

Des centrales électriques aux passeports : sécuriser les données numériques

Les technologies de l'information et de la communication (TIC) sont devenues incontournables dans notre vie quotidienne. Alors que les infrastructures numériques européennes sont de plus en plus interconnectées, la défaillance d'un seul système pourrait avoir des conséquences désastreuses partout en Europe. C'est pourquoi des scientifiques du Centre commun de recherche s'intéressent aux liens entre ces systèmes, et conçoivent des méthodes visant à harmoniser la sécurité des TIC et à renforcer la protection contre les attaques informatiques. Ils contribuent également à sécuriser le passage de processus traditionnels sur papier à des systèmes électroniques.

LE SAVIEZ-VOUS ?

- Les attaques informatiques et la fraude en ligne provoquent des milliards d' Euros de dégâts chaque année.
- Le nouveau passeport électronique européen est protégé par une cinquantaine de dispositifs de sécurité différents.

Simuler les attaques de pirates

Au laboratoire de sécurité informatique du Centre commun de recherche de la Commission européenne (JRC, Joint Research Centre), des scientifiques simulent des attaques de pirates sur des systèmes informatiques de contrôle de réseaux électriques. Ils tentent de mieux comprendre les interdépendances complexes et les vulnérabilités du réseau électrique européen. Grâce aux résultats de ces simulations, ils créent et améliorent les protocoles de sécurité, et développent des standards communs traitant de la sécurisation informatique des systèmes de contrôle de réseaux électriques. Ainsi, les exploitants de centrales électriques peuvent mieux se protéger contre les attaques informatiques. Les résultats des simulations servent également à étudier l'impact d'attaques plus classiques.

Protéger les données du passeport, partout

Le passeport électronique européen ne sert pas seulement à accélérer les contrôles et à raccourcir les files d'attente dans les aéroports et aux frontières, mais il permet également d'identifier les suspects bien plus efficacement que tout système basé sur une inspection manuelle. La sécurité de son fonctionnement impose cependant que tous les pays de l'UE ainsi que les fournisseurs d'équipements techniques mettent pleinement en œuvre les normes techniques convenues. La moindre faille dans la procédure de certification de l'équipement technique pourrait mettre en danger la totalité du système. Pour s'assurer que le système de passeport électronique européen reste à l'abri des fraudeurs et des attaques informatiques, des chercheurs du JRC transposent les exigences complexes en caractéristiques techniques. Dans un futur proche, ces travaux pourraient contribuer à sécuriser d'autres documents d'identification européens, notamment les visas et les permis de séjour.



Pour en savoir plus : www.jrc.ec.europa.eu/research4u