

SECURITY COMPLIANCE: ENDING THE THREAT OF WEAK USER PASSWORDS FOR FILE TRANSFER SERVERS

ABSTRACT

The confidential information stored on your file transfer server is at risk! Over two-thirds of users create simple passwords that can be hacked quickly—in less than one second, in many cases. Your file transfer servers become the Achilles' heel of your network's defenses when your users are allowed to choose weak passwords. To effectively combat this risk, your secure file transfer solution must provide you with the tools you need to establish password policies that prevent weak passwords and ensure your network's security. This paper explains the threat of weak passwords and provides practical steps you can take to close the dangerous hole in your network defenses.

ENDING THE THREAT OF WEAK USER PASSWORDS FOR FILE TRANSFER SERVERS

Network administrators can secure their company networks using the most sophisticated firewalls and virtual private networks available, but, as any hacker knows, a network is only as secure as its weakest password. When network users routinely use the names of their pets or children, birth dates, the word “password,” or other easily deduced information as their passwords, the most secure network can be breached with minimal effort.

While the threat of weak passwords is significant throughout the network, it is a particular concern for file transfer servers. By their very nature, file transfer servers often stand guard at the edge of a network, linking the confidential data and files stored inside the network and external employees, vendors and customers.

Since most file transfer servers utilize simple password-based authentication over FTP and since many people who access FTP servers have the flexibility of choosing their own passwords, file transfer servers are favorite targets of hackers.

This paper describes the best approaches for protecting file transfer servers from the threat of weak user passwords.

USER CONVENIENCE TRUMPS NETWORK SECURITY

Despite nearly daily news reports of security breaches at high-profile corporations resulting in theft of proprietary information or sensitive customer data, users consistently rely on passwords that are susceptible to cracking using tools and methods readily available on the World Wide Web. Many studies have long suggested that the root of the issue lies in users’ lack of knowledge of best practices for passwords. However, as a Wichita State University study found, network users know the dangers of weak passwords but routinely dismiss the risk in favor of convenience.¹

The Wichita study found that:

- 73% of users knew they should change their passwords every three to six months, but over half confessed that they never change their passwords if they are not required to do so.
- While over half of the study participants reported that they knew they should use special characters (non-alphanumeric symbols) in their passwords, only 4.8% actually used special characters in their passwords.
- Nearly two-thirds of participants knew that their passwords should contain at least seven characters, but only 35.5% reported using passwords with seven or more characters.
- While nearly 70% of respondents knew they should not use names of family members, pets, or other personally significant names and words, over half admitted that they routinely use these types of words in their passwords.

When users are allowed to choose convenience over network security, weak passwords leave gaping holes in network security. In fact, a CERT® analysis of incidents of network security breaches over a six year period found that incidents involving weak passwords comprised 22% of all reported incidents—the single largest group of vulnerabilities.²

15 Common Weak Passwords

Relying on your users to take responsibility for the security of their passwords can lead to disastrous results. This list of common passwords illustrates the degree to which some users are willing to sacrifice the security of your network for their own convenience.

- password
- pass1234
- administrator
- 123456
- abc123
- asdf
- qwerty
- letmein
- name
- initials
- date of birth
- social security number
- company name
- security
- blank (ie: no password)

¹ Riley, Shannon. “Password Security: What Users Know & What They Actually Do,” Usability News, February 2006. (<http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.htm>)

ENFORCE SECURITY WITH BEST PRACTICES

The threat that weak user passwords pose to network security demands attention. Server administrators need a file transfer solution that gives them the power to control both the mechanism by which users authenticate (FTP, SSL or SSH) and the security of the authentication method.

A file transfer solution must allow administrators to:

- Establish and enforce password policies. When business requirements necessitate support for FTP, administrators can establish policies that require passwords to conform to a minimum length and mixture of alphanumeric and other characters, greatly decreasing the likelihood of a password being compromised.
- Use key-based authentication. When FTP is not required, administrators can shift to key-based authentication over SSH. Key-based authentication removes passwords entirely, opting instead for cryptographic keys that are more secure than passwords. Without these crucial components, administrators cannot properly secure a file transfer server against the threat of weak user passwords.

FTP IS MORE SECURE WITH WS_FTP

When you use WS_FTP Server and WS_FTP Professional together, your FTP transfers are more secure than if you use a combination of tools from different vendors. The WS_FTP suite includes a proprietary method of encrypting authentication information for standard FTP transfers— information that, with other solutions, is transferred as plain text in an unencrypted channel.

DEFEAT WEAK PASSWORDS

The WS_FTP suite of file transfer clients and servers has long been recognized for providing the highest standard in file transfer security. Ipswitch WS_FTP Server with SSH continues this tradition by introducing the security features that administrators need to devise an enforceable and effective security policy to guard against weak user passwords.

Generating strong passwords from passphrases

Password policies that require strong passwords increase the risk that some people will write down their password. To encourage passwords that are complex enough to provide the highest level of security and still memorable enough for people to learn without writing them down, introduce users to passphrases.

A passphrase can be used in its entirety or condensed to form an easy-to-remember password. By substituting similar looking special characters, the complexity can be increased even more.

Original Sentence	Passphrase	Condensed Password
I drive a '99 Jeep with four wheel drive.	I dr!ve a '99 J3ep w/ 4WD.	Ida'99J33pw/4wd
My mother was born in Glasgow in 1942.	My m0th3r was b0rn in Gl4sg0w in 1g42.	MmwbiGi1942
I married in 1999 at age 20.	I m4rr!3d in 1gg9 @ ag3 2o.	lmi1999@a20

PASSWORD POLICIES WITH WS_FTP SERVER

WS_FTP Server gives administrators complete control over user passwords by allowing them to specify the minimum security standards that a password must meet.

With WS_FTP Server, administrators can:

- Require passwords to have a minimum number of characters
- Track a number of passwords and prevent users from reusing old passwords

² Howard, John D. "An Analysis Of Security Incidents On The Internet," 1989 – 1995. (<http://www.cert.org/research/JHThesis/Chapter8.html>)

- Require passwords to have a minimum number of numeric characters
- Require passwords to have a minimum number of symbols/non-alphanumeric characters
- Require users to change their passwords at regular intervals

With complex rules governing user passwords, the likelihood of hackers deriving legitimate passwords is significantly reduced. The table below illustrates the time required to crack passwords of various strengths.

Amount of Time to Search All Possible Passwords (at 1 million passwords/second)³

Password Length (in characters)					
Character Set	4	5	6	7	8
Lowercase letters (26)	0.5 sec.	12 sec.	5.2 min.	2.2 hours	2.4 days
Lowercase letters/digits (36)	1.7 sec.	1 min.	36.7 min.	21.7 hours	32.4 days
All alphanumeric characters (62)	15 sec.	15 min.	15.8 hours	40.5 days	7 years
Printable characters (95)	1.4 min.	2.1 hours	8.6 days	2.2 years	209 years
7-bit ACSII characters (128)	4.5 min.	9.4 hours	50.9 days	17.8 years	2283 years
8-bit ACSII characters (256)	1.2 hours	12.7 days	8.9 years	2283 years	570,776 years

WHEN PASSWORDS FAIL

Even with advanced security policies forcing users to generate more secure passwords, the threat of a brute force attack remains. In a brute force attack, a hacker systematically tries every combination of characters in search of a legitimate password. With enough time and computing resources, a brute force attack can compromise any password, regardless of its strength. To answer that threat, WS_FTP Server is attack-aware: it can proactively disable an account after an administrator-specified number of failed attempts to log in, effectively shutting down any brute force attacks. In addition, WS_FTP Server encrypts all stored passwords by default, adding an additional layer of protection should the worst-case scenario of a hacker gaining access to your server ever become reality. Load balancing, clustering groups, and robust logging capabilities can ensure data retrieval and quick response in the event of a disaster. Also, client side, programmatic retries, checkpoint-restart, and auto-reconnect capabilities add to end-to-end high availability.

KEY-BASED AUTHENTICATION WITH WS_FTP SERVER

Ipswitch WS_FTP Server with SSH introduces the ability to transfer files over an SSH tunnel using the SFTP protocol.

SSH clients can authenticate to WS_FTP Server with SSH using password or public key authentication. With public-key authentication, the client's public key is stored on and trusted by the server. When the client connects, it sends a digital signature that is signed and encrypted by the client's private key. The server validates the signature against the stored public key. Since the SSH keys are never transmitted over the network — only the digital signatures — SSH keys are more secure than passwords, providing the highest security possible.

CONCLUSION

WS_FTP Server provides network administrators the tools they need to have confidence that their network perimeter is not compromised by the threat of weak passwords.

³Kessler, Gary C. "Passwords-Strengths and Weaknesses." (<http://www.garykessler.net/library/passwords.html>).

Every day Ipswitch WS_FTP solutions enable businesses to implement sound password policies that guarantee safely and reliably moving data across the Internet. Over 40 million customers in industries such as healthcare, financial, government, software development, retail, manufacturing, telecom and education use the market leading WS_FTP Server and WS_FTP Professional to manage the secure file transfer activities of their organizations.

Please visit www.ipswitch.com to learn more about WS_FTP and download a free 30-day evaluation of WS_FTP Server and WS_FTP Professional.

WHAT PEOPLE ARE SAYING ABOUT IPSWITCH WS_FTP PRODUCTS

“WS_FTP Server is the perfect HIPAA compliant file-transfer solution for us. Its security features and exceptional support from Ipswitch make it a clear-cut choice.”

— Margaret McDonald, Senior Network & Security Specialist, Pacific Medical Centers

“WS_FTP Professional is the vehicle we use to transfer our data. The encryption, security, and reporting capabilities ensure that our processing of personal client data is compliant with Sarbanes-Oxley.”

— John Beede, Team Lead, Raymond James Financial

“WS_FTP has always met my needs of simplicity, management, security, automation and value.”

— Bill Buehler, President of Foresight Automation

“I always recommend that my customers use WS_FTP software to securely upload their files and data to my server. As an owner of a Web hosting business, it is critical that I ensure that my client’s data remain safe and secure. I am fully satisfied with WS_FTP.”

— Ron Pineda, Owner, Bolibong Web Hosting

ABOUT IPSWITCH FILE TRANSFER

Ipswitch File Transfer division makes software that allows you to securely move your most valuable data. Ipswitch brands, MOVEit®, and WS_FTP® deliver industry leading secure and managed file transfer solutions to over 40 million users. For product and sales information, write to FTsalesNA@ipswitch.com. Visit www.ipswitchFT.com for more information on the Ipswitch File Transfer division and its solutions.

ABOUT IPSWITCH

More than 100 million people worldwide use Ipswitch software to monitor their networks with Ipswitch WhatsUp®, transfer files over the Internet using the market leading WS_FTP® and MOVEit® brands of secure and managed file transfer clients and servers, and communicate via Ipswitch IMail™ Server.

