ملخص رسالة ماجستير بعنوان

تحسين أمن برتوكول DNP3 في نظام سكادا

اسم الطالب

إبراهيم زمرد

المشرف

الدكتورة: رأفة خازم

المشرف المشارك

الدكتور: مسعود الأتاسي

القسم والاختصاص

قسم هندسة الحواسيب والأتمتة

هندسة التحكم والأتمتة

الملخص

شاع استخدام مصطلح التحكم الاشرافي منذ زمن طويل حيث كانت الحساسات والمستشعرات والقواطع توصل مع المتحكم المنطقي القابل للبرمجة ومنه الى الحاسب الخاص بمدير النظام، كانت تلك الأجهزة موجودة في أماكن متقاربة والاتصالات آمنة نسبياً.

ولم يهتم المطورون في بدايات تطوير بروتوكولات الاتصال والربط بين تجهيزات منظومة التحكم الاشرافي بموضوع الأمان وإنما قاموا بتركيز جهودهم على الفعالية والسرعة والكلفة بدلاً من ذلك.

ومع تطور المنشآت الصناعية وتوسعها وإنشاء فروع لها في مناطق متباعدة أصبح استخدام الشبكات الغير الآمنة مطلبا ضرورياً كاتصال عبر خط الهاتف، وقد أدى هذا الامر إلى الجعل من مسألة الأمان والحماية من الاختراق والعبث تحديات كبيرة لابد من التصدي لها.

فجعل نظام موجود آمن هو تحدي وأمر بالغ الصعوبة وذلك بسبب وجود عدة اعتبارات منها الأداء والتوافقية من الإصدارات السابقة وسهولة الاستخدام.

يهدف هذا البحث الى تحسين وتعزيز أمن بروتوكول DNP3 المعتمد أحد في نظام التحكم الاشرافي SCADA وسيتم التحسين من خلال اقتراح استخدام شهادات موقعة رقمياً للحصول على مصادقة آمنة بالإضافة إلى تشفير قناة الاتصال للتصدي لهجمة الرجل في المنتصف MITM.

Master's thesis summary entitled

Improving the security of DNP3 protocol in SCADA

Student Name

Ibrahim Zomorrod

Co-Supervisor

Dr. Eng.Massoud Alattassi

Supervisor

Dr.Eng.Raffah Khazem

Department

Department of computers and automatic control

Summary

The term supervisory control has been known for a long time, as sensors, sensors, and relays were connected to the programmable logic controller and from there to the system manager's computer. These devices were located in close places and the communications were relatively secure.

Therefore, during the beginnings of developing communication protocols and linking between the equipment of the supervisory control system, the developers did not care about the issue of security and focused their efforts on effectiveness, speed, and cost instead.

With the development and expansion of industrial facilities and the establishment of their branches in distant areas, the use of unsecured networks became necessary, such as communication via a telephone line. This made the issue of security and protection from hacking and tampering an absolute necessity.

Adding security to an existing system is extremely challenging and difficult due to several considerations including performance, backward compatibility, and ease of use.

We will work to improve the security of one of the most important communication protocols in supervisory control systems (SCADA), which is the DNP3 protocol, as we will work to use digitally signed certificates to obtain secure authentication, in addition to encrypting the communication channel in order to protect against man-in-the-middle attacks.