Optimized Attack for NTLM2 Session Response

Daiji Sanai & Hidenobu Seki SecurityFriday.com

2004.10.15

Topics of Discussion

- Is Windows authentication really weak?
- Learn more about Windows authentications.
 - Windows authentication method
 - Vulnerability of hashes
 - Vulnerability of network authentication
 - NTLM2 Session Response
- Techniques for high-speed password analysis

Windows authentication is weak!

- What? Who said so?
- Which protocol does your company use?
 POP3, FTP, HTTP, TELNET,.....
- Even experts are confused by a lot of misinformation and misunderstanding on Windows authentication.

Is it possible to steal authentication passwords?

- "From authentication" is important!
- Where can you find authentication passwords?
 - Passwords stored by servers
 - Passwords stored by clients
 - Authentication credentials traveling on the network

FYI: How to steal a password

- Where do you keep your password?
 - In your memory, Notepad, application software for PC, or PostIt

But not

today's topic!

- Advanced techniques are not necessarily required for:
 - Ask password
 - Sneak password
 - Social engineering
 - Scavenge in a recycle bin
 - Keylogger

Where are authentication passwords stored?

- Where does Windows store authentication passwords?
- Local account
 - SAM (Security Account Manager)
- Domain account
 - Active Directory

How are passwords stored?

- Windows 9x/Me
 - RC4 encryption of data using a password
 - PWL files
- Windows NT/2000/XP/2003
 - LM hash or NTLM hash

LM hash

- DES encryption of a fixed value using a password as a key
- Passwords should not exceed 14 characters
- Every 7 characters in a password are encrypted separately
- Upper/lower cases are not distinguished
- Total number of passwords made of alphanumerics and symbols: about 7.5 trillion

NTLM hash

- A password is hashed with MD4
- A password of up to 127 characters is valid
- Upper/lower cases are distinguished
- A password is not divided by every 7 characters
- Innumerable patterns

Password credentials traveling on the network

- LM authentication
- NTLMv1 authentication
- NTLMv2 authentication
- NTLM2 Session Response
- Windows Kerberos



LM response

- LM hash
 - Passwords made up of alphanumerics and symbols: about 7.5 trillion
- Attackers can instantaneously determine if a password exceeds 7 characters or not.
- Does not protect against precomputed dictionary attacks
 - Server sending a fixed challenge



NTLMv1 response

- NTLM hash
- Does not protect against precomputed dictionary attacks
 - Server sending a fixed challenge
- Concerns
 - DES key space is not large enough: 2⁵⁶ = About
 70 quadrillion



NTLMv2 response

- NTLM hash
- DES is not used
- The client sends a challenge
 - Protects against precomputed dictionary attacks
- A domain/workgroup name is included in cryptography
 - Not easy to use since a domain/workgroup name is mandatory
- Hardly in use



Windows Kerberos

- NTLM hash
- DES is not used
- The client sends a challenge
 - Protects against precomputed dictionary attacks
- Sniffing is still valid for password cracking
- Users or administrators can't force its use
 - Attackers can change conditions on purpose to avoid its use

Comparison of Windows

Authentications

	LM	NTLMv1	NTLM2 session response	NTLMv2	Windows Kerberos
Password case sensitive	No	Yes	Yes	Yes	Yes
Hash algorithm	DES (ECB mode)	MD4	MD4	MD4	MD4
Hash value length	64bit + 64bit	128bit	128bit	128bit	128bit
Client challenge	No	No	Yes	Yes	Yes
Response key length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit	128bit
Response algorithm	DES (ECB mode)	DES (ECB mode)	DES (ECB mode)	HMAC_MD5	HMAC_MD5 & RC4
Response value length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit	36byte

Hashes and Responses by OS

	password hash	LM	NTLMv1	NTLM2 session response	NTLMv2	Windows Kerberos
9x/Me	not LM/NTLM				\bigcirc	
NT4.0	LM/NTLM				\bigcirc	
2000	LM/NTLM	~SP2 •	~SP2 •	○ SP3~ ●	\bigcirc	\bigcirc
ХР	LM/NTLM	\bigcirc	\bigcirc		\bigcirc	\bigcirc
2003	LM/NTLM	0	0		\bigcirc	\bigcirc

Vulnerability of Windows authentications

- These are different!
 - Vulnerability of hashes
 - Vulnerability of network authentication
- Well-known vulnerability
 - Division into groups of 7 characters for encryption (LM hash and LM authentication)
 - Downward compatibility (LM hash and LM authentication)
 - Rainbow table (LM hash and NTLM hash)

Vulnerability of hashes

- Ultra high-speed analysis using a rainbow table
- If a hash is cracked, it is too late
 - Useful for administrators?

Rainbow Table

- Analytical technique used to determine a password from a hash
- Optimized for Windows hashes
- Lists every password possible and its corresponding precomputed hash in order to:
 - Enable ultra high speed
 - Reduce database sizes
- Cannot be used for LM/NTLM authentication using a challenge-response scheme

Effects of a rainbow table

- Examples of RainbowCrack for LM hash
 - Total number of passwords: 80.6 billion (alphanumerics)/7.5 trillion (+ symbols)
 - Time required for precomputing: 5 days/2 years
 - Disk size: 3GB/119GB
 - Time required for analysis: within 20 seconds (+ 2 minutes and a half for disk access)/within 13 minutes (+ one hour and a half for disk access)

Vulnerability of network authentications

- Corporate employees can easily obtain network authentication credentials
- It is difficult to prevent authentication packets from leaking

A strong authentication is vitak

Analysis tools for network authentications

- Well-known tools
 - ScoopLM/BeatLM
 - Cain
 - LC (LOpht Crack)

Brute-force attacks against LM authentication

- Any password can be cracked within 2 months
 - In a round-robin fashion
 - Total number of passwords made of alphanumerics and symbols: about 7.5 trillion
- LM authentication is weak and dangerous!

Don't use LM authentication

Applying a rainbow table to network authentication

- It's said to be inapplicable to LM/NTLM authentication, but...
- We reported on BugTraq (2004//) that:
 - A rainbow table can be used for NTLMv1 if the server sends a fixed challenge
- But it can't be used for the client challenge
 - NTLMv2 authentication
 - NTLM2 session response

NTLM2 session response

- Authentication method changed behind the scenes
 - Implemented on Windows 2000
 - Used by default on Windows 2000 SRP1 or later
- SRP1 is included with SP3 or later
 - Used by default on Windows XP/2003
- Currently used by default but not prevailing
- The packet format is almost the same as that of NTLMv1

NTLM2 session response

- In July 2003, Mr. Eric Glass found out how it works
- Countermeasure for precomputed dictionary attacks
 - Mr. Eric Glass claims:
 - Precomputed dictionary attacks are no longer feasible
- Its official name is unknown
 - Specialists use the name given by Mr. Eric Glass:
 - NTLM2 session response



NTLM2 S.R. authentication



NTLM2 session response is used in the following situations:

- When NTLM2 session security is enabled
 - Note that the LMCompatibilityLevel registry value may not correspond to actual settings
- Only when the negotiation is complete and successful
 - Windows NT servers cannot receive it
- Even if its use is not specified, servers will use it if implemented
 - Windows 2000 server Gold can receive NTLM2 session response
- Users cannot force its use

Is it secure enough?

- Implementation of a client challenge
 Prevents attacks using a rainbow table
- Existing cracking tools cannot be used
 Cain can be used but it takes time to crack
- Is there any efficient cracking scheme?
- Is it really secure enough?

Rapid analysis techniques for NTLM2 S.R.

2 bytes to be closely watched



2 bytes to be closely watched



Precomputing



Brute-force attacks with 2-byte DES keys





Analysis Time and DB Sizes

Analysis Time (Pe	ntium 4 2.5GHz)	Decouverd	DB size (uncompressed)	
Cain	Optimized attack	Password space		
24 hours	2 seconds	73.5 billion	180GB	
7 days	8 seconds	514 billion	1.3TB	
14 days	14 seconds	1 trillion	2.5TB	
30 days	30 seconds	2.2 trillion	5.6TB	
3 months	90 seconds	6.6 trillion	17TB	
6 months	3 minutes	13.2 trillion	34TB	
1 year	6 minutes	26.8 trillion	68TB	

Brute force password space

- 8 lowercase alphabetics: 217 billion
- 6 lower/upper alphanumerics and symbols: 743 billion
- 7 lower/upper alphanumerics: 3.6 trillion
- 8 lower/upper alphabetics: 54 trillion
- 7 lower/upper alphanumerics and symbols: 71 trillion
- 8 lower/upper alphanumerics: 222 trillion

Limitation of precomputing

- All passwords cannot be covered
- Optimization through password inference algorithms
- Analysis time of up to 3 months is a more practical timeframe for attackers
- No impact on strong passwords
- It is vital to use sufficiently strong passwords

Obtaining authentication packets

- What if switching hubs are used
 - Switching hubs are not perfect
- Authentication packets are easily sent
 - Register a dummy server
 - Net crawl
 - Authentication credentials sent while web browsing

Attacks using dummy servers

- Fake a computer list
- It is easy to make an addition to the master browser
- It is also easy to add to the domain master browser
- Register a fake server with the master browser
- Use a name which would induce clicks
- Wait for the user to click

Net crawl

- Functionality to search for shared folders/printers
 - Runs when the user click on My Network
 - Obtains a computer list from a master browser
 - Searches for shared folders of all computers
 - At that time, sends authentication packets
- Enabled on Me, XP, and 2003 by default

Microsoft KB256248,276322,320138

Net crawl

- Can also operate on Windows XP SP2 regardless of the actual settings of:
 - Windows firewalls
 - File and printer sharing exception
- Can't operate on personal computers belonging to a domain

Authentication packets sent while web browsing

- This is an issue not addressed for 7 years
- Malicious web servers
 - Can obtain authentication packets by using the following tag:
 -
 - Authentication packets travel farther onto the Internet
 - In case of NT servers, including fake ones, LM authentication packets will be sent

New issue

- Authentication packets are sent out on Internet when viewing Word documents
 - WebClient service in Windows XP
- Authentication packets can be obtained on malicious web servers
 - IIS+.doc
- We detected this issue on September 3, 2004
 - We reported to Microsoft on September 6, 2004
 - Microsoft didn't consider it a critical issue
 - We made it public on NTBugTraq on September 27, 2004

Countermeasures

- Don't get a hash cracked!
- Start with the premise that a network authentication will be stolen.
- Don't use LM authentication.
- Use a sufficiently strong password.
 - Estimated strength of six months or more is required.
 - 13 trillionth password or later... :)

In closing,

Never forget:

- LM hash is different from LM authentication!
- NTLM hash is different from NTLM authentication!

Therefore,

 The vulnerability of hashes is different from the vulnerability of authentication.