HYPR

NIST 800-63B Threat Category	Rely on Shared Secrets				No Shared Secrets	
	Static Passwords	**SMS 2FA**	**Phone-as-a-Token MFA**	**Hard Token 2FA**	**Smart Cards (PKI)**	**True Passwordless**
Security	Low	Low	Medium	High	Very High	Highest
Theft	• Usually Stored In One Place • Users Write Them Down • Can Easily Be Shared	• OTP Easily Stolen and Reused • Only as Secure as Mobile Device • Common SS7 Network Attacks	• OTP Easily Stolen and Reused • Only as Secure as Mobile Device	• OTP Difficult to Steal and Reuse • Not Bound to Particular User	• Card Can be Stolen and Reused • Only as Secure as PIN on Card • Attacks Are Highly Targeted	• Attacks Must Be Highly Targeted • Attackers Must Have Root Access to Mobile OS
Duplication	• Written Down and Duplicated • Backups Are Easily Made	• Backups Are Often Made • Duplicated by Cloning App Data	• Backups Are Often Made • Can Be Duplicated by Cloning Application Data	• Seed Backups Are Often Made (e.g. RSA Breach)	• Not Easily Duplicated • Highly Targeted	Highly Targeted and Extremely Difficult Without Physical Access to Silicone On Chip
Eavesdropping	Malware and MITM Commonly Used to Exploit	Can Be Intercepted by Malware, MITM, and Keyloggers	OTP and MPC Can Be Intercepted by Malware and MITM	MITM Commonly Used to Exploit	• PIN Can Be Intercepted Between PC and Card Reader	Extremely Difficult Without Physical Access to Silicone On Chip
Offline Cracking	Hashed / Encrypted Passwords Can Be Cracked Offline	Hashed or Encrypted OTP/HOTP Secrets Can Be Cracked Offline	Hashed or Encrypted Secrets Can Be Cracked Offline	Hashed or Encrypted OTP/HOTP Secrets Can Be Cracked Offline	• Very Difficult, Must Be Able to Decrypt and Exploit Chip	Extremely Difficult Without Physical Access to Silicone On Chip
Side Channel Attacks	Password Size and Complexity Can Be Established Through Side Channel Analytics and Differential Power Analysis	Can Be Sniffed or Intercepted by Other Apps or Malware	• Exposed to Credential Stuffing If Using Passwords as Alias • Can Be Sniffed or Intercepted By Other Apps or Malware	Exposed Using Differential Power Analysis	Possibly Exposed to Differential Power Analysis	Possibly Exposed to Differential Power Analysis by a Very Sophisticated Attacker.
Phishing or Pharming	Passwords Are the Primary Target of Phishing	Targeted 2FA SMS 2FA Phishing (i.e. Modlishka Tool)	• OTP Susceptible to Phishing • Push Attacks Require Social Engineering (See Below)	Targeted 2FA Phishing (i.e. Modlishka Tool)	Not Possible Since Each Authentication Request Is a Unique Challenge-Response	Not Vulnerable, as Each Authentication Request Is a Unique Challenge-Response
Social Engineering	Users and Admins Duped Into Giving Password Through SE Attacks	Attacker Retrieves MFA Code Directly from User	Attacker Convinces User to Authenticate PUSH. Difficulty Depends on Implementation	Attacker Retrieves MFA Code Directly from User	Extremely Difficult as User Does Not Utilize Shared Secrets	Not Vulnerable, User Does Not Have a Shared Secret
Online Guessing	• Passwords Are Easy to Guess • People Reuse Passwords Across Multiple Services	Difficult to Guess a TOTP	• Password-Based Alias Vulnerable to Credential Stuffing & Reuse Attack • Difficult if Based on TOTP Alias	Difficult to Guess a TOTP	Not Vulnerable to Guessing Due to PKI Architecture	Not Vulnerable as Public/Private Key Pairs Are Used to Perform a Challenge-Response Mechanism
Endpoint Compromise	Vulnerable to Keyloggers, Malware	Vulnerable to Keyloggers, Malware	Vulnerable to Keyloggers, Malware	Vulnerable to Keyloggers, Malware	Not Vulnerable as Private Keys Always Remain on Smart Card	Not Vulnerable as Keys Never Leave Hardware Backed Key Store

HYPR Authentication Attack Matrix