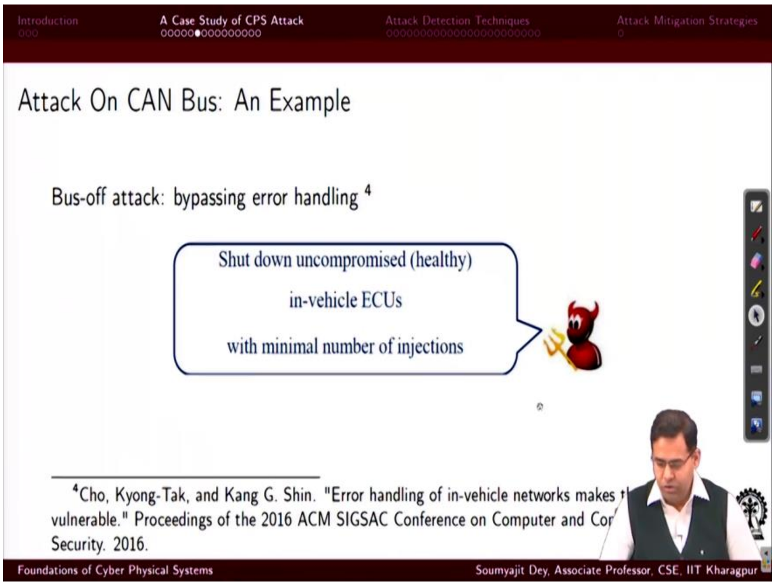
Foundations of Cyber Physical Systems

Prof. Soumyajit Dey
Department of Computer Science and Engineering
Indian Institute of Technology – Kharagpur

Lecture – 53
Attack Detection and Mitigation in CPS (Continued)

Welcome back to this lecture series on Cyber Physical Systems.

(Refer Slide Time: 00:32)



Introduction
A Case Study of CPS Attack
Attack Detection Techniques
Attack Mitigation Strategies

Attack On CAN Bus: An Example

Bus-off attack: bypassing error handling [4]

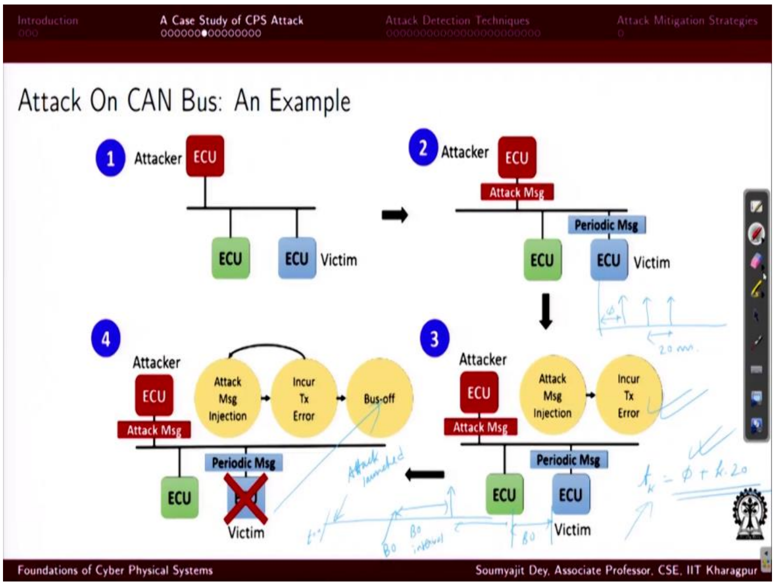
Shut down uncompromised (healthy) in-vehicle ECUs with minimal number of injections

[4] Cho, Kyong-Tak, and Kang G. Shin. "Error handling of in-vehicle networks makes t vulnerable." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Cor Security. 2016.

Foundations of Cyber Physical Systems
Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

If you remember in the last lecture, we were talking about bus-off attacks on CAN buses. right And we established that what can be the objective of the attack and we will now ah try to discuss the algorithm which is to be implemented by this malicious node.

(Refer Slide Time: 00:44)



Introduction | A Case Study of CPS Attack | Attack Detection Techniques | Attack Mitigation Strategies

Attack On CAN Bus: An Example

Foundations of Cyber Physical Systems | Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

And see that how the data can happen in real life. So, we are trying to show that well, let us say this is one attacker ECU. OK And is going to push in some attack message on the bus and let us say this is a victim ECU whom this attacker is targeting. And this victim ECU is generating periodic messages which are valid real messages. Ok Now, ah what can happen is let us say this attack messages and this periodic messages are having the same ID.

It is precisely that is what the attacker is targeting. It is targeting to replace this periodic messages of the victim ECU with it is own messages. So, this can be done in such a way, ah that this ah due to the attack message injection there will be transmission errors. Now, there is a problem here. Let us understand ah that it is not really easy also. The attacker will need to identify exactly at what time the victim's values are coming.

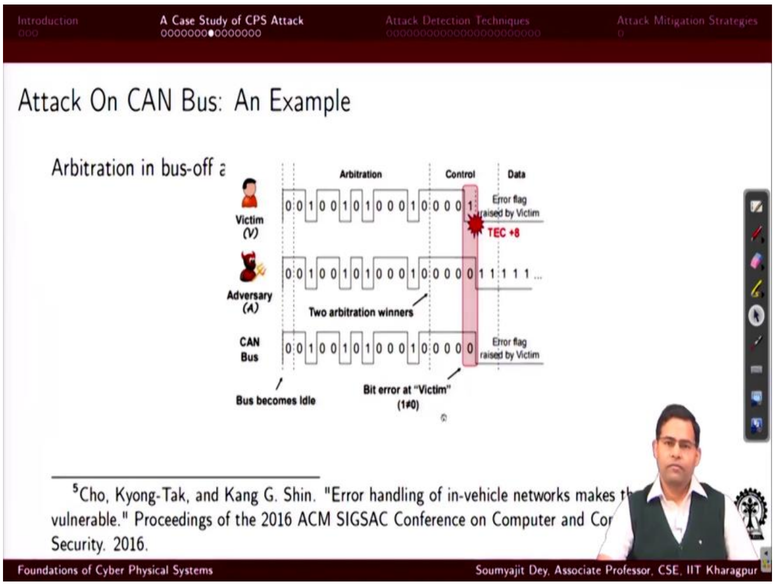
So, let us say it is a timeline and the victim is sending these messages periodically ah with a period of let us say, 20 millisecond. So, this is a periodic data stream and there may be an offset. right So, I mean, let us say the first value started with the period. I mean, of course Ah the first value may have of may have a phase like phi. So, let us say every kth message ah the transmission time is this phi Ah plus k times 20. Right

The ECU is this phi is unknown to the attacker. So, what is important is the attacker needs to first synchronize with this victim ECU. So, there are techniques for doing that. We are not discussing that here. So, once data guard has synchronized with this victim ECU, it should be able to send messages exactly at those time instance. Now, once it is able to send messages exactly at those time instance, so, you have two messages coming. right at the same time, with the same content, the attacker will force a transmission error. ok Now, like we said that with multiple such transmission errors, this victim is used transmission error counts with increase and this will go to the bus-off mode. right So that is that is what the attacker is targeting and why, for the time being, for an interval up to which Ah so, let us say here, things were fine.

And here an attack was launched and at this point this ECU goes to bus-off mode. And this is the bus off interval, after which this ECU is back online. ok So, inside this bus off interval, the attacker is mimicking messages of this victim ECU with malicious messages. So, this entire thing can start happening again. Right Again, there will be an attack window and again there will be a bus off period, etcetera, etcetera. right.

So, if the attacker is smartly able to increase the bus off period and do this attack very often, there may be issues with the system. Of course, modern day CAN systems have known how to have learn how to bypass this kind of vulnerabilities and they can prevent such attacks. But well some some issues still remain Ah so that is why this attack class is really important.

(Refer Slide Time: 04:19)



Introduction | A Case Study of CPS Attack | Attack Detection Techniques | Attack Mitigation Strategies

Attack On CAN Bus: An Example

Arbitration in bus-off a

[5] Cho, Kyong-Tak, and Kang G. Shin. "Error handling of in-vehicle networks makes t vulnerable." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Cor Security. 2016.

Foundations of Cyber Physical Systems | Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

So, let us first understand this issue of how the attacker will force the victim ah to increases transmission error count. So, let us say this victim is transmitting his data stream and there is this adversary who is transmitting the data stream and here is the CAN bus ok. The bus is idle here. What the victim is trying to do is he is trying to mimic the adversaries transmission data stream.

And the first task of the victim definitely is that he will have to synchronize with this first task for the adversary is that we have to synchronize with the victims, transmission, timings. OK And then ah there will be a time when it is sure that it has got itself fully synchronized and when, at that time, ah when the victim is transmitting a message. Ah Then this adversary will start transmitting a sequence of zeros. Ok

So, basically, this is the point we are talking about that when one arbitration phase is beginning. And at this point this adversary the adversary is transmitting a sequence of zeros the idea is that well it has to win the arbitration. ok So, ah the adversary is essentially forcing the victim to lose out the arbitration by transmitting a lower priority Ah identifier which is having more zeros. And due to this, the victim will eventually lose it is arbitration.

And that is why it is TEC count will go to a plus 8 because this is not really ah fair, win. right Because they are they are trying to go start with 2 ah 2 ID's, ah where the adversary has to try to kind of assume the victim's ID but with more number of zeros here. ok So, it will lose the arbitration the victim will lose the arbitration and after that ah what will happen is ah um Fine. ah Whatever the adversary is sending, those values will be going. Right

So, let us again understand the process. Initially, ah the attacker will synchronize with the victim and then there will be the original arbitration phase with every other node who wants to ah wants to participate. What this adversary is doing is he is using the same idea as the victim and using that idea the victim ah will be wining let us say the arbitration at some stage with respect to some other lower priority messages by other ECUs.

And the adversary is also winning that arbitration stage. Let us understand this because this is not how the original CAN system is designed. right Because in the original CAN system, a designer who wants his system to work, he will never have ah same ID for different messages in the system coming from different ECUs like that. But this is the adversarial scenario, right. So, the adversary, who is sitting in some ECU will actually force the situation.

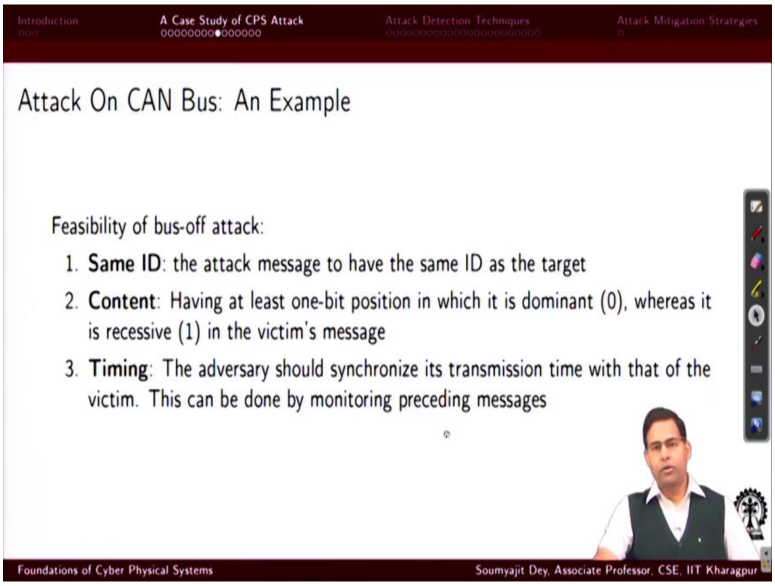
Or who is sitting in a newly attached malicious ECU ah coming from rogue service centre stuff like that or due to some code download which should have should not have happened. ah He is trying to send messages with exactly the same ID as the victim. right So, due to this, what happens is whenever the victim wins arbitration, with respect to other competing messages, the adversary is also winning the arbitration.

So, after this arbitration win, what they are doing is whatever message the victim is sending the can on the CAN the adversary will send a stream of zeros. Now, let us understand that it is not that the CAN bus is going to check for arbitration at some specific phase and then it will transmit message. It is a simple to wear connection. Right So, it is always in AND mode that the arbitration happens right at the physical layer itself. There is no software logic.

So, even the post arbitration phase, when there are two actual winners which should not have been the case even when the payload transmission is happening. The arbitration physics is still there. right So, due to this arbitration physics of the bus for the for the real payload transmission, even in that phase, due to the adversary is sending a stream of zeros it will eventually win and the victim will receive a transmission error.

And due to this transmission error, it is error flag will the transmission error count will go by a plus 8. right ah Because here the victim can see that it was transmitting a 1 but the adversary transmitted as 0 and that is why, ah this bit error happened here. Right

(Refer Slide Time: 08:58)


Introduction
A Case Study of CPS Attack
Attack Detection Techniques
Attack Mitigation Strategies

Attack On CAN Bus: An Example

Feasibility of bus-off attack:

1. **Same ID**: the attack message to have the same ID as the target
2. **Content**: Having at least one-bit position in which it is dominant (0), whereas it is recessive (1) in the victim's message
3. **Timing**: The adversary should synchronize its transmission time with that of the victim. This can be done by monitoring preceding messages

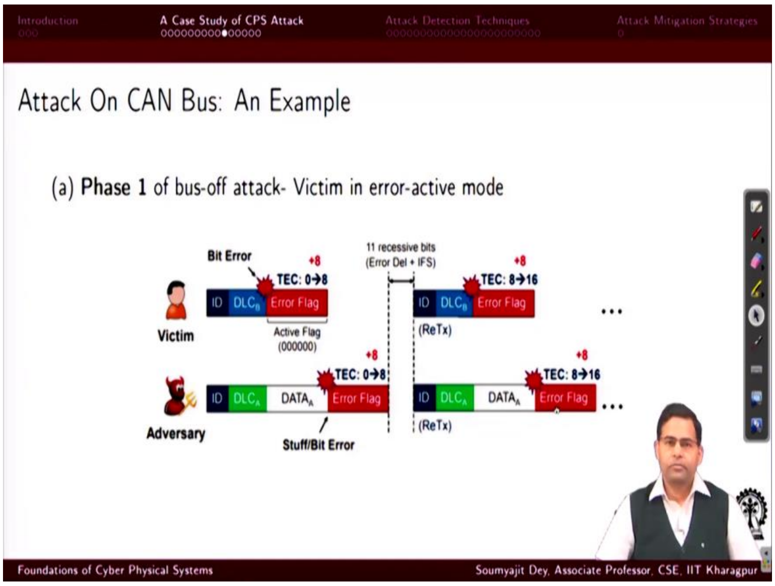
Foundations of Cyber Physical Systems
Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

So, let us understand the feasibility of this attack. The attack message will have the same idea as the target and the content of the message ah which is in that which is inside the attack message will have at least one bit position in which it is dominant, whereas ah the victim's message is recessive. So, let us understand that whatever was I am repeating maybe third time is this is also an arbitration but happening in the place where only the payload was supposed to be there that is, the content was supposed to be there. The original arbitration has already happened. And unfortunately, due to this adversaries present, there are two winners here with respect to the other messages. ok Now, in the in the payload part, the contents are almost same but the ah there is at least one bit position where, ah the adversary is dominant. Right

So, this is what the adversary is aiming at ah but what is important is that necessary needs to synchronize. It is transmission time with that of the victim that means, in order for this thing to happen, this is not very trivial. We are just speaking at a model and slide level but let us understand this is also this requires significant hardware expertise and significant inside of the real time system, when the packets are scheduled how to push in a higher priority, using using scheduling tricks like higher and lower priority. It is possible for the adversary to actually synchronize with the victim at some specific points and attain this thing that it should be it is sending ah sending values exactly the at the point where the victim is also sending. OK right So, ah the by what I am trying to say is this needs to be done and it is difficult but it can be done.

The adversary can synchronize it is transmissions with that of the victim. Ah And the method at a high level is that it will kind of monitor the preceding messages and try to figure out when exactly it should be injecting it is attack payload.

(Refer Slide Time: 11:00)



Introduction | A Case Study of CPS Attack | Attack Detection Techniques | Attack Mitigation Strategies

Attack On CAN Bus: An Example

(a) **Phase 1** of bus-off attack- Victim in error-active mode

Foundations of Cyber Physical Systems

Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

So now, let us go deeper into this situation. We have already said that there will be a transmission error count. right But that is not the end of the story, the story is much more complex. So, this is what we are talking about that at the length of this DLC there is this bit error. The transmission error count of the victim is going ah I mean increasing by 1 ah by 8. Right So, TEC count increases by a plus 8. By the way this this attack is kind of detailed in this paper which was published in 2016 CCS.

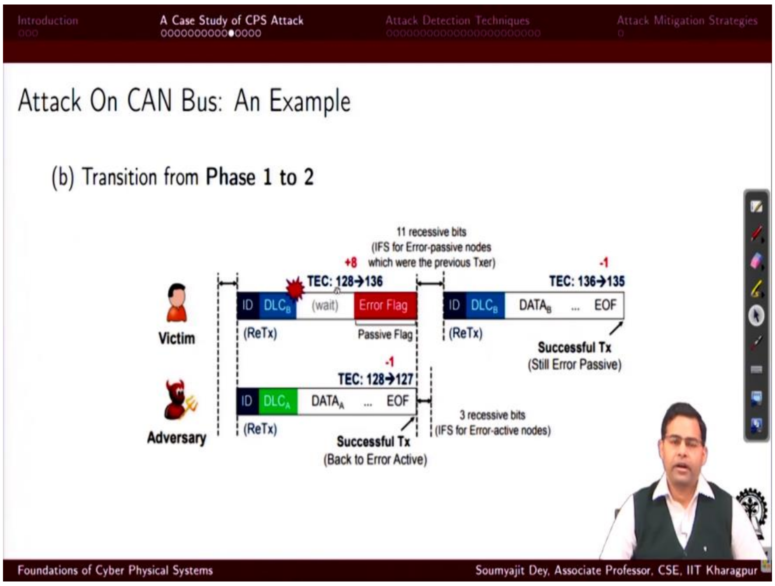
So, ah the TEC count goes plus 8 here for the victim but is that all? No. When this happens by the CAN protocol. ah What happens is the victim will kind of ah emit an active flag? Ah The error active flag which is the sequence of all zeros. Ok And now, due to this, ah what will happen is that the adversary? If it is doing any transmission now this will be ANDed with this sequence of zeros. And due to that ah this transmission error I mean it will also have another flag. Right

Because now, ah it is getting ended with the zeros that are here. right So, what will happen is the adversary ah will now have a transmission error. So, the adversary is transmission error count will increase by a plus 8. right so So that is fine, Ah there will be a plus 8 here and the adversary will also have a plus 8 here. But let us understand that they are not happening together. This is happening afterwards for the adversary.

Because this is this is a reaction to the error active flag from the victim, when ah this sequence of 0s get ended with some 1 that the adversary is transmitting. ok So, at this point, what will happen is there will be an 11 recessive bits transmitted the error frame as per the CAN protocol and then the inter frame space will be maintained. And then again the transmission cycle will increase.

And let let us say that the malicious node will it has it is software right and it will just ah repeat this process. So, while repeating this process, the victims transmission count will again increase. And the adversary is transmission count will again increase. So, both of them are having a plus 8 increase but for the victim is have it is happening earlier and for the adversary it is happening later on.

(Refer Slide Time: 13:27)



Introduction A Case Study of CPS Attack Attack Detection Techniques Attack Mitigation Strategies

Attack On CAN Bus: An Example

(b) Transition from **Phase 1 to 2**

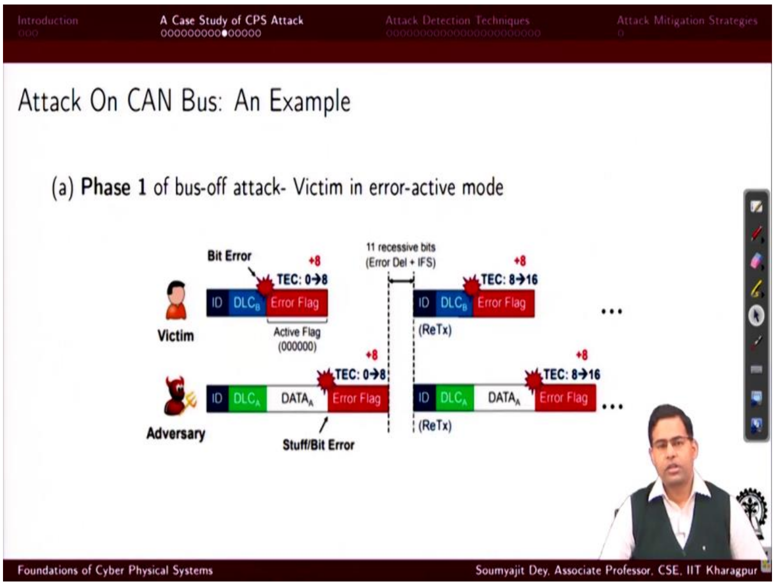
Foundations of Cyber Physical Systems Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

Now, this would mean for both of them at some point ah they will reach 128 right ah because ah see 128 is of course divisible by 8. So, both of them will reach 128 and then again, when the attack will repeat, the transmission count for the victim will go from 128 to a plus 8 that is 136. Now, this is the important phase of the attack, this is phase two of the attack. So, this is all the phase 1 in which both of them start doing plus 8 increase in TEC.

And then we have a time when 1 is both of them one of them is sitting at 128 and the other has also received 128. And the victim again goes to a plus 8 but now this is phase 2 of the attack. When what happens is this moves from 128 to 136. Now, this is important, if you remember the original automaton of this protocol. We said that when this is beyond 127, ah beyond beyond 128. right ah So that is like it is moving from the error active through the error passive mode.

So, here, ah as you can see that why, when this goes from 128 to 136, ah victim is following that original automata and it is moving from an error active phase to a error passive phase.

(Refer Slide Time: 14:47)



Introduction A Case Study of CPS Attack Attack Detection Techniques Attack Mitigation Strategies

Attack On CAN Bus: An Example

(a) **Phase 1** of bus-off attack- Victim in error-active mode

Foundations of Cyber Physical Systems Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

Now, what is the difference that is coming out of this? The difference is when it was in error active state due to which error it was sending an active flag which was a sequence of zeros here. right But now, while it is in the passive place, it will send a passive error flag which is not such a sequence of zeros. And it does not dominate the adversary is any future message.

So, due to that I do not have any sequence of zeros coming, this is a passive flag. So, whatever transmission the adversary is doing now, will be fine. OK And since that is fine, ah well ah there will be no more plus 8 increase in the transmission error count of the adversary. Rather, it will be successful and due to that the transmission error count will decrease by 1. right So So, at this point, what will happen is this stage in 136 and this stage in 127. Ok

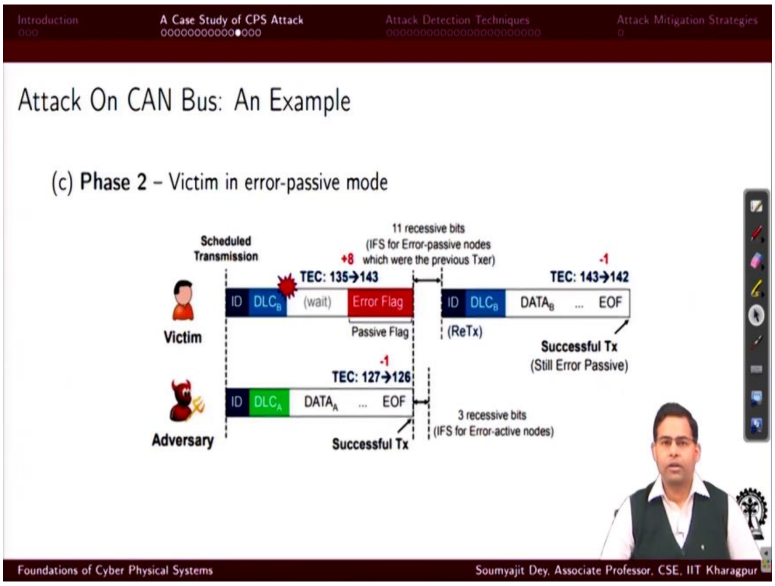
And after this there will be an 11 recessive bits here and there will be three recessive bits due to the interference space. right And then ah what will happen is well ah for each successful transmission because although I am in error passive mode but still I can do transmissions. Ah There will be decrements happening. Right So, there will be a decrement here in the victim to 135. right Now, let us understand again, but this behaviour will now continue.

Now, again ah when ah so, this is happening because let us say here the adversary is not doing anything. ok But ah and also what is important is understand to understand is this thing that well at this point ah in the in the error passive phase. What happens is that well ah you did ah you you did something you you highlighted the error passive flag. But after that you will also try to do a retransmission of your original message. So ok

So, when you are trying to do a retransmission of your original message which you failed initially that will go through successfully. So, that is why this there will be this ah a subtraction coming from 136 to 135. So, let us understand again I hope this process was clear that for everybody it was increasing. But now, ah in this in this case, when it went for 128 to 136, the difference was instead of an error active the error passive flag came.

Due to that for the adversary there was no kind of increase of a plus 8 because it could successfully transmit. So, it actually had a decrease to 127. But then the victim went to the retransmission mode and that was so, successful and it decreased to a 135. right But but that does not clear the problem. Right

(Refer Slide Time: 17:28)



Introduction | A Case Study of CPS Attack | Attack Detection Techniques | Attack Mitigation Strategies

Attack On CAN Bus: An Example

(c) **Phase 2** – Victim in error-passive mode

Foundations of Cyber Physical Systems

Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

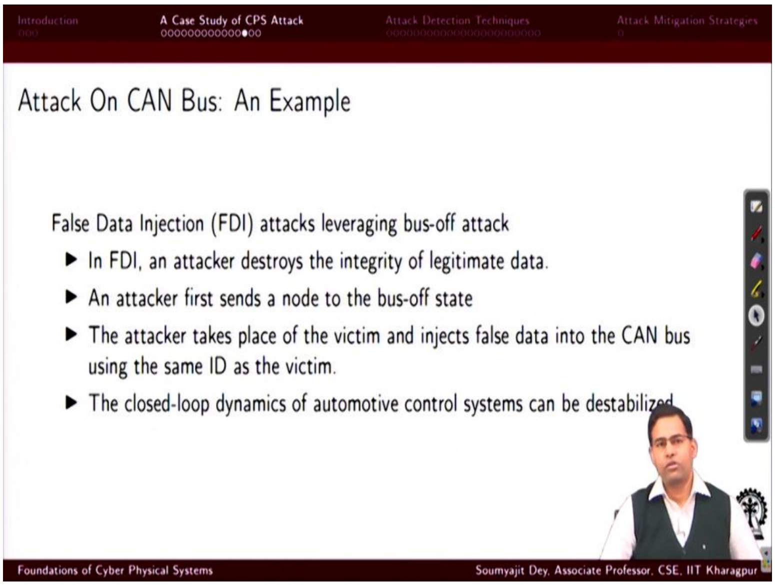
But now again, when there we every time there is a message collision created by the adversary we will have this as plus 8 and we will have here are minus 1. And then there will be retransmission due to which there will be a minus 1 here. So, in effect, what is happening is every transmission the victim is having an effective plus 7 and the adversary is having an effective minus 1 right So, in this phase 2 when the victim is error, passive mode.

So, let us understand again when I was in the phase 1 both of our TECs were increasing, with the only difference that for the victim that TEC was increasing in the previous cycle. When I come to phase 2 ah what is happening is both for the victim and the adversary, ah well ah I have a I mean the the victim will since it was having this increments happening earlier than the adversary. At this point it will it will get inside the error passive mode.

And due to that the flag will change from passive active to passive and due to that the adversary, you would not get any transmission error increase in. In fact, it will be a decrease and for the victim it will be a net increase of plus 7 with every collision. And this will keep on repeating in every round with a effective plus 7 right and an effective minus 1 here. And this will keep on happening until unless this guy goes to ah beyond 25 and that is when it is is stuck out of the bus. Right

So, it is in a bus off state for the period and that is when the adversary, who is sending messages with the same ID those messages will keep on going only and it can it can it can create instability it is it can create answered situations with plants. Right

(Refer Slide Time: 19:10)


Introduction
A Case Study of CPS Attack
Attack Detection Techniques
Attack Mitigation Strategies

Attack On CAN Bus: An Example

False Data Injection (FDI) attacks leveraging bus-off attack

- In FDI, an attacker destroys the integrity of legitimate data.
- An attacker first sends a node to the bus-off state
- The attacker takes place of the victim and injects false data into the CAN bus using the same ID as the victim.
- The closed-loop dynamics of automotive control systems can be destabilized

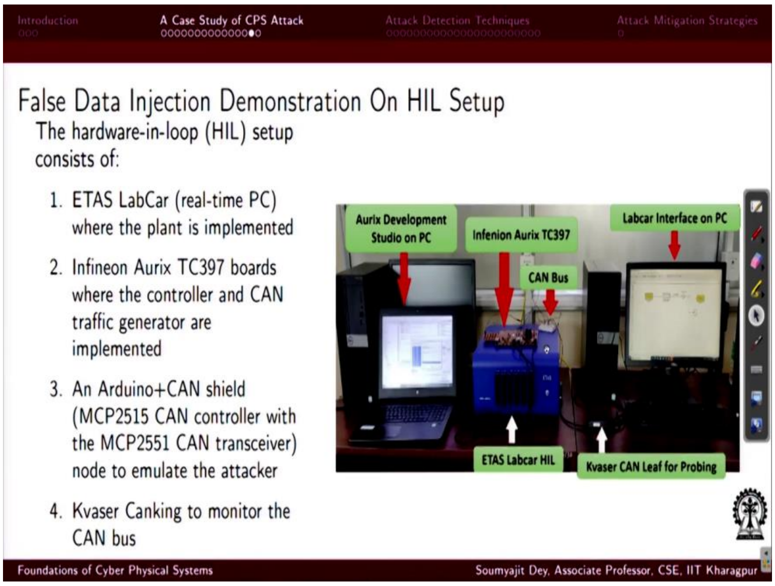
Foundations of Cyber Physical Systems

Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

So, ah this is how, in the false data injections in injection situation, the attacker destroys the integrity of the legitimate data. And the attacker first sends the node to a bus off state like we discussed. And then the attacker takes the victim's role and it will inject false data into the bus using the same ID and that can destabilize closed-loop dynamics of automotive control systems. So that is a classical example. How can buses ah vulnerabilities can be exploited?

But like I said that well there are counter measures that have come into also. And CAN bus are nowadays I mean there are CAN FDI can be flexible data that we are doing this synchronization may be difficult and all these issues also coming. Ok

(Refer Slide Time: 19:54)



Introduction A Case Study of CPS Attack Attack Detection Techniques Attack Mitigation Strategies

False Data Injection Demonstration On HIL Setup

The hardware-in-loop (HIL) setup consists of:

1. ETAS LabCar (real-time PC) where the plant is implemented
2. Infineon Aurix TC397 boards where the controller and CAN traffic generator are implemented
3. An Arduino+CAN shield (MCP2515 CAN controller with the MCP2551 CAN transceiver) node to emulate the attacker
4. Kvaser Canking to monitor the CAN bus

Foundations of Cyber Physical Systems Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

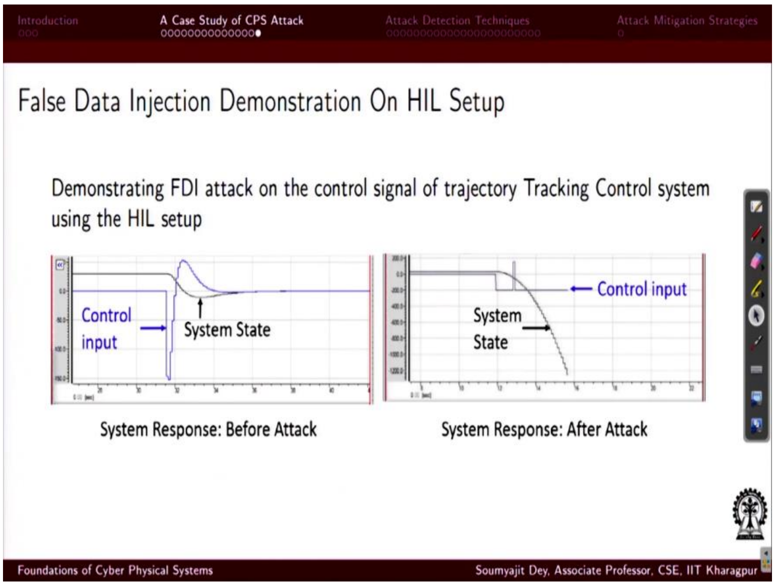
Now, ah this is a small setup using which you can actually do such a ah attack injections. So, let us say you have this Infineon board which is an ECU. And you are attaching a CAN controller and a CAN bus to that and that say there is Ah you are you are running a controller in this board and that controller is ah attached to a plant. And that plant is kind of ah running in this hardware in the loop simulator.

It is a real time simulator, where you are actually simulating the plant model in real time. And this Infineon Aurix TC397 board is where the CAN controller is running and CAN traffic generator is also implemented. So that is another code which you send creating other messages mimicking other ECUs. And this is the this is 1 ECU with some controller for the plant. And let us say you implement an attacker in another node, ah which is an Arduino with a CAN shield.

So that is a CAN, if you you can actually mimic such ah such CAN nodes by using simple, cheap Arduino boards and attaching CAN shields with them. right ah It has a it has a The CAN shield is nothing but it has a CAN controller and transceiver and it will emulate the attacker. right Also for measurement purposes you can actually use a Kvaser ah Canking monitor ah to the CAN bus. So, using such a monitor you can actually attach this monitor to the CAN bus and you can and you can actually see what are the CAN messages. You can see that CAN bus a stream in a PC. right So, using this setup you can you you can actually program and write the controller program. This controller using or it is development studio download it on the Infineon board. So, in a normal situation, the using this CAN bus from the board to the HIL you are sending messages for the plant and the plant is running ah on this HIL system the hardware in the loop system.

Now, you can attach, like I said, the other attacker ECU you can attach to the CAN bus and you can also have some can traffic generated which mimics other ECUs. Right

(Refer Slide Time: 22:05)



Introduction | A Case Study of CPS Attack | Attack Detection Techniques | Attack Mitigation Strategies

False Data Injection Demonstration On HIL Setup

Demonstrating FDI attack on the control signal of trajectory Tracking Control system using the HIL setup

System Response: Before Attack

System Response: After Attack

Foundations of Cyber Physical Systems

Soumyajit Dey, Associate Professor, CSE, IIT Kharagpur

And when the attack happens ah we you can see, you can monitor, ah that what really goes on. So, let us say this is your control input and this is your system state. We are having a simple trajectory control trajectory tracking control system and eventually it stabilizes as you see that both the control input and the system state are stabilizing here. But let us say you did such a bus off attack and for a period you have taken this ah CAN no CAN the, the ECU of the system. OK

And so, from here there is no control input available ah right here. ok And then ah because the attacker has assumed the identity of the ECU and you can see that the system state is coming down. It was supposed to be somewhere around this reference where it has come down. So that is how we can actually see that well due to such false data injection what can happen in up to a plant. So, we can actually study that.

So that is about some examples of how CPS attacks can really happen. ah With this, we will end this lecture. Thanks for your attention.