Doctoral Dissertations 1911-2013

Off-campus UMass Amherst users: To download campus access dissertations, please use the following link to log into our proxy server with your UMass Amherst user name and password.

Non-UMass Amherst users: Please talk to your librarian about requesting this dissertation through interlibrary loan.

Dissertations that have an embargo placed on them will not be available to anyone until the embargo expires.

Dynamic Secrets in Communication Security

Sheng Xiao, *University of Massachusetts - Amherst*

Date of Award
2-2013

Document Type
Campus Access

Degree Name
Doctor of Philosophy

Degree Program
Electrical and Computer Engineering

First Advisor
Weibo Gong

Second Advisor
Donald F. Towsley

Third Advisor
Hossein Pishro-Nik

Keywords
Applied sciences, Communication security, Dynamic secrets, Key management, Wireless security

Subject Categories
Computer Engineering | Computer Sciences | Engineering

Abstract
This dissertation focuses on both theoretic and practical aspects of using a new approach, *dynamic secrets,* to provide secrecy to cryptographic keys in secure communications. In the conventional paradigm of communication security, cryptographic keys and the users' communication are independent. The cryptographic keys are generated using dedicated algorithms, protocols, and even specialized hardware. Contrarily, the dynamic secrets approach extracts shared secrecy from the users'

communication traffic to generate and update the cryptographic key.

The dynamic secrets approach offers several distinctive security benefits over conventional cryptographic key management approaches. Dynamic secrets can harvest true randomness from the communication channel and render the cryptographic key truly random without using any random number generator. Dynamic secrets can quickly and automatically restore a stolen cryptographic key by frequently updating the key using the secrecy extracted from users' communication traffic. Last but not least, dynamic secrets provide an extremely accurate method to detect intrusions to the secure communication system when a stolen key is used.

We present the dynamic secrets approach in a secure packet communication model and verify its applicability in practical secure wireless communication scenarios. We further explore the security properties of dynamic secrets from a theoretic perspective and prove that dynamic secrets can achieve near optimal utilization of all possible secrecy in a secure communication.

In this dissertation, we study the application of dynamic secrets in smart grid communications, where scalability and many other engineering factors are considered. We also investigate possible theoretic outreaches of dynamic secrets and find the reliability theory in system engineering as an important quantitative methods to evaluate the consistency of communication security. Finally, we present several dynamic secrets related topics as potential research directions.