Vérification de protocoles cryptographiques à l'aide de l'outil PROVERIF

Type de contenu : Texte

Titre(s) : Vérification de protocoles cryptographiques à l'aide de l'outil PROVERIF ; PARRAUD, Patrice ; SLT DELVALLET, Xavier ; VAN HEULE, Dirk

Autre(s) responsabilité(s) : PARRAUD, Patrice (Directeur de thèse)
SLT DELVALLET, Xavier Promotion Chef de bataillon Bulle (2010-2013) (Secrétaire)
VAN HEULE, Dirk (Directeur de thèse)

Editeur, producteur : Ecoles Militaires de Saint-Cyr Coëtquidan

Description matérielle : 1 CD

Note sur le contenu : mémoire

Note de thèses et écrits académiques : Filière Scientifique - Option Informatique Promotion Chef de bataillon Bulle Date de soutenance : 01/01/2013

Résumé ou extrait : PRÉSENTATION : Depuis son apparition dans les années 90, plusieurs expérimentations de vote électronique ont été réalisées à travers le monde aux Etats-Unis mais aussi en Suisse ou aux Pays-Bas. Mais la découverte de failles de sécurité dans les protocoles de vote électronique a poussé certains gouvernements à abandonner ce système de vote électronique. Ceci a poussé une partie de la communauté cryptographique à s'intéresser à la sécurité des votes électroniques. Notre étude porte sur la phase de création du reçu de vote à travers l'étude de la logique d'un protocole de signature et de ses différentes propriétés de sécurité avec l'outil Provérif. SÉCURITÉ : Dans un premier temps, nous définissons ce qu'est la sécurité informatique afin de permettre de mieux analyser les problèmes et les contraintes qui en découlent. LANGAGE FORMEL : Dans un second temps, nous étudions le langage formel utilisé par l'outil Provérif : le Pi-calcul appliqué. TRAVAUX EFFECTUÉS : Nous avons modélisé un protocole de signature à seuil dans le but de pouvoir l'utiliser comme reçu de vote dans le cas d'une utilisation lors d'un vote électronique. Ensuite, nous avons modélisé l'adversaire c'est-à-dire ses objectifs et ses capacités pour voir quelles sont les propriétés de sécurité vérifiées par ce protocole de signature à seuil. Enfin nous avons analysé les résultats obtenus et définis les propriétés de sécurité que vérifie ce protocole de signature à seuil. RÉSULTATS OBTENUS : Grâce à Provérif, nous avons pu étudier les résultats suivants sur notre modélisation de signature à seuil : o Impossibilité de forger une signature. (Un adversaire n'est pas en mesure d'obtenir une signature valide sans connaitre la clé de chiffrement) o La signature se fait sans connaître le vote. o Impossibilité de récupérer le vote à partir d'une signature valide. o Résistance à la coercition et à l'achat de votes. LIMITES : Il existe cependant plusieurs limites. Une limite liée au logiciel Provérif. Si les équations utilisées pour modéliser le protocole sont trop complexe, le logiciel Provérif n'est pas en mesure de terminer. Une limite liée à la modélisation de l'adversaire. Il est assez difficile de modéliser un adversaire théorique pour qu'il semble réaliste. Un adversaire trop faible n'aura aucun intérêt pour l'étude car il n'aura aucun moyen de de remplir ses objectifs. CONCLUSION : Grâce à Provérif, nous avons pu voir que le protocole de signature à seuil que nous avons utilisé remplit

les conditions de sécurité nécessaires et peut donc être utilisé comme reçu de vote lors d'un vote électronique. Cependant, il serait intéressant de l'étudier dans le cadre d'un protocole de vote électronique complet.

Sujet(s) : clé de cryptage
contrôle
cryptographie
modélisation objet
protocole
sécurité informatique
vote électronique