevented or even detected in a timely manner.

00:43:40:09 - 00:44:17:18
Unknown
So how can we make the function, you know, how can we sort of, you know, how can we contain the damage and provide reduce functionality and make the vehicle, you know, reach a safe state so that these are some of the directions in which we are investing our current efforts. And our original sponsor of this work was a eager grant from the National Science Foundation, which was followed up by the C program.

00:44:17:20 - 00:44:53:21
Unknown
And I must thank my sponsors and the students who have done this work. I would like to give them a thanks and acknowledgment. Mukherjee, he's very passionate about heavy vehicle security. He's been he's helped me a lot in understanding, you know, how heavy vehicles actually work. I'd like to thank my student, Hossein Shirazi and William Picard, who are helping me understand machine learning and data analytics of heavy vehicles.

00:44:53:23 - 00:45:24:10
Unknown
And I also would like to thank, Jacob Walker, who was who's the first who was a first generation student, freshman student. We hired him through our REU and he graduated in three years. He's now part of the auto Isac, which is a information sharing. Committee for Automotive Vehicles. So he's been hired by Auto Isaac. And I would also like to thank doctor Jeremy Daly.

00:45:24:12 - 00:45:53:08
Unknown
Back when we started this project, he was a faculty in the mechanical engineering at the University of Tulsa. And, right now, he's a faculty in the systems engineering department at Colorado State University. I would also like to thank the Neft and National Motor Frac Fred Truck Association. And they are very much invested in our work.

00:45:53:10 - 00:46:31:09
Unknown
And, they are they we have a half yearly meetings in which, all the major Cybertruck companies are, you know, attend. And we get to present our results and we get to do a lot of information sharing. And very recently, the Army has also showed interest in, this work. And, because Jane 39, the variation of that is used in is milk and, and that is used by the US Army itself.

00:46:31:11 - 00:47:02:22
Unknown
So with that I conclude my talk. So thank you. Thank you. And fascinating. We have we have about ten minutes for questions. Maybe if you just raise hands or speak out. I'm not sure about how best to do

this, but any questions? Looks like Joseph devotee might have one. Yes, Jan. Thank you. Wonderful work in Rashi.

00:47:03:03 - 00:47:33:14
Unknown
I'm curious whether or not the, the attacks that you are analyzing and studying have any bearing on the attacks of the Stuxnet that were used a few years ago on the Iranian centrifuges. Wondering whether they have a can network associated with them and whether that has any, any, any bearing whatsoever. So, the attacks that we carried out are extremely, extremely simple.

00:47:33:16 - 00:47:55:20
Unknown
So that is, you know, and that makes the problem very scary. So when we started this project, you know, we were looking at IT networks because, you know, we are computer science people. And we thought that, you know, there are a lot of attacks that are launched on the IT networks even. Can such attacks happen in heavy vehicles.

00:47:55:22 - 00:48:19:14
Unknown
And so we we started with that. It has much less you know, it's it's not at all sophisticated at all. You know, it's it's very, very rudimentary and very simple. What is very alarming is that we were able to carry out this attacks on the trucks. And this was the this was what we did in the very first year.

00:48:19:16 - 00:48:51:08
Unknown
In the second year, we have another first generation, first generation diversity student. You know, he basically, so the so, we had a first generation student and, you know, he wanted to participate in the Cybertruck challenge. He had no background on any Cybertruck. He was like, you know, taking my database class, and I don't believe he even took a security course, you know, and he just looked over some of the materials.

00:48:51:08 - 00:49:18:10
Unknown
He studied for them for two days, and he went to the Cybertruck challenge competition. And, so, and they just give some training for a day. And with this three days of training, you know, he actually broke into the telematics unit and, you know, were able to hack into the, into the, into the truck. So which, you know, tells you how very scary the situation is.

00:49:18:12 - 00:49:54:18
Unknown
I mean, it's just a that's such an attack has not yet happened. It's it's extremely simple actually. And the other thing is the other thing that is like, you know, really, really scaring us a lot is that people have begun to talk about hybrid vehicles where hybrid hybrid trucks. So you can very easily, you know, give messages and divert and, you know, and they have

it has like, you know, driver to all the trucks to one station and cause, you know, blackouts and things like that.

00:49:54:20 - 00:50:17:09
Unknown
It is the ease with which we can launch these attacks. You know, that is the most scary parts. You know, it's not at all sophisticated at all and does not require much, you know, advanced planning and unlike, you know, the softness or even the attacks that are happening in other sectors, you know, where it's very long drawn process.

00:50:17:11 - 00:50:45:13
Unknown
So in, in this J. 1939 protocol, it's clearly very vulnerable. Is that is that also are similar protocol used used in aircraft and maybe even like power plants or you know, just seems like this could be a real national security threat. It is a national security issue. They are used. The aircraft's icon, but they're definitely used in marine vessels.

00:50:45:15 - 00:51:02:22
Unknown
Marine vessels are used in the agricultural equipment used by locomotives, used by, you know, variation of it is used by RV. It's called the RV. Can, Army Army tanks. It's very ubiquitous.

00:51:02:24 - 00:51:22:15
Unknown
So military. That's what you were saying has shown some great interest? I would think so. Exactly. And only I think two days back, you know, actually, yesterday we just submitted the white paper, and they're also funding my NSF Iasi Arc Center. We showed them and and part of the predictive analytics work we've given, we had given them a presentation.

00:51:22:20 - 00:51:43:05
Unknown
And part of the work is inspired through them. You know, they said that is it possible that we sort of attack, you know, if one sensor gets compromised, can be predict. So they are very much interested in our, you know, in this work and. Yeah.

00:51:43:07 - 00:51:49:07
Unknown
Are there any any other questions?

00:51:49:09 - 00:52:25:11
Unknown
I have one more but I'll see if anybody else. So I, I actually have one question. So that you, one question that I have is that, you know, you attacked the J 1939 protocol. Now does this attack also transfer to the underlying Can protocol, which is a main constituent protocol for many industrial control systems. So, so the so basically we looked at the message semantics and we can so now we've understood, you know, how the J.

00:52:25:12 - 00:52:57:15
Unknown
1939 works and how it can be attacked now in the industrial control systems. You know, we of course. Do not use the J 1939, but we might be using a similar protocol. And if we and we can study those protocols and see whether, you know, they have such abilities as well. And and very recently, you know, we are also working with, together with the Energy Institute, we are looking at some of the protocols that are being used in the energy sector.

00:52:57:16 - 00:53:21:13
Unknown
And, you know, they are coming up with their own standard, which is called the IEC 61850. And we are looking for vulnerabilities in those protocols as well. So, so I guess once we interpret the message and we, once we understand the specific protocols, you know, maybe these work also apply.

00:53:21:15 - 00:53:38:10
Unknown
Is there a way to inject some more cyber security into the protocol remotely, or do you have to go in and just swap out hardware? So you're saying about defense mechanisms.

00:53:38:12 - 00:54:13:06
Unknown
Just to improve the protocol that's used in these control systems, is that something that can be remotely done, like on my Tesla? No, it's over-the-air updates of the software. But for these simpler modules, you literally have to go to each truck and change the hardware or. Exactly. And that has important implications actually. So and one of the implication is that, you know, we are sending we have this eight byte message which we are transmitting.

00:54:13:11 - 00:54:42:18
Unknown
Now, if we are to implement some, say, cryptographic mechanisms, then all year you are sending something in, say one message. Now you will require multiple messages to be sent. And so that has implications on the timeliness aspect of the various components of the system as well. So so that is a bit challenging coming back to your Tesla and heavy vehicles.

00:54:42:19 - 00:55:08:15
Unknown
You know, there is another very significant difference between cars and trucks. And one of the difference is that you can very easily install, install, and I guess Tesla and some of the companies, many companies are doing so an intrusion detection system. So when the car is ready to be shipped out, you know. Exactly. You know how the like you have the data.

00:55:08:17 - 00:55:33:00
Unknown
And so you can have machine learning algorithms which, you know, profiles the behavior and detects detect anomalies behavior in in trucks the

design is very open ended, which means that you buy the truck and, you know, maybe five years from now you plug in another issue. So the design is very open. And so you plug in another issue.

00:55:33:01 - 00:55:57:16
Unknown
So now the machine learning, you know those other anomaly detection no longer work actually. Because you know, you can keep on upgrading your truck much later on. And so then there is a dynamic, you know, address allocation that is happening. So which essentially pose some technical challenges. Cars, on the other hand, you know, Tesla is in total control.

00:55:57:16 - 00:56:12:24
Unknown
They can, you know, swap out things. They can do everything. But here because of the open ended nature of things, there are some additional challenges that must be kind of, you know, overcome.

00:56:13:01 - 00:56:37:03
Unknown
Well, I think, I'll just say I'll kind of close our, our afternoon by saying thank you and drop it was a fascinating talk. I look forward to seeing where the work goes. I mean, this is really, really very interesting. I want to congratulate both of our laureates and thank everybody for being here. And then finally, I want to thank Aubrey Kent from my office, who organized this and made sure we could all get together rather seamlessly.

00:56:37:09 - 00:56:58:05
Unknown
So I hope I see you all in for the second Professor Laureate lecture, which Bob Wilson will provide in the fall. We don't have a date set up for that yet, but it'll be along with the teaching, teaching and mentoring awards of the college. And I wish you well for the rest of your evening, and let's hope we can get together soon.

00:56:58:05 - 00:57:03:24
Unknown
I hope you're all staying safe and that your families are as well. So thank you all for attending. Appreciate it.

END TRANSCRIPTION