

THESIS SUMMARY

ARNAB ROY

Present-day internet users and networked enterprises rely on key management and related protocols that use cryptographic primitives. In spite of the staggering financial value of, say, the total number of credit card numbers transmitted by SSL/TLS in a day, we do not have correctness proofs that respect cryptographic notions of security for many of these relatively simple distributed programs. In light of this challenge, there have been many efforts to develop and use methods for proving security properties of network protocols.

As part of work towards my PhD thesis, I made the following theoretical contributions to the security analysis of network protocols:

- (1) I formalized a form of inductive reasoning about secrecy in a set of new axioms and inference rules that are added to Protocol Composition Logic (PCL) and proved soundness of the system over a conventional symbolic protocol execution model.
- (2) I developed foundations for inductive analysis of computational security properties by proving connections between selected trace properties of protocol executions and non-trace complexity theoretic properties standard in the literature.
- (3) I formalized the aforesaid inductive properties in a set of new axioms and inference rules that are added to Computational PCL and proved soundness of the system over a standard cryptographic model with a probabilistic polynomial time adversary.

On the practical side, I have applied the above techniques to the analysis of real world network security protocols:

- (1) I proved authentication and secrecy properties of the Kerberos V5 protocol with both symmetric-key and public-key initialization in both the symbolic and the complexity theoretic models. The proofs of key secrecy of Kerberos V5 in the complexity theoretic model are first in the literature.
- (2) I discovered a deficiency in Kerberos V5 with Diffie-Hellman initialization and suggested simple corrective measures. For the first time in the literature, I proved secrecy and authentication properties of this mode of Kerberos in the complexity theoretic model, thus constructing proofs of security of all three modes of Kerberos V5 in a uniform formal framework.
- (3) I proved secrecy and authentication properties of the IKEv2 protocol in the complexity theoretic model for the first time in the literature.

The formal logic framework that I have developed have also been used by other researchers to prove the security properties of complex industrial protocols, such as researchers at Motorola Corporation who analyzed the security of the IEEE 802.11s standard, which is tasked to provide ways of establishing and securing a wireless mesh network.

Along with colleagues, I have also reviewed and analyzed the following industry track security protocols: IEEE 802.16e, IEEE 802.1af, IEEE 802.11r, EMU EAP GPSK and Binding Update and Fast handover protocols in Mobile IPv6. The analyses consisted of identifying flaws or deficiencies as well as providing assurance through formal proofs. In many cases, our recommendations were followed for improving the protocols. In addition, our analyses led to precise articulation and documentation of the security properties to be expected of the protocols.