Cryptocurrency Hot Wallet STRIDE Analysis

Component	Name	STRIDE	Attack Vector	Attack Library
Entity	E1. User	S	A1. An attacker can impersonate a user by bypassing user authentication.	1, 2, 29, 30, 31
		R	A2. An attacker can repudiate attacks by bypassing user authentication.	1, 2, 29, 30, 31
	E2. Download Server	S	A3. An attacker can impersonate a provider by bypassing authentication.	1, 2, 29, 30, 31
		R	A4. An attacker can repudiate attacks by bypassing authentication.	1, 2, 29, 30, 31
	E3. Blockchain Node or API Server	S	A5. An attacker can impersonate a normal blockchain node using MITM attacks.	34, 35, 36, 37
		R	A6. An attacker can repudiate attacks using MITM attacks.	34, 35, 36, 37
		D	A7. An attacker can prevent the wallet from accessing the blockchain node using MITM attacks.	34, 35, 36, 37
		D	A8. An attacker can execute DDoS attacks using zombie malware.	33
		D	A9. An attacker can execute DoS attacks by installing malware on the blockchain node or API server.	15, 16, 17, 18
Data Store	S1. User Device (Mobile or PC)	T	A10. An attacker can modify authentication credentials, a recovery phrase, passphrase or private key using malware attacks.	13, 14, 15, 16, 17 ,18
		T	A11. An attacker can modify authentication credentials, a recovery phrase, passphrase or private key using malware with root or admin privilege.	26
		T	A12. An attacker can modify authentication credentials, a recovery phrase, passphrase or private key by getting root or admin privilege using row hammer attack.	28
		T	A13. An attacker can modify a recovery phrase, passphrase or private key by bypassing user authentication.	1, 2, 27, 29, 30, 31
		I	A14. An attacker can obtain authentication credentials, recovery phrase, passphrase or private key by bypassing user authentication.	1, 2, 27, 29, 30, 31
		I	A15. Obtain the recovery phrase or private key using physical attacks (e.g., probing, reverse engineering or cold boot attack).	4, 19
		I	A16. An attacker can obtain authentication credentials, recovery phrase, passphrase or private key using malware with root or admin privilege.	26
		I	A17. An attacker can obtain authentication credentials, recovery phrase, passphrase or private key by getting root or admin privilege using a row hammer attack.	28
		I	A18. An attacker can obtain authentication credentials, recovery phrase, passphrase or private key using a brute-force attack.	31, 32
		D	A19. Delete the wallet application or key files using factory reset or disk formatting by accessing the wallet physically.	29
		D	A20. Encrypt the wallet application key files by installing ransomware.	9, 12
Process	P1. Install or update wallet application	S	A21. An attacker can install a modified wallet application by bypassing OS authentication.	1, 2, 27, 29, 30, 31
		S	A22. An attacker can install a modified wallet application using social engineering.	15
		S	A23. An attacker can install a modified wallet application using supply chain attack.	3, 23
		T	A24. An attacker can modify the wallet application using reverse engineering.	3
	P2. Set a PIN code or password	I	A25. An attacker can obtain PIN code or password using screen recording malware.	5
		I	A26. An attacker can obtain PIN code or password using keylogger malware.	9, 10, 11
		I	A27. An attacker can obtain PIN code or password using shoulder-surfing attack.	30
		I	A28. An attacker can obtain PIN code or password by installing malware with root or admin privilege using buffer overflow attack.	26
	P3. Create a new wallet	S	A29. An attacker can create a new wallet by accessing the wallet physically and bypassing OS authentication.	1, 2, 27, 29, 30, 31
	P4. Generate a random	T	A30. An attacker can modify the seed by installing a modified wallet application using social engineering or supply chain attack.	3, 15, 23

seed	I	A31. An attacker can obtain known random seed by installing a modified wallet application using social engineering and supply chain attack.	3, 15, 23
	I	A32. An attacker can find random seed if the wallet uses a weak random number generator.	32
P5. Generate a recovery phrase and private key	I	A33. An attacker can obtain a known recovery phrase or private key by installing a modified wallet application using social engineering and supply chain attack.	3, 15, 23
	I	A34. An attacker can obtain a recovery phrase, passphrase or private key by installing a screen recorder malware.	5, 11, 24
	I	A35. An attacker can obtain a recovery phrase, passphrase or private key by installing a clipboard hijacker.	6, 7, 11, 24
	I	A36. An attacker can obtain passphrase by installing a keylogger malware.	9, 10, 11, 24
P6. Recover a wallet	S	A37. An attacker can recover a new wallet by accessing the wallet physically and bypassing OS authentication.	1, 2, 29, 30, 31
	T	A38. An attacker can modify a recovery phrase, passphrase or private key by installing a clipboard modifier malware.	8
	I	A39. An attacker can obtain a recovery phrase, passphrase, or private key by installing a screen recorder malware.	5, 11, 24
	I	A40. An attacker can obtain a recovery phrase, passphrase, or private key by installing a clipboard hijacker.	6, 7, 11, 24
	I	A41. An attacker can obtain a recovery phrase, passphrase, or private key by installing a keylogger malware.	9, 11, 24
P7. Authenticate a user	S	A42. An attacker can bypass user authentication using brute-force attack.	31
	S	A43. An attacker can bypass user authentication using evil maid attack.	1
	S	A44. An attacker can bypass user authentication using shoulder-surfing attack.	30
	S	A45. An attacker can bypass user authentication by guessing a PIN code or password.	31
	S	A46. An attacker can bypass user authentication by accessing the wallet when it is unlocked.	29
	S	A47. An attacker can bypass user authentication using physical attacks (e.g., fault injection(glitching)).	2
	D	A48. An attacker can lock the wallet by accessing the wallet and try the wrong PIN or password consecutively.	29
	E	A49. An attacker can execute authorized processes by bypassing user authentication.	1, 2, 27, 29, 30, 31
P8. Generate an account address	S	A50. An attacker can generate an account address by bypassing user authentication.	1, 2, 27, 29, 30, 31
	T	A51. An attacker can generate a fake address by modifying the wallet application using social engineering or supply chain attack.	3, 15, 23
	T	A52. An attacker can replace an address with a fake address by installing a clipboard modifier.	8
	I	A53. An attacker can obtain the account address by installing a screen recorder malware.	5, 11, 24
	I	A54. An attacker can obtain the account address by installing a clipboard hijacker.	6, 7, 11, 24
P9. Derive a public key	T	A55. An attacker can modify a public key by installing a modified wallet application using social engineering or supply chain attack.	3, 15, 23
P10. Get account balance	T	A56. An attacker can modify an account address or account balance using MITM attacks.	34, 35, 36, 37
	I	A57. An attacker can obtain an account address or account balance using MITM attacks.	34, 35, 36, 37
	D	A58. An attacker can prevent the wallet fetching account balance address using MITM attacks.	34, 35, 36, 37
	D	A59. An attacker can prevent the wallet fetching account balance address by executing DoS attacks on the blockchain node.	15, 16, 17, 18, 33
P11. Generate a transaction	S	A60. An attacker can generate a transaction by bypassing user authentication.	1, 2, 27, 29, 30, 31
	T	A61. An attacker can modify the destination address by installing a clipboard modifier.	8
	T	A62. An attacker can modify transaction information by installing a modified wallet application using social engineering or supply chain attack.	3, 15, 23

P12. Validate a transaction	I	A63. An attacker can observe transaction information by installing a screen recorder.	5, 11, 24
	I	A64. An attacker can observe transaction information by installing a clipboard hijacker.	6, 7, 11, 24
	T	A65. An attacker can modify transaction information by installing a modified wallet application using social engineering or supply chain attack.	3, 15, 23
P13. Derive a private key	T	A66. An attacker can derive a known private key by installing a modified wallet application using social engineering or supply chain attack.	3, 15, 23
P14. Sign a transaction	S	A67. An attacker can sign a transaction by bypassing user confirmation by accessing the wallet application.	1, 2, 27, 29, 30, 31
	T	A68. An attacker can modify a transaction by installing a modified wallet application using social engineering or supply chain attack.	3, 15, 23
	I	A69. An attacker can obtain a private key using side channel attacks.	20
	I	A70. An attacker can compute a private key using ECDSA nonce exploits.	21, 22
	R	A71. An attacker can repudiate confirmation by accessing the wallet application.	29
P15. Broadcast a transaction	S	A72. An attacker can impersonate a normal blockchain node using MITM attacks.	34, 35, 36, 37
	T	A73. An attacker can modify the transaction using MITM attacks.	34, 35, 36, 37
	I	A74. An attacker can obtain the transaction information using MITM attacks.	34, 35, 36, 37
	I	A75. An attacker can obtain the transaction information by installing screen recorder malware.	5, 11, 24
	D	A76. An attacker can prevent the wallet broadcasting the transaction by MITM attacks.	34, 35, 36, 37
	D	A77. An attacker can prevent the wallet broadcasting the transaction by executing DoS attacks on the blockchain node.	15, 16, 17, 18, 33
P16. Display a recovery phrase or private key	S	A78. An attacker can obtain a recovery phrase or private key by bypassing user authentication.	1, 2, 27, 29, 30, 31
	T	A79. An attacker can modify a recovery phrase or private key using a clipboard modifier.	8
	T	A80. An attacker can modify a recovery phrase or private key by installing a modified wallet application using social engineering or supply chain attack.	3, 15, 23
	I	A81. An attacker can obtain a recovery phrase or private key using screen recorder malware.	5, 11, 24
	I	A82. An attacker can obtain a recovery phrase or private key using a clipboard hijacker.	6, 7, 11, 24
P17. Register a user	S	A83. An attacker can impersonate a provider using MITM attacks.	34, 35, 36, 37
	S	A84. An attacker can impersonate a user by bypassing OS authentication.	1, 2, 27, 29, 30, 31
	T	A85. An attacker can modify personal information using MITM attacks.	34, 35, 36, 37
	I	A86. An attacker can obtain personal information using MITM attacks.	34, 35, 36, 37
	I	A87. An attacker can obtain personal information using screen recorder malware.	5, 11, 24
	I	A88. An attacker can obtain personal information using a clipboard hijacker.	6, 7, 11, 24
	I	A89. An attacker can obtain personal information using keylogger malware.	9, 11, 24

Cryptocurrency Cold Wallet STRIDE Analysis

Component	Name	STRIDE	Attack Vector	Attack Library
Entity	E1. User	S	A1. An attacker can impersonate a user by bypassing user authentication.	1, 2, 29, 30, 31
		R	A2. An attacker can repudiate attacks by bypassing user authentication.	1, 2, 29, 30, 31
	E2. Download Server	S	A3. An attacker can impersonate a provider by bypassing authentication.	1, 2, 29, 30, 31
		R	A4. An attacker can repudiate attacks by bypassing authentication.	1, 2, 29, 30, 31
	E3. Blockchain Node or API Server	S	A5. An attacker can impersonate a normal blockchain node using MITM attacks.	34, 35, 36, 37
		R	A6. An attacker can repudiate attacks using MITM attacks.	34, 35, 36, 37
		D	A7. An attacker can prevent the wallet from accessing the blockchain node using MITM attacks.	34, 35, 36, 37
		D	A8. An attacker can execute DDoS attacks using zombie malware.	33
		D	A9. An attacker can execute DoS attacks by installing malware on the blockchain node or API server.	15, 16, 17, 18
Data Store	S1. User Device (PC)	T	A10. An attacker can modify the wallet manager using malware with root or admin privilege.	26
		T	A11. An attacker can modify the wallet manager using malware attacks.	13, 14, 15, 16, 17 ,18
		I	A12. An attacker can obtain authentication credentials, recovery phrase, passphrase or private key using malware with root or admin privilege.	26
		D	A13. Delete the wallet manager using factory reset or disk formatting by accessing the wallet physically.	29
		D	A14. Encrypt the wallet manager by installing ransomware.	9, 12
	S2. Hardware Wallet Device (Embedded System)	T	A15. An attacker can modify authentication credentials, a recovery phrase, passphrase or private key by getting root or admin privilege using row hammer attack.	28
		T	A16. An attacker can modify a recovery phrase, passphrase or private key by bypassing user authentication.	1, 2, 27, 29, 30, 31
		I	A17. An attacker can obtain authentication credentials, recovery phrase, passphrase or private key by bypassing user authentication.	1, 2, 27, 29, 30, 31
		I	A18. Obtain the recovery phrase or private key using physical attacks (e.g., probing, reverse engineering or cold boot attack).	4, 19
		I	A19. An attacker can obtain authentication credentials, recovery phrase, passphrase or private key by getting root or admin privilege using a row hammer attack.	28
		I	A20. An attacker can obtain authentication credentials, recovery phrase, passphrase or private key using a brute-force attack.	31, 32
		I	A21. An attacker can obtain authentication credentials, recovery phrase, passphrase or private key by connecting a debugger (e.g., JTAG).	23
		D	A22. An attacker can delete authentication credentials, recovery phrase, passphrase or private key by connecting a debugger (e.g., JTAG).	23
		D	A23. Delete the wallet application or key files using factory reset or disk formatting by accessing the wallet physically.	29
Process	P1. Install or update wallet application	S	A24. An attacker can install a modified wallet application by bypassing OS authentication.	1, 2, 27, 29, 30, 31
		S	A25. An attacker can install a modified wallet application using social engineering.	15
		S	A26. An attacker can install a modified wallet application using supply chain attack.	3, 23
		T	A27. An attacker can modify the wallet application using reverse engineering.	3
	P2. Download firmware	S	A28. An attacker can download a modified firmware by bypassing OS authentication.	1, 2, 27, 29, 30, 31
		S	A29. An attacker can download a modified firmware using social engineering.	15
		S	A30. An attacker can download a modified firmware using supply chain attack.	3, 23

	T	A31. An attacker can modify the firmware using reverse engineering.	3
P3. Update firmware	T	A32. An attacker can modify the firmware by installing a modified wallet application using social engineering or supply chain attack.	3, 15, 23
P4. Set a PIN code or password	I	A33. An attacker can obtain PIN code or password using screen recording malware.	5
	I	A34. An attacker can obtain PIN code or password using keylogger malware.	9, 10, 11
	I	A35. An attacker can obtain PIN code or password using shoulder-surfing attack.	30
	I	A36. An attacker can obtain PIN code or password by installing malware with root or admin privilege using buffer overflow attack.	26
P5. Create a new wallet	S	A37. An attacker can create a new wallet by accessing the wallet physically and bypassing OS authentication.	1, 2, 27, 29, 30, 31
P6. Generate a random seed	T	A38. An attacker can modify the seed by installing a modified wallet application using social engineering or supply chain attack.	3, 15, 23
	I	A39. An attacker can obtain known random seed by installing a modified wallet application using social engineering and supply chain attack.	3, 15, 23
	I	A40. An attacker can find random seed if the wallet uses a weak random number generator.	32
P7. Generate a recovery phrase and private key	I	A41. An attacker can obtain a known recovery phrase or private key by installing a modified wallet application using social engineering and supply chain attack.	3, 15, 23
	I	A42. An attacker can obtain a recovery phrase, passphrase or private key by installing a screen recorder malware.	5, 11, 24
	I	A43. An attacker can obtain a recovery phrase, passphrase or private key by installing a clipboard hijacker.	6, 7, 11, 24
	I	A44. An attacker can obtain passphrase by installing a keylogger malware.	9, 10, 11, 24
P8. Recover a wallet	S	A45. An attacker can recover a new wallet by accessing the wallet physically and bypassing OS authentication.	1, 2, 29, 30, 31
	T	A46. An attacker can modify a recovery phrase, passphrase or private key by installing a clipboard modifier malware.	8
	I	A47. An attacker can obtain a recovery phrase, passphrase, or private key by installing a screen recorder malware.	5, 11, 24
	I	A48. An attacker can obtain a recovery phrase, passphrase, or private key by installing a clipboard hijacker.	6, 7, 11, 24
	I	A49. An attacker can obtain a recovery phrase, passphrase, or private key by installing a keylogger malware.	9, 11, 24
P9. Authenticate a user	S	A50. An attacker can bypass user authentication using brute-force attack.	31
	S	A51. An attacker can bypass user authentication using evil maid attack.	1
	S	A52. An attacker can bypass user authentication using shoulder-surfing attack.	30
	S	A53. An attacker can bypass user authentication by guessing a PIN code or password.	31
	S	A54. An attacker can bypass user authentication by accessing the wallet when it is unlocked.	29
	S	A55. An attacker can bypass user authentication using physical attacks (e.g., fault injection(glitching)).	2
	D	A56. An attacker can lock the wallet by accessing the wallet and try the wrong PIN or password consecutively.	29
	E	A57. An attacker can execute authorized processes by bypassing user authentication.	1, 2, 27, 29, 30, 31
P10. Get account balance	T	A58. An attacker can modify an account address or account balance using MITM attacks.	34, 35, 36, 37
	I	A59. An attacker can obtain account balance by installing a screen recorder malware.	5, 11, 24
	I	A60. An attacker can obtain an account address or account balance using MITM attacks.	34, 35, 36, 37
	D	A61. An attacker can prevent the wallet fetching account balance address using MITM attacks.	34, 35, 36, 37
	D	A62. An attacker can prevent the wallet fetching account balance address by executing DoS attacks on the blockchain node.	15, 16, 17, 18, 33

P11. Get an account address	S	A63. A malicious device can impersonate a hardware wallet by modifying the wallet firmware and installing using social engineering or supply chain attack.	3, 15, 23
	T	A64. An attacker can generate a fake address by modifying the wallet manager using social engineering or supply chain attack.	3, 15, 23
	T	A65. An attacker can replace an address with a fake address by installing a clipboard modifier.	8
	I	A66. An attacker can obtain the account address by installing a screen recorder malware.	5, 11, 24
	I	A67. An attacker can obtain the account address by installing a clipboard hijacker.	6, 7, 11, 24
P12. Derive a public key	T	A68. An attacker can modify a public key by installing a modified wallet firmware using social engineering or supply chain attack.	3, 15, 23
P13. Generate an account address	S	A69. An attacker can generate an account address by bypassing user authentication.	1, 2, 27, 29, 30, 31
	S	A70. A fake wallet manager can generate an account address by modifying the wallet manager using social engineering or supply chain attack.	3, 15, 23
	T	A71. An attacker can generate a fake address by modifying the wallet firmware using social engineering or supply chain attack.	3, 15, 23
P14. Generate a transaction	S	A72. An attacker can generate a transaction by bypassing user authentication.	1, 2, 27, 29, 30, 31
	T	A73. An attacker can modify the destination address by installing a clipboard modifier.	8
	T	A74. An attacker can modify transaction information by installing a modified wallet manager using social engineering or supply chain attack.	3, 15, 23
	I	A75. An attacker can observe transaction information by installing a screen recorder.	5, 11, 24
	I	A76. An attacker can observe transaction information by installing a clipboard hijacker.	6, 7, 11, 24
P15. Validate a transaction	T	A77. An attacker can modify transaction information by installing a modified wallet firmware using social engineering or supply chain attack.	3, 15, 23
P16. Derive a private key	T	A78. An attacker can derive a known private key by installing a modified wallet firmware using social engineering or supply chain attack.	3, 15, 23
P17. Sign a transaction	S	A79. An attacker can sign a transaction by bypassing user confirmation by accessing the hardware wallet.	1, 2, 27, 29, 30, 31
	T	A80. An attacker can modify a transaction by installing a modified wallet firmware using social engineering or supply chain attack.	3, 15, 23
	I	A81. An attacker can obtain a private key using side channel attacks.	20
	I	A82. An attacker can compute a private key using ECDSA nonce exploits.	21, 22
	R	A83. An attacker can repudiate confirmation by accessing the hardware wallet.	29
P18. Broadcast a transaction	S	A84. An attacker can impersonate a normal blockchain node using MITM attacks.	34, 35, 36, 37
	T	A85. An attacker can modify the transaction using MITM attacks.	34, 35, 36, 37
	I	A86. An attacker can obtain the transaction information using MITM attacks.	34, 35, 36, 37
	I	A87. An attacker can obtain the transaction information by installing screen recorder malware.	5, 11, 24
	D	A88. An attacker can prevent the wallet broadcasting the transaction by MITM attacks.	34, 35, 36, 37
	D	A89. An attacker can prevent the wallet broadcasting the transaction by executing DoS attacks on the blockchain node.	15, 16, 17, 18, 33

Attack Library

Num	Attack Vectors	Description
1	Nick Lewis, "Evil maid attacks: How can they be stopped?," Mar. 2016. [Online] Available: https://searchsecurity.techtarget.com/answer/Evil-maid-attacks-How-can-they-be-stopped	evil maid attack
2	Colin O'Flynn, "Stealing Bitcoins with Electromagnetic Fault Injection," in USA:Black Hat, 2019.	fault injection
3	Saleem Rashd, "Breaking the Ledger Security Model," Mar. 2018. [Online] Available: https://saleemrashid.com/2018/03/20/breaking-ledger-security-model/	supply chain attack, reverse engineering (hardware, firmware modification)
4	Courbon, Franck, Sergei Skorobogatov, and Christopher Woods, "Reverse engineering flash EEPROM memories using scanning electron microscopy," in *International Conference on Smart Card Research and Advanced Applications*. Springer, Cham, 2016.	reverse engineering, flash memory microscopy
5	Danny Palmer, "This malware will take screenshots, steal your passwords and files - and drain your cryptocurrency wallet," Apr. 2018. [Online] Available: https://www.zdnet.com/article/this-malware-will-take-screenshots-steal-your-passwords-and-files-and-drain-your-cryptocurrency/	screenshot malware
6	Graham Cluley, "Newly-discovered KryptoCibule malware has been stealing and mining cryptocurrency since 2018," Sep. 2020. [Online] Available: https://www.tripwire.com/state-of-security/featured/kryptocibule-malware-stealing-mining-cryptocurrency/	clipboard monitor
7	Lawrence Abrams, "First CryptoCurrency Clipboard Hijacker Found on Google Play Store ," Feb 2019. [Online] Available: https://www.bleepingcomputer.com/news/security/first-cryptocurrency-clipboard-hijacker-found-on-google-play-store/	clipboard hijacker
8	Brandon Levene and Josh Grunzweig, "Sure, I'll take that! New ComboJack Malware Alters Clipboards to Steal Cryptocurrency," Mar. 2018. [Online] Available: https://unit42.paloaltonetworks.com/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/	clipboard data modifier
9	Nicole Lorenz, "MysteryBot – the Android malware that's keylogger, ransomware, and trojan," Jun. 2018. [Online] Available: https://www.avira.com/en/blog/mysterybot-the-android-malware-thats-keylogger-ransomware-and-trojan	keylogger, ransomware, trojan
10	Cai, Liang, and Hao Chen, "TouchLogger: Inferring Keystrokes on Touch Screen from Smartphone Motion." *HotSec* 11.2011 (2011): 9.	smartphone touch screen logger
11	Marvin the Robot, "Cryptoshuffler trojan has quietly stolen $140,000 worth of bitcoin kaspersky lab official blog," Oct. 2017. [Online] Available: https://www.kaspersky.com/blog/ cryptoshuffler-bitcoin-stealer/19976/	trojan
12	Lindsey O'Donnell, "EvilQuest Mac Ransomware Has Keylogger, Crypto Wallet-Stealing Abilities ," Jun. 2020. [Online] Available: https://threatpost.com/evilquest-mac-ransomware-keylogger-crypto-wallet-stealing/157034/	ransomware, keylogger
13	Ophir Harpaz, Magal Baz and Limor Kessem, "Trickbot's cryptocurrency hunger: Targeting exchange users to steal coins," Feb. 2018. [Online] Available: https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/	webinjection
14	Provos, N., McNamee, D., Mavrommatis, P., Wang, K., & Modadugu, N, "The Ghost in the Browser: Analysis of Web-based Malware," *HotBots*, *7*, 4-4. 2007.	web-based malware infection
15	Peltier, T. R., "Social engineering: Concepts and solutions," *Information Security Journal*, *15*(5), 13., 2016.	social engineering
16	M. Cova, C. Kruegel, and G. Vigna, "Detection and analysis of driveby-download attacks and malicious javascript code," in *Proceedings of the 19th international conference on world wide web*. ACM, 2010, pp. 281–290., 2010.	drive-by download attack
17	Sood, Aditya K., and Richard J. Enbody, "Malvertising–exploiting web advertising," *Computer Fraud & Security* 2011.4 (2011): 11-16.	malvertising attack
18	Smutz, Charles, and Angelos Stavrou, "Malicious PDF detection using metadata and structural features," in *Proceedings of the 28th annual computer security applications conference*. 2012.	malicious PDF file
19	M. Gruhn and T. Müller, "On the Practicability of Cold Boot Attacks," 2013 International Conference on Availability, Reliability and Security, Regensburg, 2013, pp. 390-397, doi: 10.1109/ARES.2013.52.	cold boot attack
20	Jochen Hoenicke, "Extracting the Private Key from a TREZOR," [Online] Available: https://jochen-hoenicke.de/crypto/trezor-power-analysis. 2015.	side channel attack

21	Breitner, Joachim, and Nadia Heninger, "Biased nonce sense: Lattice attacks against weak ECDSA signatures in cryptocurrencies," in *International Conference on Financial Cryptography and Data Security*. Springer, Cham, 2019.	ECDSA signature attack
22	Brengel M., Rossow C. (2018) Identifying Key Leakage of Bitcoin Users. In: Bailey M., Holz T., Stamatogiannakis M., Ioannidis S. (eds) Research in Attacks, Intrusions, and Defenses. RAID 2018. Lecture Notes in Computer Science, vol 11050. Springer, Cham. https://doi.org/10.1007/978-3-030-00470-5_29	ECDSA signature same nonce exploit
23	Dmitry Nedospasov, Thomas Roth and Josh Datko, "wallet.fail", in *35th Computer Chaos Congress*, 2018. [Online] Available: https://wallet.fail/	supply chain attack, fault injection(glitching), firmware modification, JTAG debugger attack
24	M. Guri and Y. Elovici, "Bridgeware: The air-gap malware," Commun. ACM, vol. 61, no. 4, pp. 74–82, Mar. 2018. [Online]. Available: http://doi.acm.org/10.1145/3177230	bridgeware
25	M. Guri, "BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 2018, pp. 1308-1316, doi: 10.1109/Cybermatics_2018.2018.00227.	usb driver malware
26	Höbarth, Sebastian, and Rene Mayrhofer. "A framework for on-device privilege escalation exploit execution on Android." *Proceedings of IWSSI/SPMU* (2011).	buffer overflow, privilege escalation (root privilege)
27	C. Cowan, F. Wagle, Calton Pu, S. Beattie and J. Walpole, "Buffer overflows: attacks and defenses for the vulnerability of the decade," Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00, Hilton Head, SC, USA, 2000, pp. 119-129 vol.2, doi: 10.1109/DISCEX.2000.821514.	buffer overflow, code injection (control flow corruption)
28	K. S. Yim, "The Rowhammer Attack Injection Methodology," 2016 IEEE 35th Symposium on Reliable Distributed Systems (SRDS), Budapest, 2016, pp. 1-10, doi: 10.1109/SRDS.2016.012.	row hammer attack
29	Lily Hay Newman, "Cryptocurrency Hardware Wallets Can Get Hacked Too," May 2020. [Online] Available: https://www.wired.com/story/cryptocurrency-hardware-wallets-can-get-hacked-too/	physical access attack
30	Eiband, Malin; Khamis, Mohamed; von Zezschwitz, Emanuel; Hussmann, Heinrich; Alt, Florian (May 2017). "Understanding Shoulder Surfing in the Wild: Stories from Users and Observers" (PDF). *CHI '17 – Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*: 4254–4265. doi:10.1145/3025453.3025636. Retrieved May 3, 2018.	shoulder-surfing attack
31	Mike Stark, "Brute-Force Password Guessing Attacks," July 2020. [Online] Available: https://www.ibeta.com/brute-force-attacks-password-guessing/	brute-force attacks on password
32	Scott Chipolina, "How Hard Is It to Brute Force a Bitcoin Private Key?," Feb 2021. [Online] Available: https://decrypt.co/43093/how-hard-is-it-to-brute-force-a-bitcoin-private-key	brute-force attacks on private keys
33	P. K. Agrawal, B. B. Gupta and S. Jain, "SVM Based Scheme for Predicting Number of Zombies in a DDoS Attack," 2011 European Intelligence and Security Informatics Conference, Athens, 2011, pp. 178-182, doi: 10.1109/EISIC.2011.19.	DDoS attack using zombie PC
34	F. Callegati, W. Cerroni and M. Ramilli, "Man-in-the-Middle Attack to the HTTPS Protocol," in IEEE Security & Privacy, vol. 7, no. 1, pp. 78-81, Jan.-Feb. 2009, doi: 10.1109/MSP.2009.12.	MITM attack on HTTPS protocol
35	M. A. Hussain, H. Jin, Z. A. Hussien, Z. A. Abduljabbar, S. H. Abbdal and A. Ibrahim, "DNS Protection against Spoofing and Poisoning Attacks," 2016 3rd International Conference on Information Science and Control Engineering (ICISCE), Beijing, 2016, pp. 1308-1312, doi: 10.1109/ICISCE.2016.279.	DNS spoofing and poisoning attack
36	S. Puangpronpitag and N. Masusai, "An efficient and feasible solution to ARP Spoof problem," 2009 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, Pattaya, Chonburi, 2009, pp. 910-913, doi: 10.1109/ECTICON.2009.5137193.	ARP spoofing attack
37	H. Wang, C. Jin and K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," in IEEE/ACM Transactions on Networking, vol. 15, no. 1, pp. 40-53, Feb. 2007, doi: 10.1109/TNET.2006.890133.	IP address spoofing