Security in embedded systems

Thilo Schumann, CAN in Automation

Security in embedded systems is currently an ignored topic. But there are possibilities to easily add a broadcast authentic communication. This will allow diagnostic and debugging possibilities.

Introductions

Security in embedded systems is a long time ignored topic. Because embedded systems were regarded as closed systems with no access to and from the world. Closed system were some educated technicians have access and access control by a physical key inserted into a physical door. Days have changed and embedded systems became accessible to the world by means of remote access. The physical access control became meaningless. Some examples are automotive, lift control, medical devices, and others.

Threat models

These days security is easily just an added feature: "just use certificate based authentication." But this gives a wrong sense of security. Security is not easy and is not convenient. Before security can be designed in so-called threat models have to be identified and appropriate counter measures have to be identified. Each an every threat model has its own requirements.

To identify the different threat models I have to assume different scenarios. The main requirement of any of those scenarios is, that there are two entities communicating with each other, lets name them Alice and Bob.

Eavesdropping

One threat model is Alice and Bob exchange messages. Now there is Eve. Eve is able to passively intercept the communication. Eve as such can read any of those messages, but is unable to modify, repeat, or whatever do to manipulate the communication between Alice and Bob.

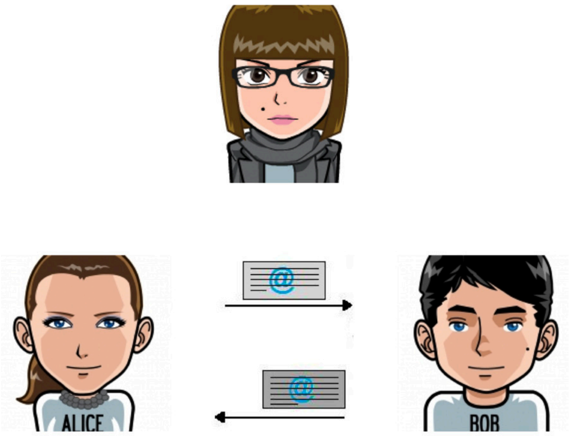

Figure 1: Alice and Bob exchanging messages while Eve is listening

There is also Mallory. Mallory wants not only to read the communication between Alice and Bob, but also wants to manipulate the communication. Mallory may want to modify messages, or the reply messages. Any of those manipulations by Mallory will be detected by Alice and Bob. But they will not be able to detect that there is Eve.

Privacy

Another threat model is again Alice and Bob exchange messages and they want to hide their communication from Eve. Eve shall not be able to intercept the communication and to read anything. The communication shall be private.

Advantages and disadvantages

When I allow eavesdropping in the communication and I don't care about privacy, than I have a big advantage. I can add Carol to the communication between Alice and Bob more easily. Maybe I also add Dan to the communication. That means I can easily add others to the communication,

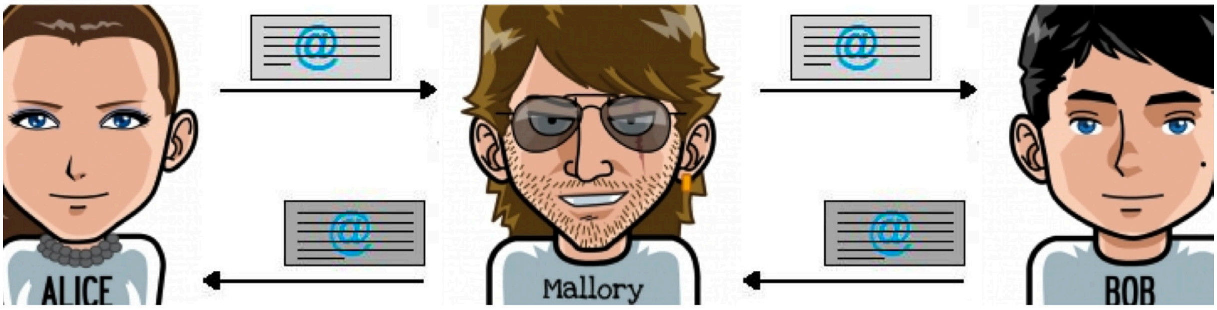

Figure 2: Alice and Bob exchanging messages while Mallory is intercepting

because I have a broadcast communication. The disadvantage is, that the communication is not private.

With the privacy requirement it is difficult to provide a broadcast communication between Alice, Bob, Carol, and Dan. It is not impossible, but it requires a lot of overhead or a central trustfully entity, like Faith.

Communication principles

With that knowledge there can be two types of communication distinguished, the authentic communication and the private communication.

Authentic communication

Authentic communication follows the paradigm: "I have nothing to hide, and I will follow only your command." Alice and Bob have to authenticate each other. Then every message is appropriately signed and as such, everybody can verify that the message is authentic. If Carol and Dan want to join into the conversation passively, like Eve, they just can read the messages. They are even able to verify that the messages are authentic and transmitted by Alice and Bob. If Carol and Dan join into the conversation actively, than Alice and Bob have to prove that Carol and Dan are authentic as well.

Private communication

Private communication follows the paradigm: "I have everything to loose." Alice and Bob need not only to authentic to each other. They also have to scramble each and every message. In this case, Carol and Dan can be added to the communication easily. They have to be added actively. Because they need to know how each other scrambles the messages. Depending on the message transmission each and every single message has to be individually scrambled for each and every communication relationship.

Embedded communication and threat models

In embedded system we have a CAN based communication between different devices. If I have a door control system there is a door knob or presence device that is able to detect, if someone wants to open the door. Then there is the drive that will open door. If the door control system is placed in a sensitive area like a bank, or police station, then the according threat models have to be evaluated. One possibility is, I add an device, which is able to read any of those commands to open the door, then that is eavesdropping. Reading the message that the door knob requested door opening is not an issue. The drive only needs to assure that the opening command is requested by the door knob and not by someone else. This would require only authenticated communication.

But if the door knob requires a personal identification, then it could become a privacy issue. Because then I can identify the person who requested the opening of the door. Then a private communication between the door knob and the drive is required.

CANopen and Security

CANopen is designed for broadcast communication for control purposes. Currently there is no security defined for CANopen. There is one proposal to encrypt any communication within one system.

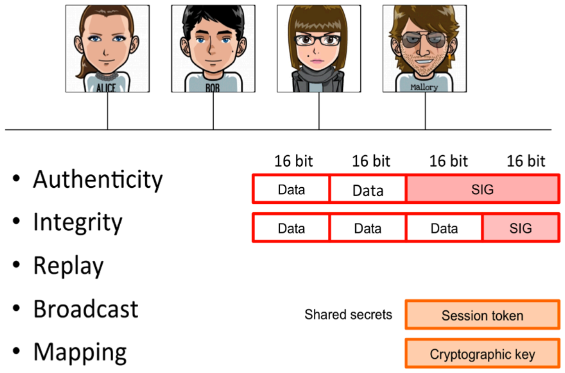

Figure 3: Requirements in CAN-based systems

The advantage is, that anything is encrypted and for an outsider it is difficult to identify network management from control data. The disadvantage is, debugging and diagnosing the system is impossible, because everything is encrypting. Either the logging device is part of the system initially, or it is impossible.

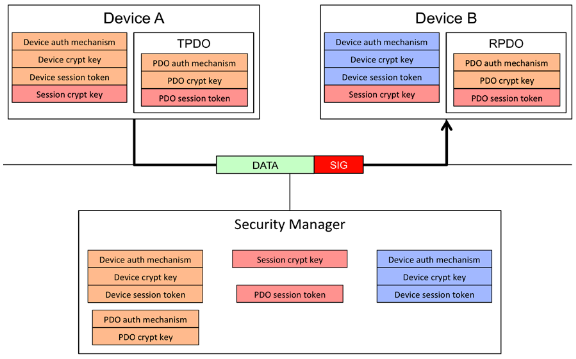

Figure 4: One possible implementation requiring a trusted device

One idea

An idea would be to allow authenticated communication and private communication between devices in the same network at the same time without encrypting all the communication. That allows many possibilities for future enhancements.

As seen in the communication between device A(lice) and B(ob) is broadcast, because it is based in a process data object (PDO). Some additional data is added, called signature. The signature may either is used to authenticate the message or to verify that the message is decrypted correctly. The information about the currently uses mechanism is inherently known by Alice and Bob.

The question then is, how to setup the communication between Alice and Bob. To setup a trusted third party Trent is required. Trent will introduce Alice and Bob to each other, and may add others like Carol and Dan to the communication. The strong requirement then is Trent can be trusted under any circumstances.

Security related requirement

History has shown, that security is not only an issues of the security services. It is also an issue of wrong doings and bugs. That takes security along the lines of safety. The implementation itself must be secure and safe. The implementation had to be developed according to the latest standards of software development. That it has to be assumed, that anything can be input. A typical ignorance of this rule could be, CAN is always of 8 bytes of data. But what happens tomorrow when CAN FD will be deployed?

Security, like safety, requires that any possible input data is considered and an appropriate response is defined. As such security, like safety, requires proper implementation including testing. In testing input data is produced, that the device forces into a certain error behavior. Testing becomes also an integral part for security implementations.

Thilo Schumann
CAN in Automation (CiA)
Kontumazgarten 3
DE-90429 Nuremberg
Tel.: +49-911-928819-0
Fax: +49-911-928819-79
headquarters@can-cia.org
www.can-cia.org