بخشی از ترجمه مقاله

عنوان فارسی مقاله :

شناسایی(احرازهویت) همتا به همتا (نظیر به نظیر) برای سیستم های کوچک نهفته (تعبیه شده) یک روش صفر مبتنی بر دانش برای امنیت اینترنت اشیا

عنوان انگلیسی مقاله :

Peer to Peer Authentication for Small Embedded Systems

A zero-knowledge-based approach to security for the Internet of Things

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

IX. Conclusion and Future Work

In this paper we propose a new method to provide privacy, data integrity and end-entity authentication among peers in a static IoT / IoE network, primarily focusing on the issue of security in small embedded systems. It is based on a zero-knowledge proof and has two unique features, e.g. it provides mutual authentication based on the GMW protocol, while integrating a public key transport mechanism for a complementary key negotiation protocol.

The proposed protocol provides perfect forward secrecy, but requires the distribution of credentials (e.g. graphs) pre-deployment, which does not scale well with large deployments. However, it avoids computational and management overheads created by alternative solutions that provide PFS, e.g. X.509 certificates and public key infrastructures.

نتیجه گیری و تحقیقات آینده

در این مقاله یک روش جدید برای حفظ حریم خصوصی ، تمامیت داده ها و شناسایی نهاد پایانی در میان همتایان در یک شبکه ی IoT / IoE استاتیک ارائه نمودیم ، که در درجه ی اول بر مسئله ی امنیت در سیستم های نهفته (تعبیه شده) کوچک متمرکز است. این روش بر اساس اثبات دانش صفر قرار دارد و دارای دو ویژگی منحصر به فرد می باشد ، به عنوان مثال ، شناسایی (تصدیق) دو جانبه را بر اساس پروتکل GMW امکان پذیر می سازد، در حالی که شامل یک مکانیسم انتقال کلید عمومی برای یک پروتکل مکمل ارتباط کلید می شود.

پروتکل مطرح شده PFS (perfect forward secrecy) را امکان پذیر می سازد ، اما مستلزم توزیع اسناد (به عنوان مثال گراف) پیش از استقرار می باشد. با این حال ، در این روش از سربارهای محاسباتی و مدیریتی ایجاد شده به واسطه ی راه حل های جایگزین که PFS را امکان پذیر می سازند ، اجتناب می شود ، به عنوان مثال اسناد X.509 و زیرساخت های کلید عمومی. در پیاده سازی فعلی ، این پروتکل از تبادل کلید دیفی هلمن استفاده می کند.