How to cheat in chess

Presentation by

Amodha Wijekoon

J. Black, M. Cochran, and R. Gardner, "How to Cheat at Chess: A Security Analysis of the Internet Chess Club", Cryptology ePrint Archive, Report 2004/203, 14 pp., 2004.

What is included in the article

- Article explains serious security concerns found in online chess playing system by ICC (internet chess club)
- Article discuss serious security issues on
  - Weakness in time stamping which allows players to cheat by specifying less time than they actually took to make a move
  - Weakness in encryption algorithm allowing data to be read by a third party
  - Weakness in key exchanging mechanism

Appreciative comment

As article suggest, self designed algorithms can seriously compromise security.

- Self designed encryption standards, without using a well tested algorithms such as AES can include weaknesses can be exploited
- Relaying on closed source components to secure encryption algorithm can be dangerous.

Standards such as SSL or AES are proven to be strong and infeasible to break in with current technology.

Appreciative comment

Key exchange has to be done securely, and exchanging seeds for the keys in plain text is unacceptable.

- Exchanging seeds in plain text allows man in the middle attacks.
- A large RSA key such as a 4096 bit can provide reasonable security

If key exchange is secured and encryption algorithm is secured, reasonable security can be assumed.

Critical Comment

As writers suggest, using methods like Ping can cause false positive.

- Due to the nature of internet, what if packets use a much faster alternative path than the one bench marked
- Can all cheating be recognized, how much can the actual time differ from the benchmarked time to be considered as cheating.

Relaying on a un-reliable measurement is not sufficient to take an action against a player.

Having a false positive seriously harm a players reputation, and his status in a tournament

Question

What should be done to securely calculate the time taken for a move, and how can ICC server verify time received is valid ?