

ECE 646:
Cryptography and Computer Network-Security
Fall 2005
George Mason University
Professor Kris Gaj

Project Specification:
“Attacks on MD5 hashed passwords”

Version 3
October 1, 2005

Team Members
Elizabeth J. Goff
Antony G. Robertiello
Kiran A. Bandla

1. Introduction

Today, many network protocols that require user authentication (such as those used for instant messaging), utilize Message Digest 5 (MD5) hashes to encrypt passwords sent from a user client to the system server. Often this is the only information that is encrypted in the authentication exchange. When transmitted over wireless networks, for example, these transmissions are subject to intercept, which means a cracker has access to user identification in plain text and password as a MD5 hash. These protocols, such as America Online's Instant Messenger (AIM®) and YAHOO!® Messenger, depend on the strong hashing function provided by MD5, but is hashing the password alone good enough to protect it?

In 2003, Philippe Oechslin's paper [2] introduced Rainbow Tables, a time-memory trade-off used for cryptanalysis of hashed passwords. Since then, Rainbow Tables have been used extensively to break Windows LAN Manager passwords. We plan to explore the possibility of using Rainbow Tables as a cryptanalytic tool to break other password schemes, such as the MD5 hashes used for user authentication in instant messenger protocols. We will also be doing a comparison of Rainbow Table scheme with the more traditional dictionary attack. We will look at pre-computation time, analysis time, storage, and other factors relevant to these two attacks.

a. Motivations

Many protocols use hashes to secure passwords for remote logins or user authentication to access network services. In most cases, the user identification information and these hashes are sent as plain-text over a wired or wireless network. Considering the ease of capturing wireless network traffic and the growing popularity of wireless "Hot Spot" usage for electronic mail, instant messaging, and possibly e-commerce transactions, an analysis needs to be made of the various attacks on these password schemes and the ease at which they can be broken.

b. Originality and Practicality

Though fairly extensive work has been done with Rainbow Tables and the LAN Manager password scheme, very little analysis has been done with regard to Rainbow Tables and MD5 password schemes. Also, we have not discovered any research on the performance differences between using lookup tables and dictionary attacks. This study is useful because it shows the differences in attacks on hashed passwords. It is practical in not only showing security (or insecurity) of passwords and password schemes, but could be applied to password audit capability as well.

2. Protocols, algorithms

The MD5 hash is currently the most widely distributed hashing algorithm in use. Other hashes have been compromised or are not in common use anymore.

We plan to compare Rainbow Tables and Dictionary attacks because they are the most practical password cracking tools.

Two of the most commonly used instant messaging programs, AOL Instant Messenger and YAHOO!® Messenger, use MD5 hashes to secure their passwords during authentication.

3. Problems and Hypotheses

By sending plain text user identification and MD5 hash of just the password, users of these protocols are almost daring someone to try and break them. Since we are talking about using a hash of just the password, which tends to be short "message", the security of the password is not as dependent on strength of the hashing algorithm as it is on the "strength" of the password itself. Simple passwords are vulnerable to both Rainbow Table and Dictionary attacks.

What can be done to improve the security of these protocols and the hashing algorithms, especially if they will be used over wireless networks, where interception of clear text data and even encrypted/hashed data is possible? A simple salting of the password before hashing would significantly increase the effort required to crack even a "simple" password using either of these methods. There could be other simple options as well to improve security of the protocols and use of the hashing algorithm(s).

Part of this effort will show that "simple" passwords are easy to crack and that salting passwords before hashing significantly increases effort required cracking passwords using these two methods.

4. Questions we will be seeking an answer to

- a. When would you use a Dictionary attack vs. a Rainbow Table attack?
- b. What are the resource requirements for each type of attack? Which uses more storage? Which takes more pre-computation? Which requires more analysis time? (per-hash vs. batch cracking)
- c. How did these protocols (e.g. AIM® and YAHOO!® Messenger) evolve over time? Have previous weaknesses in authentication been addressed? What discoveries led to changes in these protocols? Can the protocols be improved further? What can be done or needs to be done in the future to secure these protocols?
- d. What are the implications of time-memory trade-offs such as Rainbow Tables being able to identify passwords? How does this affect the use of MD5 as a hashing algorithm for passwords?
- e. What is the feasibility of these attacks on hashes... considering pre-computation, storage and analysis time, plus any optimization of computations?
- f. What are the pre-computation time, look-up & cracking time, and storage necessary for a Rainbow Table attack versus a Dictionary attack?

5. Outline of Final Report

- a. Introduction
- b. Review of MD5 hashes
 - i) How MD5 works
- c. Rainbow Tables
 - i) What are Rainbow Tables
 - ii) How do they work
 - iii) What are the advantages and disadvantages of using them
 - iv) Computation information (how long to build tables, how long to crack, etc.)
- d. Dictionary Attacks
 - i) What is a Dictionary Attack
 - ii) How does it work
 - iii) What are the advantages and disadvantages of using this attack
 - iv) Computation information (how long to crack, etc.)
- e. Protocols using MD5 hashes for passwords
 - i) America On-line (AOL) Instant Messenger (AIM®)
 - (1) Discussion of protocol
 - (2) Evolution of protocol
 - ii) YAHOO!® Instant Messenger
 - (1) Discussion of protocol
 - (2) Evolution of protocol
 - iii) Others
- f. Analysis
 - i) Comparison of two cracking techniques
 - (1) Pre-computation time
 - (2) Lookup/analysis time
 - (3) Storage requirements
 - ii) Results and analysis of two cracking techniques against protocols using MD5 hashes
 - iii) Impact of salting password before hashing on cracking time
 - iv) Other Considerations
- g. Enhancements / Optimization

- i) Suggestions for improving use of MD5 hash for passwords
- ii) Possible improvements to protocols using MD5 hashed passwords
- h. Summary and Conclusion
- i. Appendix
 - i) Applications that use MD5 hashes for security
 - ii) Tools for Rainbow Tables

6. Time Schedule

- a. October 1, 2005 – Final specification
- b. October 17, 2005 – First Progress Report
 - i) Understanding Rainbow Tables
 - ii) Understanding Dictionary Attacks
 - iii) Begin analysis of computation time for various password lengths
 - iv) Analysis of protocols using MD5 hashes for passwords
- c. November 14, 2005 – Second Progress Report
 - i) Finish computation time analysis
 - ii) Begin lookup / cracking time analysis for various password lengths
 - iii) Begin storage analysis for various password lengths
- d. December 6, 2005 – Final Progress Report
 - i) All research finished
 - ii) Draft of presentation
- e. December 12, 2005 – Project Report
- f. December 19, 2005 – Presentation

7. Possible Areas of Change

Depending on the progress of the research, there might be possible changes in specifications in regard to analysis of the challenge-response and issues related to MD5 rounds. However, the goal will still remain cracking MD5 hashes using Rainbow tables.

If time permits, we may implement dictionary attacks to discover passwords for these AIM® and YAHOO!® Messenger protocols from monitored wireless network transmissions.

8. References / Literature

- [1] R. Rivest (April 1992). "RFC 1321 - The MD5 Message-Digest Algorithm."

- [2] P. Oechslin, "Making a Faster Cryptanalytic Time-Memory," Proceedings of Crypto'03, 2003. Available: <http://lasecwww.epfl.ch/~oechslin/publications/crypto03.pdf>
- [3] M. E. Hellman. A cryptanalytic time-memory trade off. IEEE Transactions on Information Theory, IT-26:401–406, 1980.
- [4] Z. Shuanglei. (2004, January 1) "Parameter optimization of time-memory trade-off cryptanalysis in RainbowCrack," Project RainbowCrack [Online] Available: www.antsight.com/zsl/rainbowcrack.
- [5] X. Wang, et. al. "Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD" - <http://eprint.iacr.org/2004/199.pdf>
- [6] D. Kaminsky 2004, Dec 6). "MD5 to be considered harmful someday" Doxpara Research [Online] Available: http://www.doxpara.com/md5_someday.pdf.
- [7] Neal Hindocha (2003, January). "Threats to Instant messaging", Symantec Security Response Whitepaper [Online]. Available: <http://securityresponse.symantec.com/avcenter/reference/threats.to.instant.messaging.pdf>
- [8] "Yahoo Messenger Protocol" [Online]. Available: <http://www.venkydude.com/articles/yahoo.htm>
- [9] X. Wang and S. Manoharan. "Comparative Analysis of Instant Messaging." *From Proceeding (431) Advances in Computer Science and Technology - 2004*. Available: <http://www.actapress.com/PaperInfo.aspx?PaperID=17278>.
- [10] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," Proceedings of the 9th ACM conference on Computer and communications security, Session - Authentication and authorization: 161 - 170, 2002.
- [11] I. Thomson (2005, March 14) "Microsoft to abandon passwords," CeBIT [Online] Available: <http://www.vnunet.com/vnunet/news/2126966/microsoft-abandon-passwords>.
- [12] J. Davis (2005, March 12). "Password Cracking and Time-Memory Trade Off" [Online] Available: http://neworder.box.sk/newsread_print.php?newsid=13362
- [13] M. Stamp (2003, July 26). "Once Upon a Time-Memory Tradeoff" [Online] Available: <http://www.cs.sjsu.edu/faculty/stamp/RUA/TMTO.pdf>
- [14] A. Biryukov (2005). "Some Thoughts on Time-Memory-Data Tradeoffs," Cryptology ePrint Archive [Online]. Available: <http://eprint.iacr.org/2005/207.pdf>
- [15] Gaim Source code – <http://gaim.sf.net>
- [16] OSCAR <http://iserverd.khstu.ru/oscar/>