



Transcending Cloud Limitations by Obtaining Inner Piece

WITH DEEPAK CHOPPA



Who am I?






- I am the terror that flaps in the night
- The modern man (secret secret)
- Just this crazy guy, y'know?



Cloud Storage

- Sharing “large” (10mb+) files w/ friends
- Availability/Accessibility
 - Replaces USB keys?
- Backups

Cloud Storage: Provider Comparison

Service					
Web Accessible	Yes	Yes	Yes	Yes	Yes
Free Quota Limit	25gb	2gb*	5gb	7gb	5gb
API Available	Yes	Yes	Yes	Yes	Yes
History Retention	Yes	28 days	Yes* (Pro)	?	?
Quota Counts Δ s	Yes	No	?	N/A	?

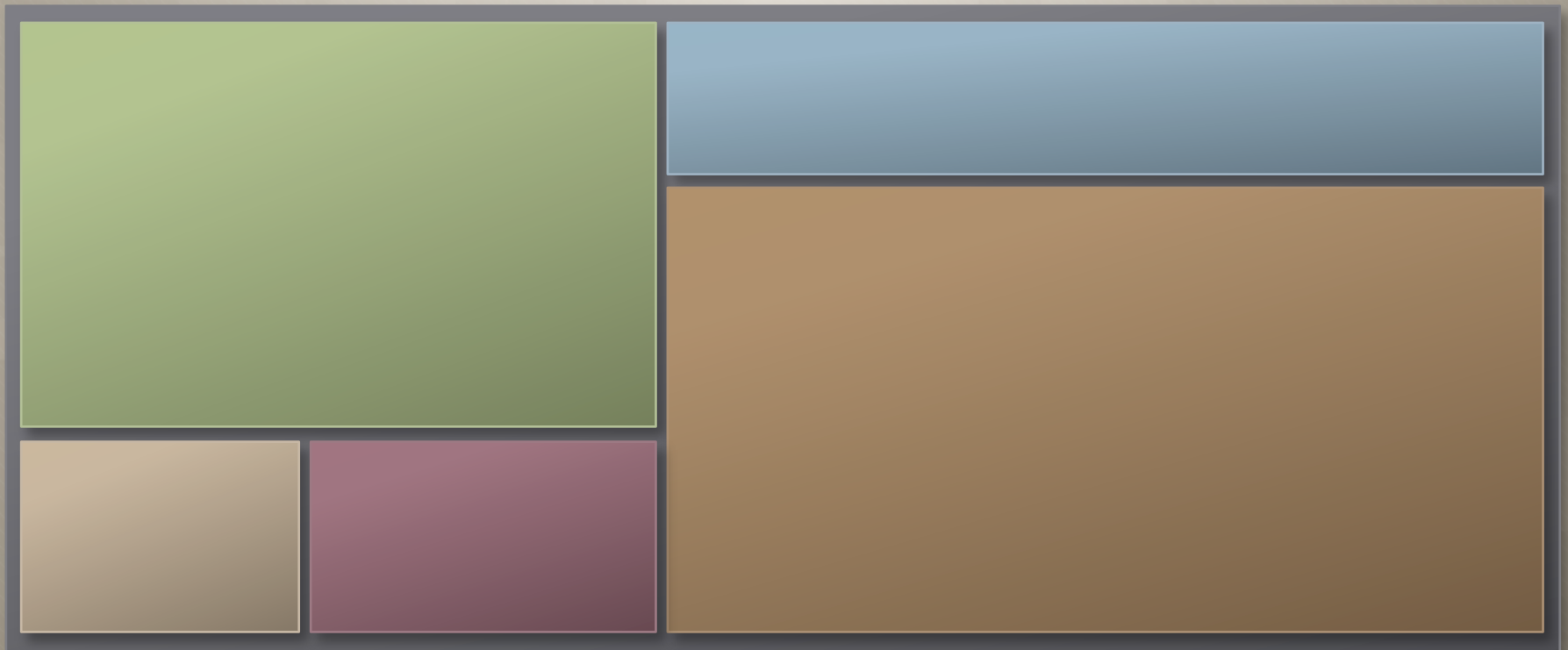


Data Representation



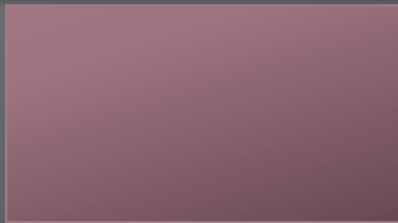


Data Representation





Data Representation





The Vulnerability

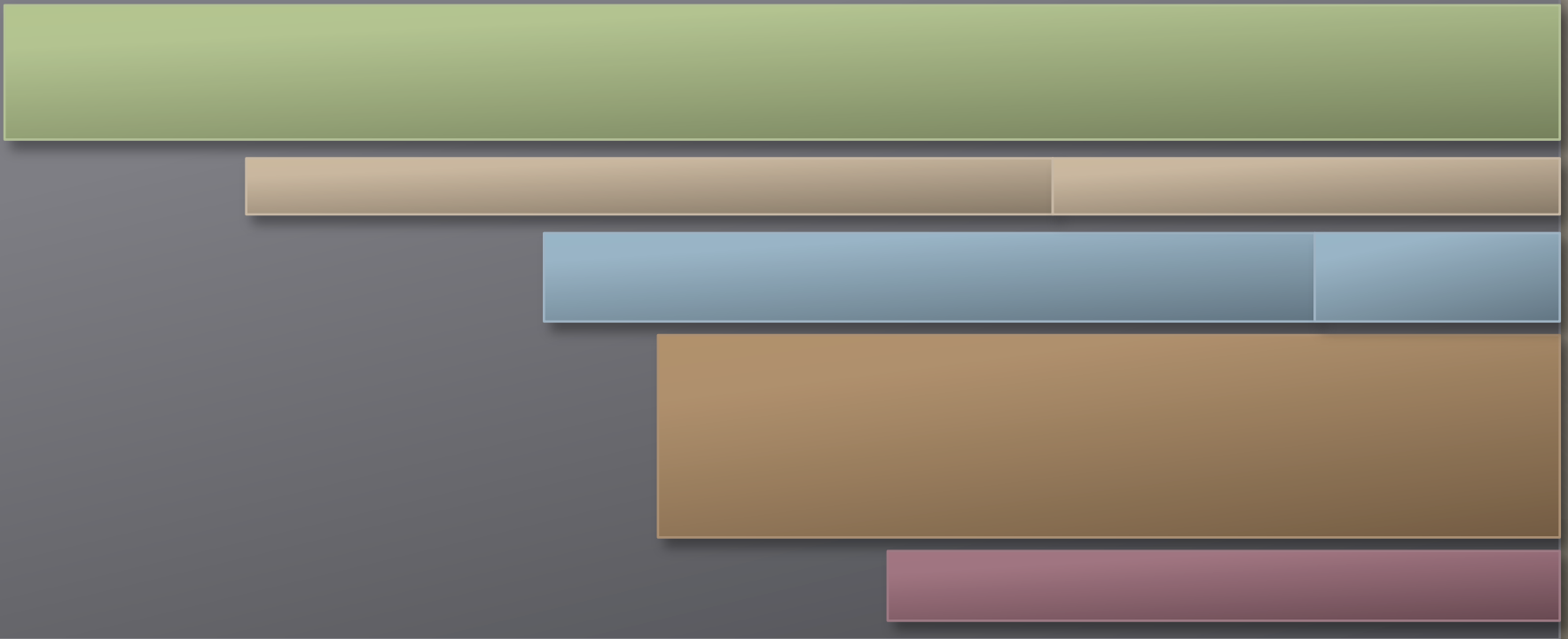
The moment you've all been waiting for



Time Representation

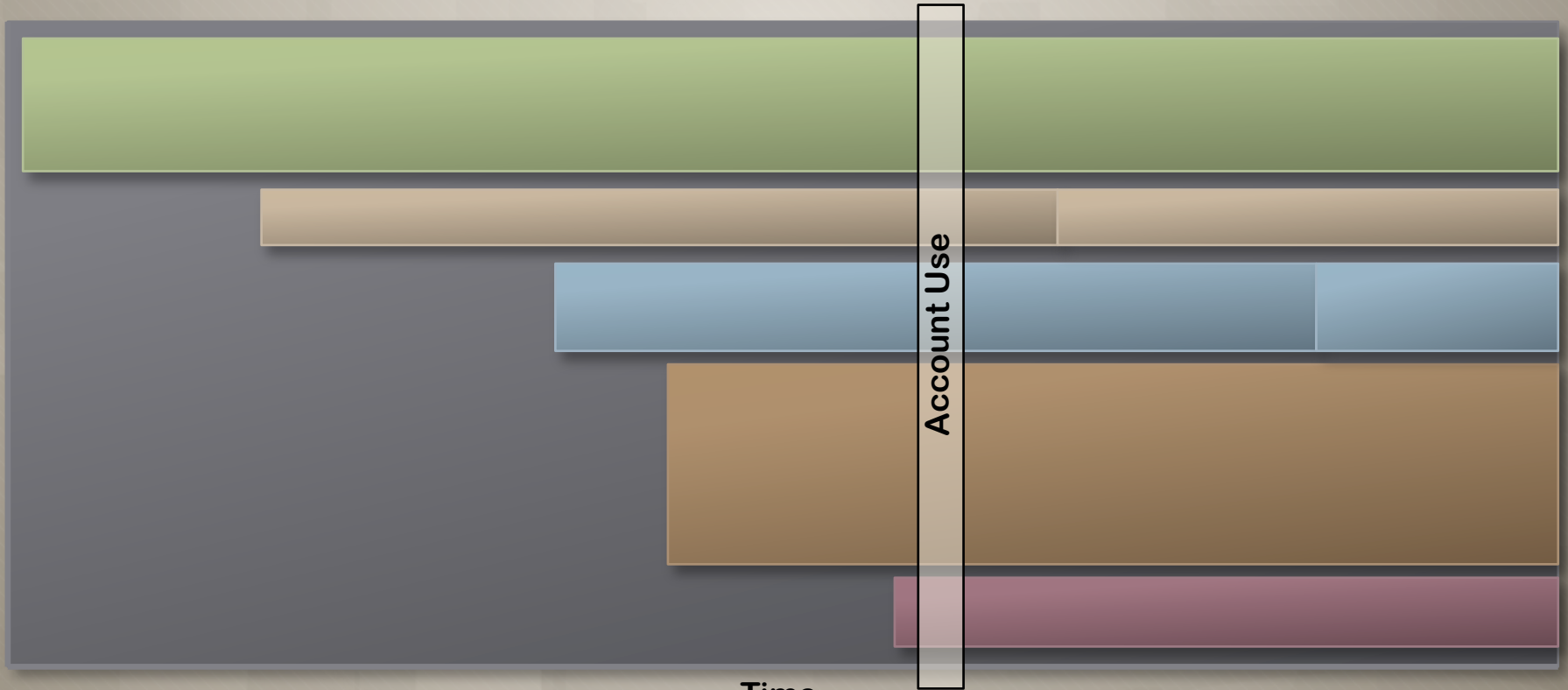
Space

Time



Time Representation

Space

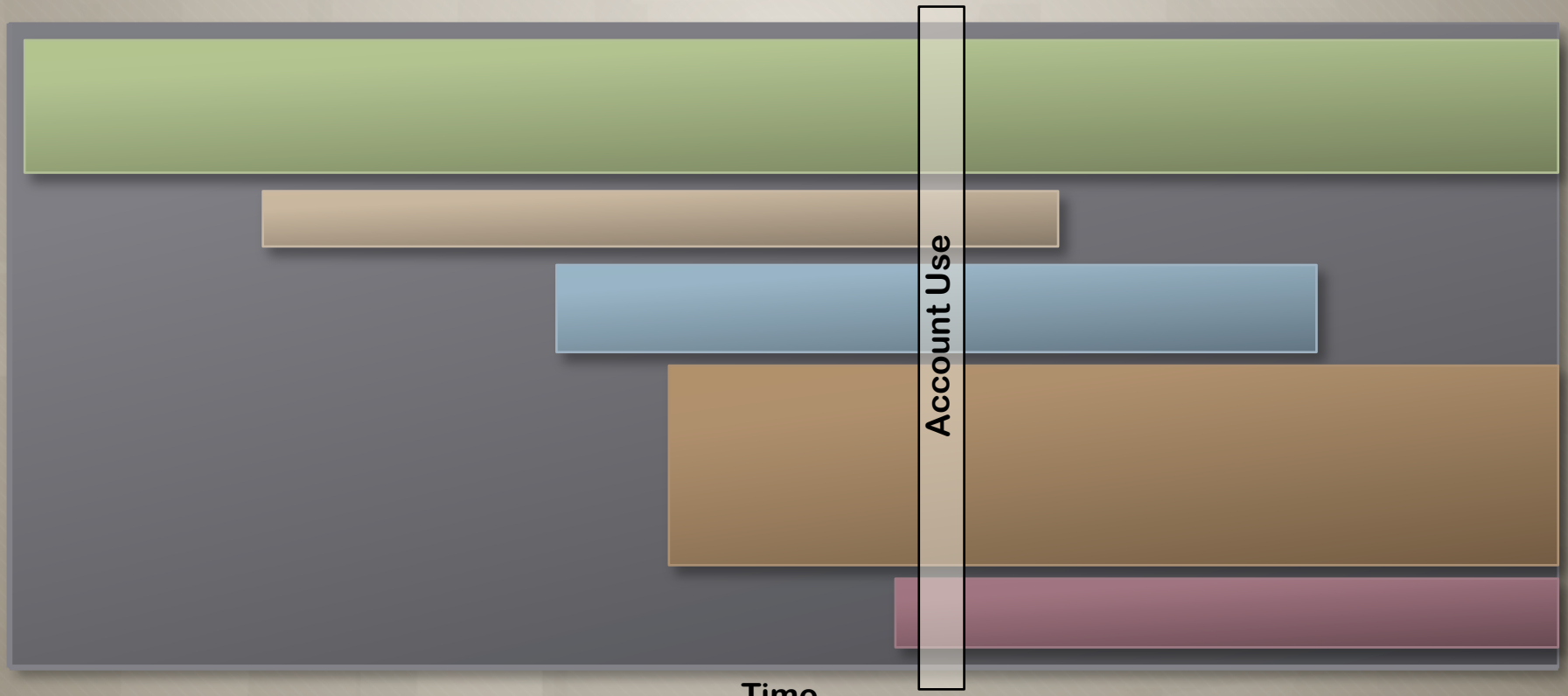


Time

Account Use

Time Representation

Space

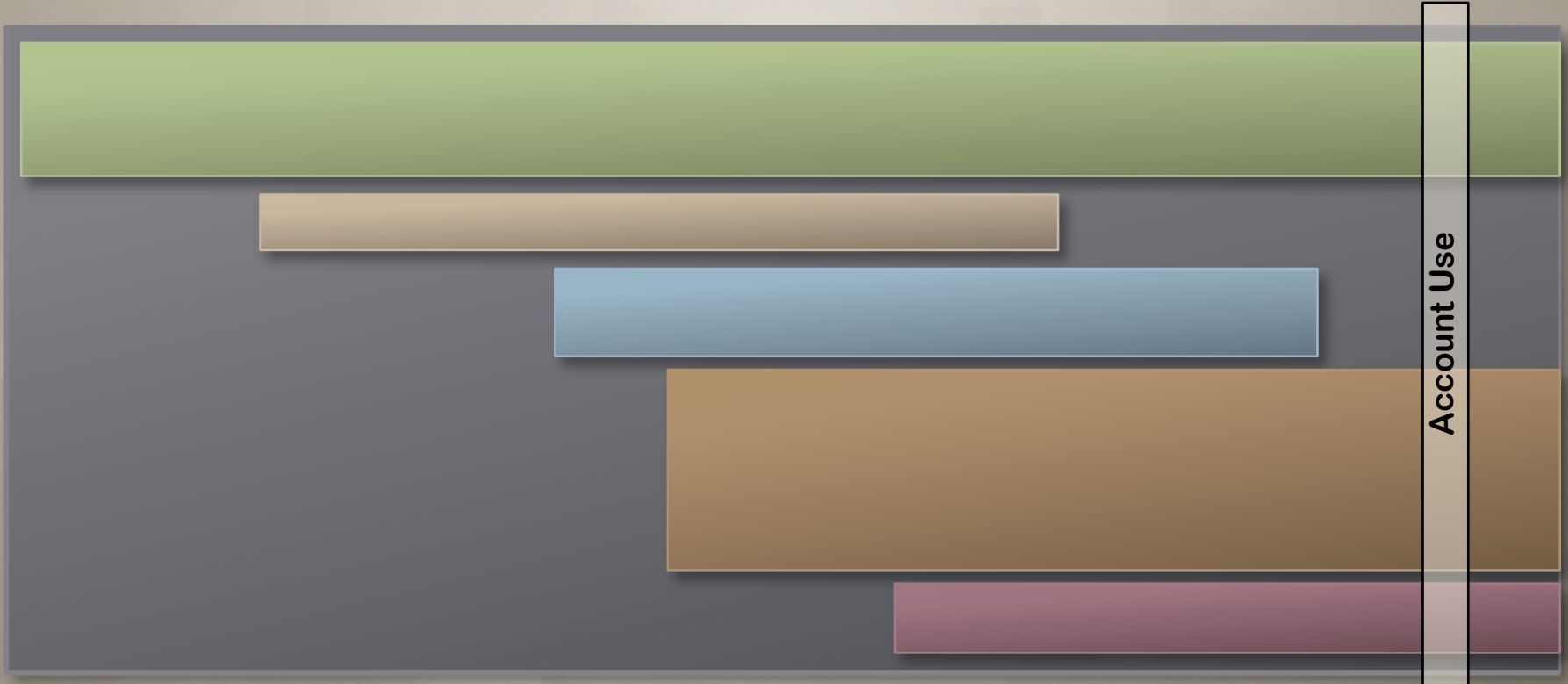


Time

Account Use

Time Representation

Space



Time

Account Use



Mechanism of Action I

- SIZE-quota Storage
- TIME-limit History
- 2 Independent Quota Measurement Dimensions
- = Unlimited Storage*
 - *Technically limited by provider upload bandwidth



Mechanism of Action II

- Storage:
 - Take a large file
 - Cut it up into fragments
 - Upload each fragment as a 'version'
 - Top it off with an 0b-sized chunk
- Retrieval:
 - Pull & concat all 'versions' in uploaded order



Time Representation II

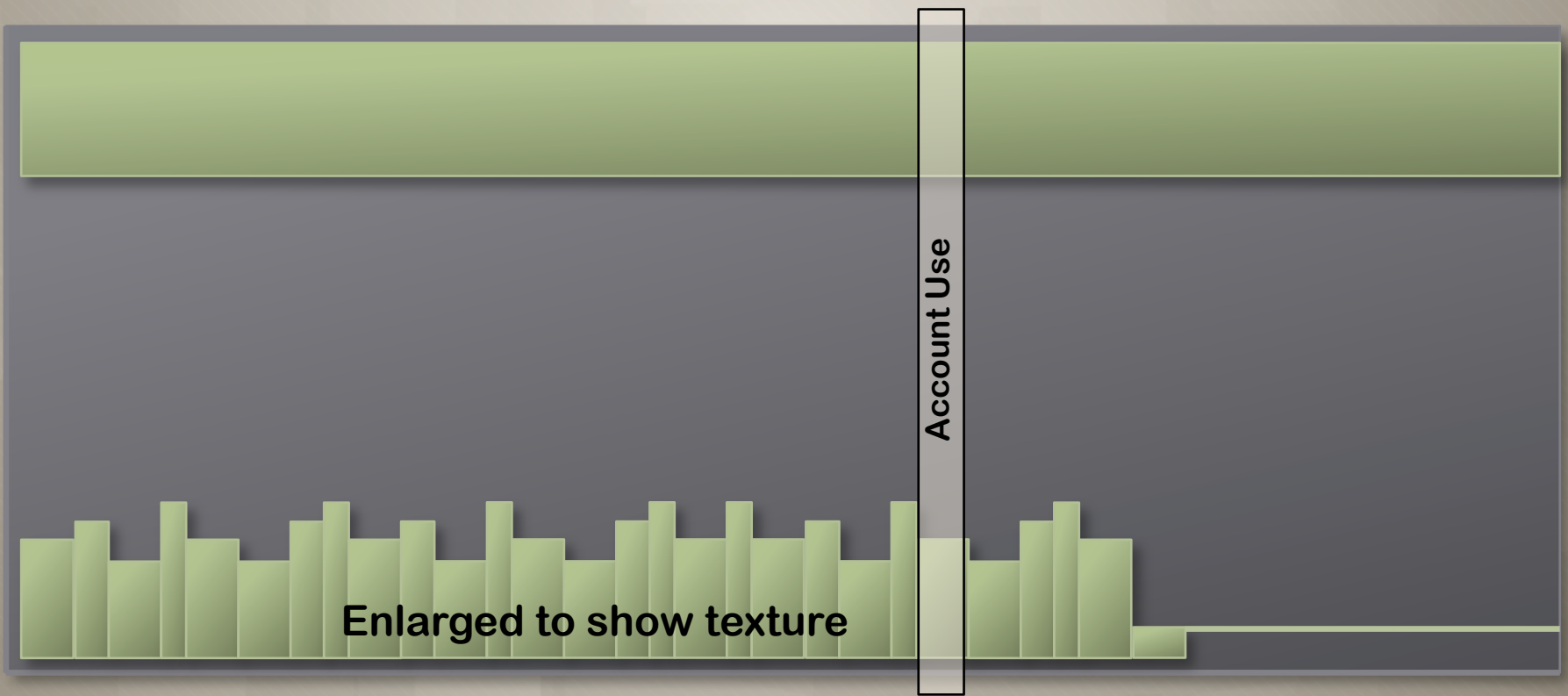




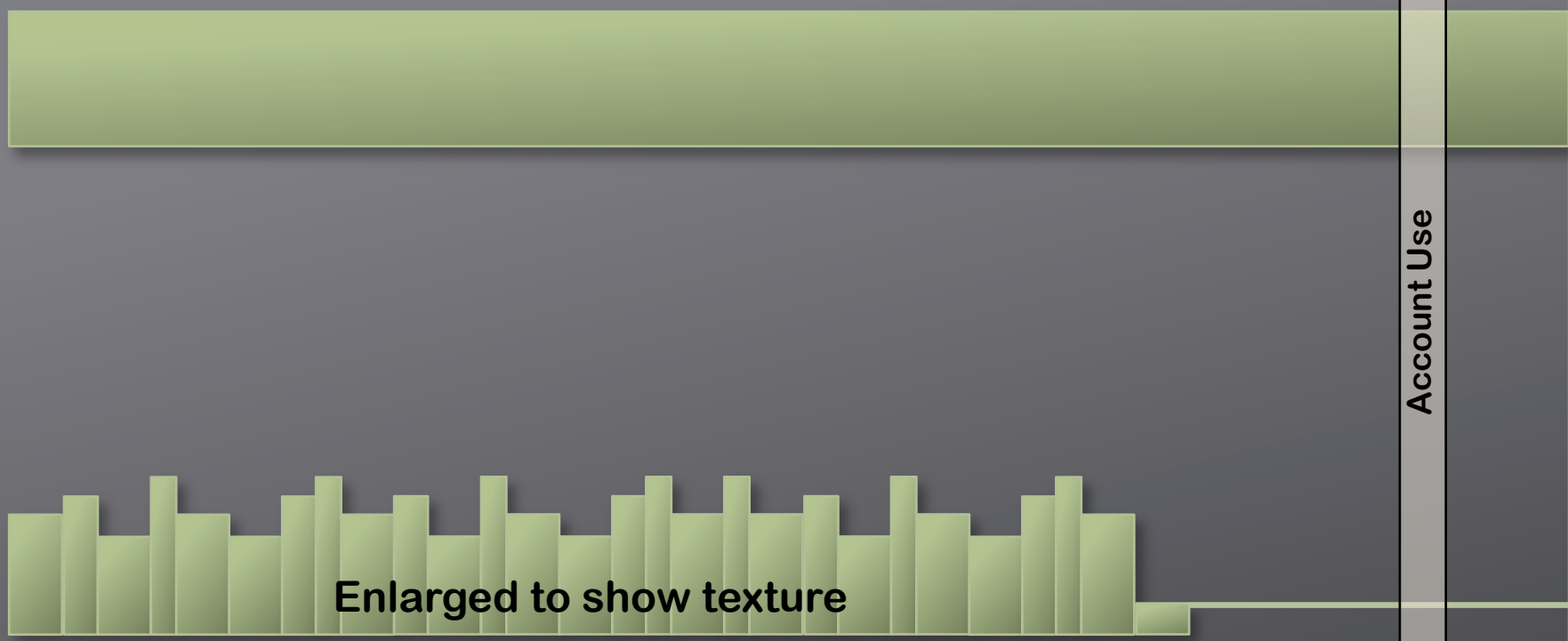
Time Representation II



Time Representation II



Time Representation II



Enlarged to show texture

Account Use



Introducing: DeePack Choppa

Vertical Storage Management Framework



What is it?

- “Pluggable Service Framework”
 - Abstracts out API/Implementation Specifics
 - Maintains storage db backend
 - Provides CLI access to core functions



Demo

- o It's been running *the whole time*



What can be done?

Aftermath



Blue-Team Concerns I

Detection Method

- Constantly Rewriting Fixed Size/Time/Name
- API Key Ban Whackamole
- Null Caps

Countermeasure

- Generators to introduce variability & flexibility
- Get a new one
- 1-byte?



Blue-Team Concerns II

- Unlimited space undermines business model
- Barring large binary writes may break existing compatibility
 - encfs, git, etc.
- Deep analysis is time consuming/frowned upon



Special Thanks

- ◊ Randy Fortier – Original Security Interest
- ◊ Sarah Harvey – Encouraging a DEFCON Talk
- ◊ Tao Wang – Encouraging pursuit of original
- ◊ Marlinspike, Schneier, Goldberg, DT et. al.