清华大学高等研究院

Institute for Advanced Study, Tsinghua University

密码学学术报告 Cryptology Seminars

Date: **2013-09-02, Monday**

Venue: **Conference Hall 322, Science Building, Tsinghua University**

Talk I 9:00-10:00am: Improving Counter-cryptanalysis

Dr. Marc Stevens（*Centrum Wiskunde & Informatica, Netherlands*）

Flame, a highly advanced malware for cyberwarfare discovered in May, spread itself as a properly, but illegitimately, signed Microsoft Update security patch. Flame achieved this by forging a signature from Microsoft using a so-called chosen-prefix collision attack on the very weak cryptographic hash function MD5. In this talk I will focus on counter-cryptanalysis, a new paradigm for strengthening cryptographic primitives, and the first example thereof, namely an efficient anomaly detection technique that detects whether a given signature was forged using a cryptanalytic collision attack on the underlying hash function. We used counter-cryptanalysis to expose Flame's yet unknown variant chosen-prefix collision attack even though only one of the two colliding certificates was available.Besides forensic analysis, counter-cryptanalysis can be effectively used to detect whether digital signatures are possible forgeries created using a collision attack.Finally, I will discuss ongoing work on improving the complexity of this new techniqueand efforts to reduce the chance of false negatives, i.e., existence of feasible yet-undetected collision attacks.

Talk Ⅱ 10:15-11:15am: New Generic attacks on Hash-based MACs

Dr. Gaëtan Leurent（*Université Catholique de Louvain, Belgique*）

In this talk we study the security of hash-based MAC algorithms(such as HMAC and NMAC) above the birthday bound. Up to the birthday bound, HMAC and NMAC are proven to be secure under reasonable assumptions on the hash function. On the other hand, if an n-bit MAC is built from a hash function with a l-bit state (l > n), there is a well-known existential forgery attack with complexity 2^l/2. However, the remaining security after 2^l/2 computations is not well understood. In particular it is widely assumed that if the underlying hash function is sound, then a generic universal forgery attack should still require 2^n computations and some distinguishing (e.g. distinguishing-H but not distinguishing-R) and state-recovery attacks should still require 2^l computations.

In this work, we show that above the birthday bound, hash-based MACs offer significantly less security than previously believed. Our main result is a generic distinguishing-H and state-recovery attack against hash-based MACs with a complexity of only 2^l/2. In addition, we show a key-recovery attack with complexity 2^3l/4 against HMAC used with a hash functions with an internal checksum, such as GOST. This surprising result shows that the use of a checksum might actually weaken a hash function when used in a MAC.