How to cheat at chess

A Security Analysis of the Internet Chess Club

Presentation by
Steve Liu

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.

Summary of the Article

- Conducted a security analysis of the Internet Chess Club (ICC)
- Implemented code to exploit ICC security flaws
- Offered suggestions for repairs

ICC Security Flaws

Reverse engineered the Linux client to figure out ICC security processes

- Time stamping mechanism can be cheated
  - zero out registers for time
  - intercept or modify system time calls
- Network security protocol is not secure

Cryptanalysis

- key establishment

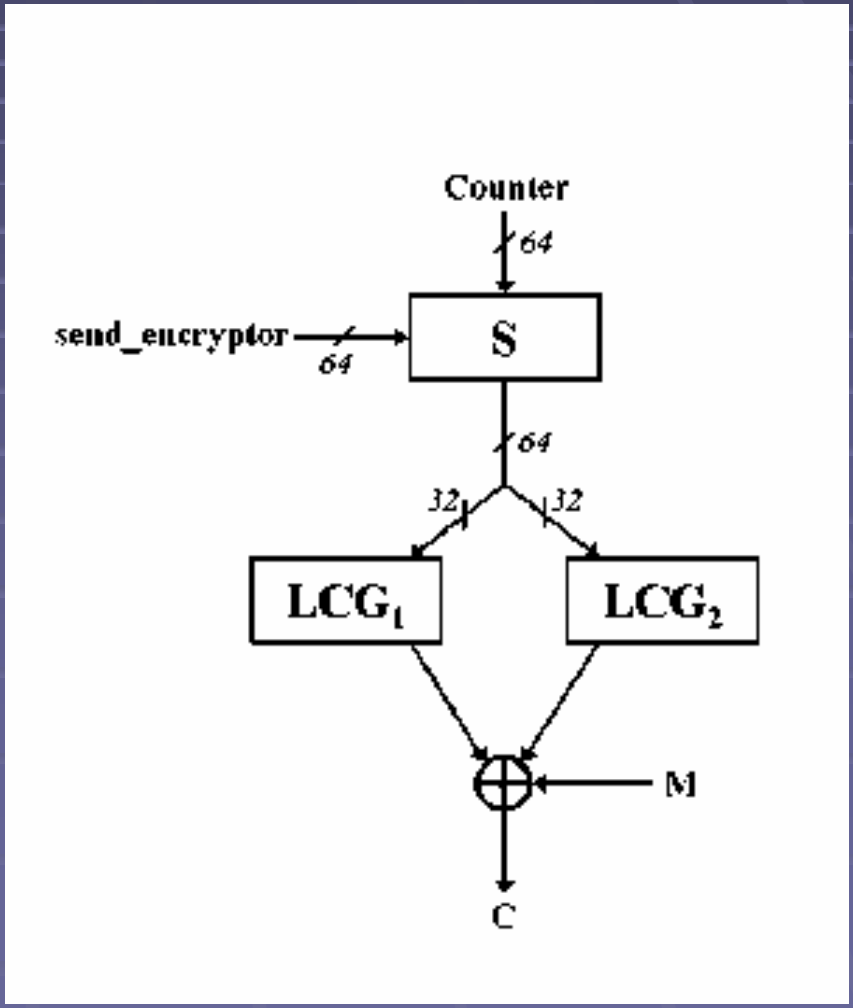
  exchange keys in the clear

  no authentication at all
- mode of operation

  LCG: $x_{n+1} = a\,x_n + b \bmod c$

  able to predict the whole sequence after knowing the first few bits
- block cipher

  invariant



Appreciative Comment

- Most websites are secure
- A straight hacking paper is rare
- More so if you believe

one needs to know how to hack to avoid being hacked

- It makes this article important

Appreciative Comment

- Specified time it took for implementation
  - zero out registers – 30 minutes
  - reverse engineer the client – 65 hours
  - only reverse engineer the part for encryption – 25 hours
- Trivial computation VS

  Trivial implementation

Critical Comment

- This article could be more ``useful``
  - Conclusion

    “It seems that whenever a non-expert invents his own, [security protocol] even if he is very clever, it is often broken.”
  - Implementation

    very specific techniques

Question

Which part of ICC would you attack ?

In general is this type of attack a big concern for websites ?

	How long does it take	Will the code work	What is the reward	Will you get the reward
Zero out registers	30 minutes	yes	prize money 1350 euros	probably get caught
More sophisticated timestamp tampering	65 hours	yes	prize monez 1350 euros	maybe. still needs good chees skills
Mess up the messages	may not take too long	yes	???	maybe ???
Crypto-attack	25 hours + a lot more	maybe	credit card infomations etc	maybe
Apply for scholorship/ research fund	maybe a year	nobody will test it	lots of money publications a degree etc etc	yes !