Offchain Security Model Auxiliary

Bucket Security Method Points Maps & Requirements Maps

NB: ABK points can only be applied after verifying credentials (logging in)

▼ Bucket Level 0

Security Method Points Map

Aa Name	Points
Active Browser Key (ABK)	20.0
Email OTP	5.0
Authenticated Credentials	1.0
Authenticator MFA	0.0
Mobile SMS MFA	0.0
Passkey MFA	0.0
Ethereum Signer	0.0

Points Ruleset Map

Aa Security Action	(Points) Requirement	Notes
Login	5.0	
Reset Password	5.0	
Add Authenticator	26.0	Requires all security measures to add an MFA method: user will need to be on an active device.
Add Mobile SMS	26.0	
Add Passkey	26.0	
Change Email	26.0	
Change Authenticator	999999.0	

Aa Security Action	(Points) Requirement	Notes
Change Mobile SMS	999999.0	
Change Passkey	999999.0	
Get MFA Signature	6.0	Ensures Bucket 0 Requires Credentials + Email OTP

▼ Bucket Level 1

Security Method Points Map

Aa Name	Points
Active Browser Key (ABK)	20.0
Email OTP	5.0
Authenticated Credentials	1.0
Authenticator MFA	10.0
Mobile SMS MFA	10.0
Passkey MFA	10.0
Ethereum Signer	10.0

Requirements Map

Aa Security Action	(Points) Requirement
Login	5.0
Reset Password	15.0
Add Authenticator	30.0
Add Mobile SMS	30.0
Add Passkey	30.0
Change Email	30.0

Aa Security Action	(Points) Requirement
Change Authenticator	26.0
Change Mobile SMS	26.0
Change Passkey	26.0
Get MFA Signature	7.0

▼ Bucket Level 2

Security Method Points Map

Aa Name	Points
Active Browser Key (ABK)	20.0
Email OTP	6.0
Authenticated Credentials	1.0
Authenticator MFA	10.0
Mobile SMS MFA	10.0
Passkey MFA	10.0
Ethereum Signer	9.0
Untitled	

Requirements Map

Aa Name	(Points) Requirement
Login	6.0
Reset Password	15.0
Add Authenticator	30.0
Add Mobile	30.0
Add Passkey	30.0
Change Email	31.0

Aa Name	(Points) Requirement
Change Authenticator	28.0
Change Mobile	28.0
Change Passkey	28.0
Get MFA Signature	9.0

▼ Bucket Level 3

Security Method Points Map

Aa Name	Points	Notes
Active Browser Key (ABK)	15.0	Reduced too — want slightly more influence on MFA, why else would user have 3x?
Email OTP	1.0	Considered unsecure
Authenticated Credentials	1.0	
Authenticator MFA	11.5	
Mobile SMS MFA	11.5	
Passkey MFA	11.5	
Ethereum Signer	10.0	

Requirements Map

Aa Name	(Points) Requirement	Notes
Login	9.0	Requires an additional security method such as Mobile SMS on top of Email OTP.
Reset Password	15.0	
Add Authenticator	30.0	
Add Mobile	30.0	

Aa Name	(Points) Requirement	Notes
Add Passkey	30.0	
Change Email	32.0	
Change Authenticator	25.0	
Change Mobile	25.0	
Change Passkey	25.0	
Get MFA Signature	9.0	

▼ Bucket Level 4

Security Method Points Map

Aa Name	Points
Active Browser Key (ABK)	15.0
Email OTP	0.5
Authenticated Credentials	1.0
Authenticator MFA	10.0
Mobile SMS MFA	10.0
Passkey MFA	10.0
Ethereum Signer	9.0

Requirements Map

Aa Security Action	(Points) Requirement	Notes
Login	10.0	
Reset Password	24.0	
Add Authenticator	0.0	

Aa Security Action	(Points) Requirement	Notes
Add Mobile SMS	0.0	
Add Passkey	0.0	
Change Email	32.0	
Change Authenticator	27.0	
Change Mobile SMS	27.0	
Change Passkey	27.0	
Get MFA Signature	6.0	

User Security States

Exhaustive tables of user loss and hack states.

NB (I): Only the minimal criterion are shown. I.e. for a hack/loss state of x, y, z: any hack/loss states including x, y, z, t are ignored.

NB (II): In general, stealing an unlocked [Device, Mobile] is equivalent to stealing email

NB (III): “+” is equivalent to logical AND

NB (IV): “,” is equivalent to logical OR

NB (V): “**Other** MFA Method” refers to any MFA method not in the hacker’s possession

Bucket Level 0

▼ New User [No Security Methods]

Hack States [New User]

Aa Hacker Initial States	Action Path	Notes
Hacker Steals Email	→ Reset Password → Login → Get MFA Signature → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**	We can’t protect them beyond this, because ABK is encrypted and we can only gate that with password or OTP. So, email OTP will always be the point of failure

Loss States [New User]

Aa Loss State	Notes
Lose Email	Recoverable by Email Providers, e.g. Google, Microsoft, etc.

Bucket Level 1

▼ Low Security User [1x MFA Methods]

Hack States [Low Security User]

Aa Hacker Initial States	Action Path	Notes
Hacker Steals Email + [1x MFA Methods]	→ Reset Password → Login → Get MFA Signature → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**	Note that correlation is gonna depend on how the user chooses to set up their L2 MFA. Therefore, we should recommend the first L2 they add is yubikey or Google authenticator.
Hacker Steals Active Device + Credentials + [1x MFA Methods]	→ Login → Change Email → Get MFA Signature → **DRAIN**	
Hacker Steals Active Device + Credentials + Email	→ Login → Change MFA **Other** Method → Get MFA Signature → **DRAIN**	

Loss States [Low Security User]

Aa Loss State	Notes
Lose [Active Device, Credentials, Email] + Lose [1x	Most correlated items would be iPhone (SMS + Device ABK) —discouraging users from SMS as their only MFA

Aa Loss State	Notes
MFA Methods]	method is preferable.
Lose Email + Lose [Credentials, Device]	

▼ Ethereum Signer Only User [1x Ethereum Signer]

Hack States [Ethereum Signer Only User]

Aa Hacker Initial States	Action Path	Notes
Hacker Steals Credentials + Ethereum Signer	→ Login → Get Ethsig → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browse Key)** → **DRAIN**	Don’t store seed in 1P with your password
Hacker Steals Email + Ethereum Signer	→ Get Ethsig → Reset Password → Login → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**	

Loss States [Ethereum Signer Only User]

Aa Loss State	Notes
Loser Signer	Expected loss.
Lose Credentials + Lose Email	Technically: recoverable on-chain

Bucket Level 2

▼ Medium Security User w/ Ethereum Signer [1x MFA Methods + 1x Ethereum Signer]

Hack States [Medium Security User]

Aa Hacker Initial States	Action Path
Hacker Steals Credentials +	→ Login → Get Ethsig → Add New Browser Key **(Inactive)**

Aa Hacker Initial States	Action Path
Ethereum Signer	→ Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Active Device + Credentials + [1x MFA Methods]	→ Login → Change Email → Get MFA Signature → **DRAIN**
Hacker steals Email + [1x MFA Methods]	→ Reset Password → Login → Get MFA Signature → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Email + Ethereum Signer	→ Reset Password → Login → Get Ethsig → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**

Loss States [Medium Security User]

Aa Loss States
Lose Ethereum Signer + Lose [1x MFA Method]
Lose Credentials + Lose Email
Lose Active Device + Lose Email + Lose Ethereum Signer

▼ Medium Security User [2x MFA Methods]

Hack States [Medium Security User]

Aa Hacker Initial States	Action Path
Hacker Steals Active Device + Credentials + [1x MFA Methods]	→ Login → Change Email → Change **Other** MFA Method → Get MFA Signature → **DRAIN**
Hacker steals Active Device + Email + [1x MFA Methods]	→ Reset Password → Login → Change **Other** MFA Method → Get MFA Signature → **DRAIN**
Hacker steals Email + [2x MFA Methods]	→ Reset Password → Login → Get MFA Signature → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**

Loss States [Medium Security User]

Aa Loss States
Lose Active Device + Lose [1x MFA Methods]
Lose Email + Lose [Active Device, Credentials]
Lose [2x MFA Methods]

Bucket Level 3

▼ High Security User w/ Ethereum Signer [2x MFA Methods + Ethereum Signer]

Hack States [High Security User w/ Ethereum Signer]

Aa Hacker Initial State	Action Paths
Hacker Steals Credentials + Ethereum Signer	→ Login → Get Ethsig → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Active Device + Credentials + Email + [1x MFA Methods]	→ Login → Change **Other** MFA Method → Get MFA Signature → **DRAIN**
Hacker Steals Active Device + Credentials + [2x MFA Methods]	→ Login → Change Email → Get MFA Signature → **DRAIN**
Hacker Steals Email + Ethereum Signer + [1x MFA Methods]	→ Reset Password → Login → Get Ethsig → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Email + [2x MFA Methods]	→ Reset Password → Login → Get MFA Signature → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Ethereum Signer + [2x MFA Methods]	→ Get Ethsig → Change Email → Reset Password → Login → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**

Loss States [High Security User]

Aa Loss States
Lose [Active Device, Credentials, Email] + Lose [1x MFA Methods] + Lose Ethereum Signer
Lose Ethereum Signer + Lose Email + Lose [Credentials, Active Device]
Lose [Credentials, Ethereum Signer] + Lose [2x MFA Methods]
Lose Credentials + Lose Email + Lose [1x MFA Methods]

▼ High Security User [3x MFA Methods]

Hack States [High Security User]

Aa Initial Hacker State	Action Path
Hacker Steals Active Device + Credentials + Email + [1x MFA Methods]	→ Login → Change **Other** MFA Method → Get MFA Signature → **DRAIN**
Hacker Steals Email + [2x MFA Methods]	→ Reset Password → Login → Get MFA Signature → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Active Device + Credentials + [2x MFA Methods]	→ Login → Change Email → Get MFA Signature → **DRAIN**
Hacker Steals [3x MFA Methods]	→ Change Email → Get MFA Signature → Reset Password → Login → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**

Loss States [High Security User]

Aa Loss State	Notes
Lose [3x MFA Methods]	
Lose [Active Device, Credentials, Email] + Lose [2x MFA Methods]	

Aa Loss State	Notes
Lose Credentials + Lose Email + Lose [1x MFA Methods]	
Lose Device + Lose Email + Lose [1x MFA Methods]	

Bucket Level 4

▼ Maximum Security User [All Security Methods Enabled]

Hack States [Maximum Security User]

Aa Initial Hacker State	Action Path
Hacker Steals Credentials + Ethereum Signer + [1x MFA Methods]	→ Login → Get Ethsig → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Active Device + Credentials + [2x MFA Methods]	→ Login → Change Email → Get MFA Signature → **DRAIN**
Hacker Steals Credentials + Email + [2x MFA Methods]	→ Login → Get MFA Signature → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Email + Ethereum Signer + [2x MFA Methods]	→ Reset Password → Login → Get Ethsig → Add New Browser Key **(inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Email + [3x MFA Methods]	→ Reset Password → Login → Get MFA Signature → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**
Hacker Steals Ethereum	→ Get Ethsig → Change Email → Reset Password → Login → Add New Browser Key **(inactive)** → Wait 7 Days **(Activate Browser Key)** →

Aa Initial Hacker State	Action Path
Signer + [3x MFA Methods]	**DRAIN** ——————————————————— → Change Email → Get MFA Signature → Reset Password → Login → Add New Browser Key **(Inactive)** → Wait 7 Days **(Activate Browser Key)** → **DRAIN**

Loss States [Maximum Security User]

Aa Loss State
Lose [3x MFA Methods]
Lose [Credentials, Ethereum Signer] + Lose [2x MFA Methods]
Lose Credentials + Lose [Email, Ethereum Signer] + Lose [1x MFA Methods]
Lose [Credentials, Device] + Lose Email + Lose Ethereum Signer