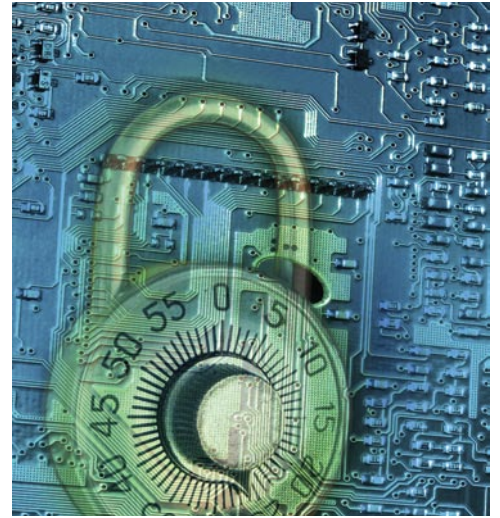


Radmin Security Brief

Radmin security

Remote control software offers great opportunities for business and home users. But whenever granting remote access to a computer, users are always running the risk of an unauthorized person getting access to their computer. Therefore, professional-grade remote control software must provide the means of protection against intruders and ensure the maximum security.



Radmin 2.2 security has long been referred to as 'paranoid' on numerous security-related forums. Radmin's security system adopted this personality because of the security breach challenge that we offered to hacker community in 2004. Famatech made one of its servers running the new installation of Radmin Server accessible through the Internet and offered a cash prize for anyone who would be successful in hacking into it. For almost 6 months of server uptime, no one managed to break the defenses.

Now the new Radmin 3.0 is even more reliable and secure than ever before. The details on how Radmin 3.0 protects itself against intrusion attempts are as follows:

1. Opt between Radmin security or Windows security

Security options have been strengthened since the previous version. The software's own security system, called Radmin security can now maintain individual user passwords and permissions. The new authentication method is based on Diffie-Hellman exchange with 2048-bit key size. Using data integrity protection and randomly generated key makes for complete immunity from any kind of attack, including 'man in the middle'.

Radmin can also use Windows native authentication services, avoiding the need to maintain separate sets of user security data, with Kerberos support available as well.

White paper

RADMIN
remote control software

2. Advanced 256-bit AES encryption for all data sent and received

Whether Windows security or Radmin security is selected, the data (desktop screens, key presses and files) being transferred over the network is strongly encrypted with the highly secure 256-bit AES algorithm. For each connection a random 256-bit key is generated and the data is checked for integrity to avoid security breach and prevent data tampering. Unlike other remote control software, the encryption in Radmin is always on and cannot be 'turned off'. The program code was optimized and the data transfer protocols were carefully inspected to ensure that the data protection works with the CPU usage not exceeding the 5% level.



3. Passwords are neither saved nor transmitted over the network

Unlike many of its competitors, Radmin ensures that the password cannot be stolen by gaining physical access to the local or remote computer. The password is stored on the Radmin Server end in the 'hash' form rather than in plain text. This hash cannot be used as a password substitute for user authorization.

The passwords for Radmin phonebook records are never stored on the Radmin Viewer end, so the program can be safely used in a corporate environment. The legitimate user can be absolutely sure that no one will be able to gain access to the remote computer in their absence. Even if the user connects from a public place such as an Internet-cafe, the remote computer will still be protected. Moreover, since passwords are never transferred over the network in any form, it doesn't make sense to try to recover passwords by merely analyzing network traffic.

4. Built-in time delays between the attempts of entering the password

Even though some users tend to use simple passwords, Radmin still remains safe. Attempts to guess the password are detected and effectively blocked by the program.



5. IP-filtering

To ensure maximum protection, Radmin Server can be configured to forbid access from other IP addresses and networks than those clearly specified in the settings.

6. Connect permission option

Radmin Server can be configured to prompt the remote user to accept an incoming connection. This option allows for making access only available if a user on the remote end accepts the connection. The connection can also be declined by the remote user when, for example, they work with private information.



7. Protected server configuration

Radmin Server settings are protected from unauthorized change. A user must have administrative privileges in order to change the settings.

8. Empty passwords are not allowed

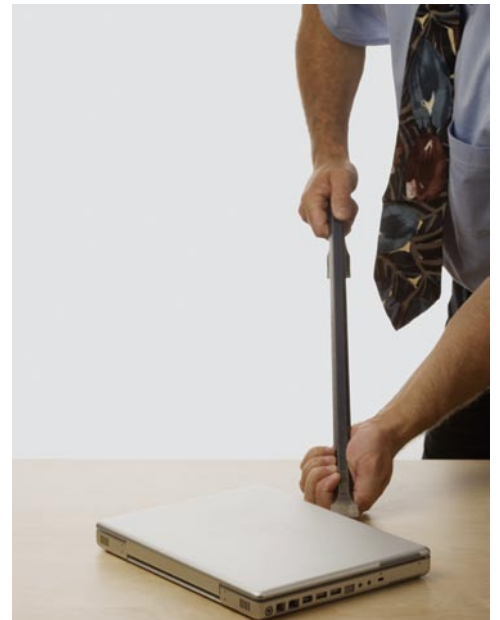
Radmin Server must be configured to use either Windows security or Radmin security. It is not possible to configure Radmin Server for remote access with the blank password.

9. Protected and digitally signed executables

Radmin has a highly secure, self-testing code that makes it practically impossible to modify the program's executable files. The code is also strongly encrypted and protected against reverse engineering. It is nearly impossible to remove the protection or make alterations to the code. Radmin program files are also digitally signed by Famatech to ensure they are authentic.

10. Connection attempts are logged

Radmin Server keeps a record of all the attempts to remotely log into the system. The log file is available in HTML format and can be used to further examine and monitor suspicious activity such as attempts to guess the password or attempts to connect at non-working hours. Logging of Windows events can also be enabled.



Possible threats prevented

Why is it so important to protect your computer from unauthorized access? The obvious answer is protecting your privacy, passwords, credit cards and other sensitive information. But there are more things to consider before making the final decision about what remote control software to use:



- Using simple passwords and storing them openly in the computer became a habit for many employees in large companies. Radmin effectively deals with the simple password problem by means of gradually increasing time delays between log-in attempts.
- Downloading and running software from non-trusted sources can alter overall computer security even if this software is not a virus. Radmin does not restrict itself to system security, but rather uses its own security to protect the program executable from being altered.
- For most networks, especially wireless networks, there is always a chance that the traffic will be monitored by someone in order to obtain sensitive information or gain access to the services inside the network. Radmin data is always strongly encrypted and passwords are never transferred over the network. Radmin data packets cannot be decrypted, modified or injected with a trojan code, thus making it impossible for a hacker to take control over the remote computer.
- Access to the remote computer can be blocked by DOS attacks, exploit crashing or placing it into the out-of-memory state. Radmin Server successfully prevents DOS attacks and is tailored to run continuously for months and even years. Radmin server always keeps CPU usage low and has proved to be very stable.