

ENGINEER



international scientific journal

ISSUE 3, 2026 Vol. 4

E-ISSN

3030-3893

ISSN

3060-5172



SLIB.UZ
Scientific library of Uzbekistan



A bridge between science and innovation



**TOSHKENT DAVLAT
TRANSPORT UNIVERSITETI**

Tashkent state
transport university



ENGINEER

A bridge between science and innovation

E-ISSN: 3030-3893

ISSN: 3060-5172

VOLUME 4, ISSUE 3

SEPTEMBER, 2026



engineer.tstu.uz

TASHKENT STATE TRANSPORT UNIVERSITY

ENGINEER

INTERNATIONAL SCIENTIFIC JOURNAL
VOLUME 4, ISSUE 3 SEPTEMBER, 2026

EDITOR-IN-CHIEF

SAID S. SHAUMAROV

Professor, Doctor of Sciences in Technics, Tashkent State Transport University

Deputy Chief Editor

Miraziz M. Talipov

Doctor of Philosophy in Technical Sciences, Tashkent State Transport University

Founder of the international scientific journal “Engineer” – Tashkent State Transport University, 100167, Republic of Uzbekistan, Tashkent, Temiryo‘lchilar str., 1, office: 465, e-mail: publication@tstu.uz.

The “Engineer” publishes the most significant results of scientific and applied research carried out in universities of transport profile, as well as other higher educational institutions, research institutes, and centers of the Republic of Uzbekistan and foreign countries.

The journal is published 4 times a year and contains publications in the following main areas:

- Engineering;
- General Engineering;
- Aerospace Engineering;
- Automotive Engineering;
- Civil and Structural Engineering;
- Computational Mechanics;
- Control and Systems Engineering;
- Electrical and Electronic Engineering;
- Industrial and Manufacturing Engineering;
- Mechanical Engineering;
- Mechanics of Materials;
- Safety, Risk, Reliability and Quality;
- Media Technology;
- Building and Construction;
- Architecture.

Tashkent State Transport University had the opportunity to publish the international scientific journal “Engineer” based on the **Certificate No. 1183** of the Information and Mass Communications Agency under the Administration of the President of the Republic of Uzbekistan. **E-ISSN: 3030-3893, ISSN: 3060-5172.** Articles in the journal are published in English language.

3	
engineer.tstu.uz	A bridge between science and innovation

Security analysis of windows local authentication recovery techniques and defensive mechanisms

M.A. Sobirov¹^a, A.A. Hamidov²^b

¹Tashkent state transport university, Tashkent, Uzbekistan

²Oxus university, Tashkent, Uzbekistan

Abstract:

Local authentication is the first line of defense in Windows environments, yet common recovery tools and forensic techniques can be exploited by attackers when defensive mechanisms are not properly configured. This research evaluates several Windows local authentication recovery scenarios, including offline SAM hash extraction, recovery-environment abuse, and Credential Guard bypass attempts, under different security configurations. Using a controlled Windows 10 testbed, we measured which credential-recovery methods succeed against full-disk encryption (BitLocker), Trusted Platform Module (TPM) protections, Secure Boot, virtualization-based security (VBS), and Credential Guard. BitLocker with pre-boot authentication effectively prevented offline hash attacks, Secure Boot blocked unauthorized boot code, and Credential Guard isolated NTLM and Kerberos credentials from memory-based extraction. Misconfigurations such as disabled encryption or VBS allowed several recovery techniques to succeed. The study presents a comparison of recovery methods against defensive controls, identifies where Windows security features still leave gaps, and offers practical recommendations, including enabling BitLocker, Secure Boot, a pre-boot PIN, and VBS, to minimize credential exposure. The results indicate that layered Windows defenses, hardware TPM, Secure Boot, BitLocker, and Credential Guard combined, substantially reduce the risk posed by local credential-recovery attacks. These findings are intended to help students, administrators, and security practitioners understand effective Windows security configurations and the practical limits of built-in recovery features under adversarial conditions.

Keywords:

Windows authentication, credential recovery, BitLocker, Secure Boot, Credential Guard, LSASS, offline attacks, local administrator, Windows Recovery Environment

1. Introduction

Windows remains the dominant desktop operating system worldwide, a position that makes it a primary target for attackers seeking unauthorized system access [1]. In most intrusions, the adversary's central goal is to obtain account credentials rather than to exploit a specific software flaw. MITRE's ATT&CK framework treats "Credential Access" as a distinct tactic, reflecting how routinely attackers attempt to steal passwords, password hashes, or Kerberos tickets once inside a system [2], [3]. Because identity verification functions as the first line of defense in any modern computing environment [4], protecting the mechanisms behind Windows authentication is not a peripheral concern, it is foundational to system security as a whole.

Microsoft has responded to this threat landscape by building a layered authentication architecture. Long-standing components, the Local Security Authority (LSA), the Security Accounts Manager (SAM), and the NTLM and Kerberos protocols, now operate alongside newer protections: full-disk encryption through BitLocker, hardware-backed key storage in the Trusted Platform Module (TPM), UEFI Secure Boot, virtualization-based security (VBS), and Credential Guard [5]. BitLocker, for instance, encrypts entire system volumes to prevent data

theft from a stolen or physically accessed disk [6], while Credential Guard uses VBS to isolate NTLM password hashes and Kerberos tickets inside a protected memory space, placing them largely out of reach of conventional extraction tools [7].

The remainder of this paper proceeds as follows. Section 2 describes the experimental methodology and the evaluation criteria applied to each recovery scenario. Section 3 reports the results, supported by comparison tables of techniques, defenses, and outcomes. Section 4 discusses these findings in light of existing Microsoft and NIST guidance. Section 5 concludes with practical recommendations for administrators and students seeking to reduce local credential exposure.

2. Research methodology

This study relied on a hands-on experimental evaluation performed on a virtualized Windows 10 Pro (version 22H2) machine. All tests ran inside VMware Workstation 17, with the guest environment configured as summarized in Table 1. Across experiments, we varied four security settings: BitLocker (disabled, TPM-only, or TPM plus PIN), Secure Boot (enabled or disabled), WinRE pre-boot authentication (enabled or disabled), and Credential Guard/VBS (enabled or disabled). Consistent with a realistic threat model, the

^a <https://orcid.org/0009-0000-4719-9481>

^b <https://orcid.org/0009-0008-9649-862X>



attacker was assumed to hold either local administrator privileges or physical access to the machine.

Table 1

Experimental environment	
Component	Specification / Setting
Host OS	Windows 11 Pro, VMware Workstation 17
Guest OS	Windows 10 Pro 22H2 (64-bit)
Hardware	4-core virtual CPU, 16 GB RAM, 80 GB virtual disk
VM Security Settings	VT-x/AMD-V enabled, UEFI firmware

For each scenario, the machine was first prepared with the target security configuration, after which each recovery technique described below was attempted. Table 2 lists the evaluation criteria applied throughout: whether the technique succeeded, the type of credential or secret obtained, the approximate effort required, the security feature (if any) that blocked the attempt, and the resulting residual risk. All techniques relied on freely available tools or built-in Windows features; no proprietary or exploit-based methods were used. Four scenarios were evaluated.

Offline SAM hash extraction involved using WinRE or a bootable USB drive to load tools such as ntdsutil or chntpw and dump the SAM database to recover password hashes. WinRE-based TPM reset involved booting into the WinRE command prompt to clear the TPM owner password and subsequently read DPAPI-protected vaults that would normally require that key. Credential Guard bypass involved disabling VBS at the firmware level, or physically removing the disk, in order to examine memory or volume contents for plaintext or hashed secrets. UEFI and bootloader compromise involved attempting to install a rootkit or a malicious bootloader, a scenario that requires Secure Boot to be disabled beforehand.

Table 2

Security evaluation criteria	
Criterion	Description
Success of Recovery	Credentials/secrets recovered (Yes/No)
Recovered Data	NT hash, Kerberos ticket, or DPAPI secret
Time / Effort	Estimated time and attack complexity
Blockers	Security features preventing recovery

For every scenario, we recorded whether authentication data, a password, hash, or LSA secret, was obtained, and we noted the primary security mechanism, if any, that prevented the attack. All experiments were carried out on our own devices under our institution's ethics policy, and no private or third-party data was accessed at any point.

3. Results and Discussions

Each recovery method was applied systematically, and the outcomes were recorded across three summary tables. Table 3 compares the recovery techniques against the protective configurations under which they were tested. Table 4 compares the relevant Windows security features in

terms of what they protect and where their known limitations lie. Table 5 provides an overall risk assessment for the main threat conditions identified during testing.

Table 3

Recovery technique comparison			
Scenario	Recovery	Risk	Defense
Offline SAM	Yes	Local account compromise	BitLocker
UEFI rootkit	Yes	System compromise	Secure Boot
WinRE reset	Yes	DPAPI exposure	PIN + Disable WinRE
CG bypass	Yes	LSASS dump	VBS + CG
TPM reset	Yes	TPM key theft	TPM PIN

It should be noted that Table 3 reflects outcomes under the specific column condition described, for instance, the offline SAM row assumes BitLocker is absent. When BitLocker, Secure Boot, and VBS are enabled together, both offline SAM attacks and credential extraction from memory fail consistently.

Table 4

Windows security feature comparison		
Feature	Protection	Main Limitation
BitLocker	Offline disk protection	Needs TPM + PIN
Windows Hello	Secure local login	Local PIN only
Credential Guard	Protects credentials	Requires VBS
Secure Boot	Stops bootkits	Needs UEFI support
WinRE	Recovery environment	Must be secured

Across the experiments, BitLocker proved to be the single most decisive control. With BitLocker enabled under a TPM-plus-PIN configuration, no offline SAM or DPAPI recovery attempt succeeded; the data remained encrypted throughout [6], [10], and even an attacker with administrative rights could not boot a recovery environment without supplying the correct PIN. With BitLocker disabled, or with the key already known, recovering the SAM or DPAPI secrets required little effort. This is consistent with Microsoft's own description of BitLocker as a control that renders data inaccessible without the appropriate key [6], [10].

Secure Boot behaved just as consistently, blocking every attempt to load unauthorized boot code. Once Secure Boot was disabled in firmware, however, we were able to install a custom bootloader and bypass Windows authentication with relatively little difficulty; re-enabling Secure Boot closed this avenue entirely [9]. A related pattern held for the TPM reset scenario; attempts to clear the TPM owner via WinRE only produced results when the TPM itself was not already protected by a BitLocker PIN.



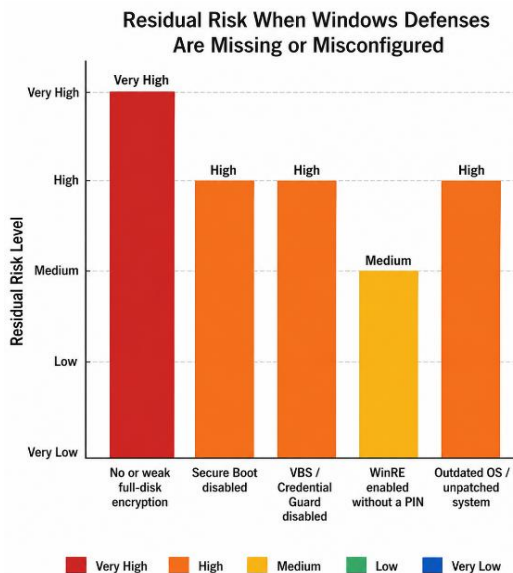


Fig. 1. Overall risk assessment when defenses are missing or misconfigured. Weak or absent full-disk encryption carries the highest residual risk, followed by disabled Secure Boot and disabled VBS / Credential Guard

Figure 1 summarizes the residual risk associated with each missing or weakened layer of defense. Weak or absent disk encryption carries a very high risk rating, since it allows an attacker to crack the SAM database offline and recover essentially all local passwords; disabling VBS or Credential Guard carries a similarly high risk of credential theft. Taken together, these results demonstrate that combining BitLocker, Secure Boot, and VBS/Credential Guard neutralized every recovery attack attempted in this study.

Discussion

These experimental findings align closely with existing Microsoft and NIST guidance [11]. UEFI Secure Boot is explicitly designed to ensure that a device boots only software trusted by its manufacturer [9], which matches our observation that Secure Boot completely blocked every low-level boot attack attempted. BitLocker's stated design goal, providing encryption for entire volumes in order to mitigate data theft [6], was likewise confirmed: every scenario in which credentials were successfully recovered involved either disabling or circumventing BitLocker. When BitLocker was active with a TPM-plus-PIN configuration, encrypted volumes stayed protected even under full physical access, and encrypted files remained unreadable without the correct key [10].

In short, the data collected here show that modern Windows security features perform well against offline and local attacks when they are correctly configured: BitLocker stops offline hash-cracking [6], [10], Secure Boot stops bootkits [9], and Credential Guard stops in-memory credential harvesting [7]. What residual risk remains is driven mainly by human and configuration factors, forgotten PINs, default settings left unchanged, or features disabled for convenience, a pattern broadly consistent with prior security literature emphasizing hardware-rooted trust and the inherent limitations of password-based recovery [12], [13].

4. Conclusion

This study systematically evaluated Windows local authentication recovery techniques against current defensive mechanisms, implementing realistic attack scenarios in a controlled environment and measuring their success. Four conclusions follow from the results. First, full-disk encryption through BitLocker with a pre-boot PIN is essential; it eliminated every offline recovery attack tested [6], [10]. Second, UEFI Secure Boot must remain enabled to prevent bootloader and rootkit compromise [9]. Third, virtualization-based isolation through Credential Guard is highly effective against in-memory credential theft [7]. Fourth, built-in recovery tools such as WinRE pose a genuine risk when left unsecured, since they can be abused to reset the TPM and access otherwise protected credential stores.

By combining hands-on experimental evaluation with a security-focused analysis, this work offers practical insight into how Windows authentication can be protected in practice. The results show that Windows already provides strong protections, but that these protections must be applied correctly, otherwise, attackers can still exploit the very recovery features meant to help legitimate users. Future work could extend this analysis to recovery mechanisms on other platforms, such as macOS recovery mode or Linux initramfs-based recovery, or examine network-based credential protocols within a similarly defensive framework [14].

References

- [1] StatCounter GlobalStats, "Desktop Operating System Market Share Worldwide," 2026. [Online]. Available: <https://gs.statcounter.com/os-market-share/desktop/worldwide>. [Accessed: Jul. 22, 2026].
- [2] MITRE, "Credential Access (TA0006)," MITRE ATT&CK, 2024. [Online]. Available: <https://attack.mitre.org/tactics/TA0006/>. [Accessed: Jul. 22, 2026].
- [3] R. A. Grimes, Hacking the Hacker: Learn from the Experts Who Take Down Hackers. Indianapolis, IN, USA: Wiley, 2017.
- [4] M. Bishop, Computer Security: Art and Science, 2nd ed. Boston, MA, USA: Addison-Wesley, 2019.
- [5] Microsoft, "Windows Security Documentation," Microsoft Learn, 2024. [Online]. Available: <https://learn.microsoft.com/en-us/windows/security/>. [Accessed: Jul. 22, 2026].
- [6] Microsoft, "BitLocker Drive Encryption Overview," Microsoft Learn, 2024. [Online]. Available: <https://learn.microsoft.com/windows/security/operating-system-security/data-protection/bitlocker/overview>. [Accessed: Jul. 22, 2026].
- [7] Microsoft, "Credential Guard Overview," Microsoft Learn, 2024. [Online]. Available: <https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/>. [Accessed: Jul. 22, 2026].
- [8] Microsoft, "Windows Hello for Business Overview," Microsoft Learn, 2024. [Online]. Available: <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/>. [Accessed: Jul. 22, 2026].



[9] Microsoft, "What Is Secure Boot for Windows?," Microsoft Learn, 2024. [Online]. Available: <https://learn.microsoft.com/en-us/windows-hardware/drivers/bringup/secure-boot>. [Accessed: Jul. 22, 2026].

[10] Microsoft, "Windows Recovery Environment (Windows RE) Technical Reference," Microsoft Learn, 2024. [Online]. Available: <https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-recoveryenvironment--windows-re--technical-reference>. [Accessed: Jul. 22, 2026].

[11] National Institute of Standards and Technology, Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, Rev. 5. Gaithersburg, MD, USA: U.S. Department of Commerce, 2020, doi: 10.6028/NIST.SP.800-53r5.

[12] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Indianapolis, IN, USA: Wiley, 2020.

[13] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Hoboken, NJ, USA: Pearson, 2020.

[14] M. A. Sobirov, I. S. Kurbanova, and Z. O. Sabirova, "Multi-Level Approach in Organizing the Energy Supply System in Telecommunication Networks," in Proc. 2023 IEEE XVI Int. Sci. Tech. Conf. Actual Problems of

Electronic Instrument Engineering (APEIE), Novosibirsk, Russian Federation, 2023, pp. 1830–1834, doi: 10.1109/APEIE59731.2023.10347846.

Information about the author

**Muzaffar
Sobirov**

Tashkent State Transport
University, Department of
Information Systems and
Technologies in Transport,
Independent Researcher

E-mail:

muzaffarsobirov538@gmail.com

Tel.: +998909314809

<https://orcid.org/0009-0000-4719-9481>

**Abdullah
Hamidov**

Oxus University, BSc in
Computer Science, Student

E-mail:

hamidovabdulloh734@gmail.com

Tel.: +998940093627

<https://orcid.org/0009-0008-9649-862X>



Kh. Tuychiev, Kh. Tuychiev

Assessment and improvement of constructive safety of the Damas light passenger vehicle.....5

A. Azizov, F. Sindarov

Comparison of the switch control circuit with main supply and central supply circuit, and analysis of the sequence of operation of the HIIC block.....10

O. Khamidov, B. Gayratov, Sh. Kudratov, F. Djuraev

An intelligent diagnostic approach based on oil analysis for assessing the technical condition of diesel locomotive engines.....14

O. Shokirov

Scientific and practical justification of safe vehicle speeds in mountainous areas of the M-39 highway of international importance.....18

M. Sobirov, A. Hamidov

Security analysis of windows local authentication recovery techniques and defensive mechanisms.....24

U. Ziyamukhamedova, J. Nafasov, E. Turgunaliev, B. Nematov, D. Akhmedova

Investigation of the tribological properties of modified composite materials used under abrasive wear conditions28