Fraunhofer AISEC

Sicherheits-Evaluierung der Endress+Hauser Bluetooth Infrastruktur (Kurzform)

Florian Bachmann, Dr.-Ing. Johann Heyszl

22. März 2016

Version 1, Revision 1

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)
www.aisec.fraunhofer.de

Fraunhofer AISEC
Parkring 4
85748 Garching b. München

Kontakt: Dr.-Ing. Johann Heyszl
johann.heyszl@aisec.fraunhofer.de

1 Zusammenfassende Bewertung der Informationssicherheit

Fraunhofer AISEC hat signifikante Kompetenzen und Projekterfahrung in der Analyse der Informationssicherheit von eingebetteten Systemen. Im Rahmen des Projekts *Sicherheits-Evaluierung der Endress+Hauser Bluetooth Infrastruktur* hat Fraunhofer AISEC auf Basis der von E+H zur Verfügung gestellten Dokumentation über das Gesamtsystem, die konkreten Geräte und die Sicherheitslösung ein Review der IT-Sicherheit mit Verbesserungsvorschlägen sowie eine Bedrohungsanalyse durchgeführt. Die Bewertung erfolgte auf Basis der zur Verfügung gestellten Dokumentation und ist in dem vollständigen Projektbericht nachvollziehbar dargestellt[1]. Folgende Schritte wurden dazu unternommen:

- Es wurden die konkreten Schutzziele erfasst, sowie das Angreifermodel definiert.
- Es wurde eine Bedrohungsanalyse auf Basis von Angriffsbäumen durchgeführt. Als erster Schritt wurden die kryptographischen Algorithmen und die verwendeten Protokolle betrachtet. Ein weiterer Fokus galt der Schlüsselverteilung und Authentifikation, sowie dem Passwort-Recovery. Es wurden außerdem übliche Angriffe aus dem Bereich der HW-Sicherheit und Angriffe auf die Funkschnittstellen berücksichtigt.
- Die Wirksamkeit der Sicherheitsmaßnahmen gegen die identifizierten Angriffe wurden analysiert.
- In einer Schwachstellenanalyse wurden kritische Aspekte ausgearbeitet und Verbesserungsmöglichkeiten dargestellt.
- Die Verbesserungsmöglichkeiten wurden durch den Auftraggeber berücksichtigt.
- Abschließend wurde ein Bericht über die IT-Sicherheit der Sicherheitslösung erstellt.

Die erfassten Schutzziele sollen einem Angreifer widerstehen, der dem folgenden Modell entspricht:

- Angreifermotivation:
  - Schaden zufügen mit und ohne spezifischen strategischen Zielen
  - Ausforschen von Betriebsgeheimnissen, Industriespionage

[1] Der Projektbericht liegt als Kurzform und als vollständiger Bericht vor. Die Kurzform umfasst nur die zusammenfassende Bewertung in Deutsch und Englisch.

- Mächtigkeit des Angreifers
  - Signifikanter Zeitaufwand realistisch (Wochen - Monate)
  - Know-How in Elektronik, Kryptographie und Seitenkanalattacken
  - Zugang zu Luftschnittstellen aller Field Device (FD)
  - Keinen direkten Zugang zum Industrial Control System (ICS)
  - Einzelne Geräte aus dem operativen Betrieb stehen zur Verfügung. Baugleiche Geräte stehen in höherer Anzahl zur Verfügung
  - Internes Wissen über den Aufbau des gesamten E+H Systems

Es wurden Verbesserungsmöglichkeiten hinsichtlich der spezifizierten Authentisierung und bei den verwendeten Algorithmen gefunden. Alle Vorschläge zur Spezifizierung der Verschlüsselungs- und Authentisierungsprotokolle wurden vom Auftraggeber übernommen. Aufgrund von Randbedingungen bei der Implementierung auf bestehenden Systemen konnte jedoch nicht immer der Empfehlung gefolgt werden. Stattdessen wird in Details von unseren Empfehlungen abgewichen. Die anstelle unserer Empfehlung durch E+H eingesetzten Alternativ-Verfahren sind aus IT-Sicherheitssicht ebenfalls angemessen sicher.

Zusammenfassend leiten wir auf der Basis der durchgeführten Analysen, gemessen an den Schutzzielen, und dem Angreifermodell, folgende Bewertung für das Schutzniveau der Bluetooth Infrastruktur ab[2][3]:

Protokoll	**Hoch**[4]
Algorithmen	**Hoch**

[2] Stand 22. März 2016 lt. angegebenen Versionsnummern

[3] Die Bewertung erfolgte auf Basis der vom Auftraggeber zur Verfügung gestellten Information und beinhaltete ein punktuelles Code-Review an besonders kritischen Stellen. Für die Vollständigkeit und Richtigkeit der Dokumentation, sowie für die dementsprechende Implementierung in betreffenden Produkten, ist der Auftraggeber verantwortlich. Die Bewertung hat nur im Kontext der verwendeten Dokumentation Gültigkeit.

[4] Auf einer mehrstufigen Skala für Sicherheitsbewertungen am Fraunhofer AISEC mit den Stufen: 'Sehr Gering', 'Gering', 'Hoch', 'Sehr Hoch'.

2 Summary of the Security Review

Fraunhofer AISEC has significant expertise and experience in the analysis of embedded systems regarding information security. Within this project, Fraunhofer AISEC has reviewed the security of the new system security concept of E+H for their new Bluetooth infrastructure environment. The review was based on the documentation provided by E+H regarding the entire system, the security solutions, and the devices. Fraunhofer AISEC conducted a threat analysis and derived recommendations for the improvement of the information security which is documented and reasoned in the full version of the report[1]. The following steps were part of the review:

- The project-specific protective goals were derived and the attacker model defined.
- A threat analysis based on attack-trees was conducted. In a first step, the cryptographic algorithms and the used protocols were analyzed. In a further effort, the key management and authentication, as well as the password recovery were analyzed. Common attacks from the field of hardware-security and attacks on wireless radio communication have been considered.
- The effectiveness of the specified countermeasures against identified attacks was analyzed.
- Critical weaknesses and recommendations for improvement have been developed.
- The recommended improvements have been considered by E+H.
- Finally, a report about the information security of the security solutions has been compiled.

The identified specific protective goals have been evaluated against the following attacker model:

- Attacker motivation:
  - Inflict damage with or without strategic goals
  - Retrieve intellectual property or industrial espionage
- Properties of attackers:

[1] The report has been provided in a short and full version. The short version only contains the summary of the review in German and English language.

- Significant time effort realistic (weeks to months)
- Know-How in electronic engineering, cryptography, and side-channel attacks
- Access to the radio communication of all devices
- No physical access to the Industrial Control System (ICS)
- Individual devices from the installation may be physically accessible. Devices of the same make are available generally
- Internal know-how about the entire E+H system

Possible improvements regarding the specified authentication and regarding the used algorithms were derived. All recommended improvements regarding the specification of the encryption and authentication protocols have been considered. Due to implementation constraints on existing systems, some of our recommendations could not be considered as-is by E+H and alternative approaches were chosen instead. AISEC has analyzed the chosen alternative approaches and evaluated them to be acceptable choices in terms of information security.

As a summary we derive the following final verdict about the information security protection level of the Bluetooth-based infrastructure after the analysis, based on the attacker model and derived project-specific protective goals[2][3]:

Protocoll	**High**[4]
Algorithms	**High**

[2] Dated 22. März 2016 based on listed documentation

[3] The assessment is based on the documentation provided by E+H and included a selective code-review of particularly critical sections. E+H is responsible for the completeness and integrity of the documentation, as well as for ensuring that the implementation within respective products will match the specification. The assessment is only valid in the context of the used documentation.

[4] On a Fraunhofer AISEC scale for security assessments with with the protection levels: 'Low', 'Medium', 'High', 'Very High'.