جامعة دمشق
كلية الهندسة الميكانيكية والكهربائية
قسم هندسة الحواسيب والأتمتة

تحسين أمن برتوكول DNP3في نظام سكادا

Improving the security of DNP3 protocol in SCADA

إبراهيم زمرد

الدكتورة المشرفة: رأفة خازم

المشرف المشارك: الدكتور مسعود الاتاسي

الملخص

عرف مصطلح التحكم الاشرافي منذ زمن طويل حيث أنه كان يتم توصيل الحساسات والمستشعرات والريليهات مع المتحكم المنطقي القابل للبرمجة ومنه الى الحاسب الخاص بمدير النظام، كانت تلك الأجهزة موجودة في أماكن متقاربة والاتصالات آمنة نسبياً.

سوف نعمل على تحسين أمن أحد أهم بروتوكولات الاتصال في أنظمة التحكم الاشرافي SCADAوهو بروتوكول DNP3حيث سنعمل على استخدام الشهادات الموقعة رقمياً للحصول على مصادقة آمنة بالإضافة إلى تشفير قناة الاتصال وذلك للحماية من هجوم الرجل في المنتصف.

القسم العملي

تتم عملية المصادقة وفق الخطوات التالية:

١.تبادل المفاتيح وفق خوارزمية ديفي هيل مان.

٢.بعدها يصبح لدى الطرفين نفس المفتاح ندعوه مفتاح الجلسة.

٣.تقوم الطرفية بإنشاء شهادة رقمية وتشفيرها بالمفتاح الخاص وارسالها للمحطة الرئيسية.

٤.تقوم المحطة الرئيسية الفرعية بفك تشفير الشهادة بالمفتاح العام والتأكد منها.

٥.بعد نجاح العملية تقوم المحطة الرئيسية الفرعية بإنشاء شهادة رقمية وتشفيرها وحفظها على انها تابعة للطرفية.

٦.بعد نجاح التأكد تنجح المصادقة ويحصل اتصال بين الطرفين.

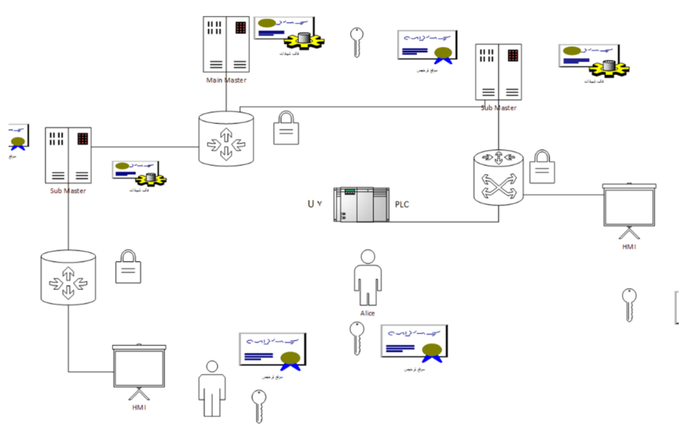
القسم العملي

يتكون النظام المقترح من المكونات التالية:

١.المحطة الرئيسية: وهو المدير الأساسي للشهادات ويصادق على الشهادات .

٢.المحطات الرئيسية الفرعية: وهو ينسق ويدير عمل المحطات والمنشئات

٣.الطرفيات: مثل المتحكمات وواجهات التخاطب البشرية: وهي لديها فقط شهادة ومفتاح.



القسم النظري

نظام سكادا هو نظام يقوم بتجميع البيانات من الحساسات المتموضعة في نظام التحكم وإرسالها إلى الحاسب الرئيسي لغرض الإدارة والتحكم والمراقبة، هو أحد البرامج التطبيقية المستخدمة من أجل عمليات التحكم التي يتم بها تجميع البيانات في الوقت الحقيقي من أماكن بعيدة لمراقبة التجهيزات والظروف المحيطة وبنفس الوقت التحكم بها.

DNP3هو بروتوكول قياسي مفتوح المصدر يستخدم كبروتوكول اتصال بين العمليات في نظام الأتمتة والتحكم في محطات الكهرباء والمياه، صمم بواسطة اللجنة الكهروتقنية الدولية ((IECالطبقة OSI الثالثة المستخدمة في هذا المجال في الأجهزة كبروتوكول اتصال، الميزة المتعددة اللغات لـ DNP3التي تسمح بأي بروتوكول للتواصل معه سمحت للكثيرين بترقية شبكتهم إلى DNP3، يمكنه العمل على شبكات الاتصال المختلفة.

النتائج والمناقشة

نقترح العمل على تطوير برامج لمراقبة وتسجيل نشاطات الخوارزمية وذلك من اجل تقديم مستوى امان أفضل من خلال مراقبة كافة نشاطات الشبكة. كما نقترح وضع الية تبادل مفاتيح امنة وخاصة بالنظام المطور ومتكاملة معه مما يعطي مستوى امان أفضل.

نقترح انشاء نسخ من الكود البرمجي قابلة للتضمين في الأجهزة المستخدمة في شبكات تحكم .SCADA

المراجع

1. Mesbah, Mohamed, et al. "Analysis of ics and scada systems attacks using honeypots." Future Internet 15.7 (2023): 241.

2. Feng, Tao, et al. "Security Analysis and Enhancement of INTERBUS Protocol in ICS Based on Colored Petri Net." Information 14.11 (2023): 589.

3. Zaitsev, Dmitry A., et al. "Verification of cryptocurrency consensus protocols: reenterable colored Petri net model design." International Journal of Parallel, Emergent and Distributed Systems 39.1 (2024): 32-50.