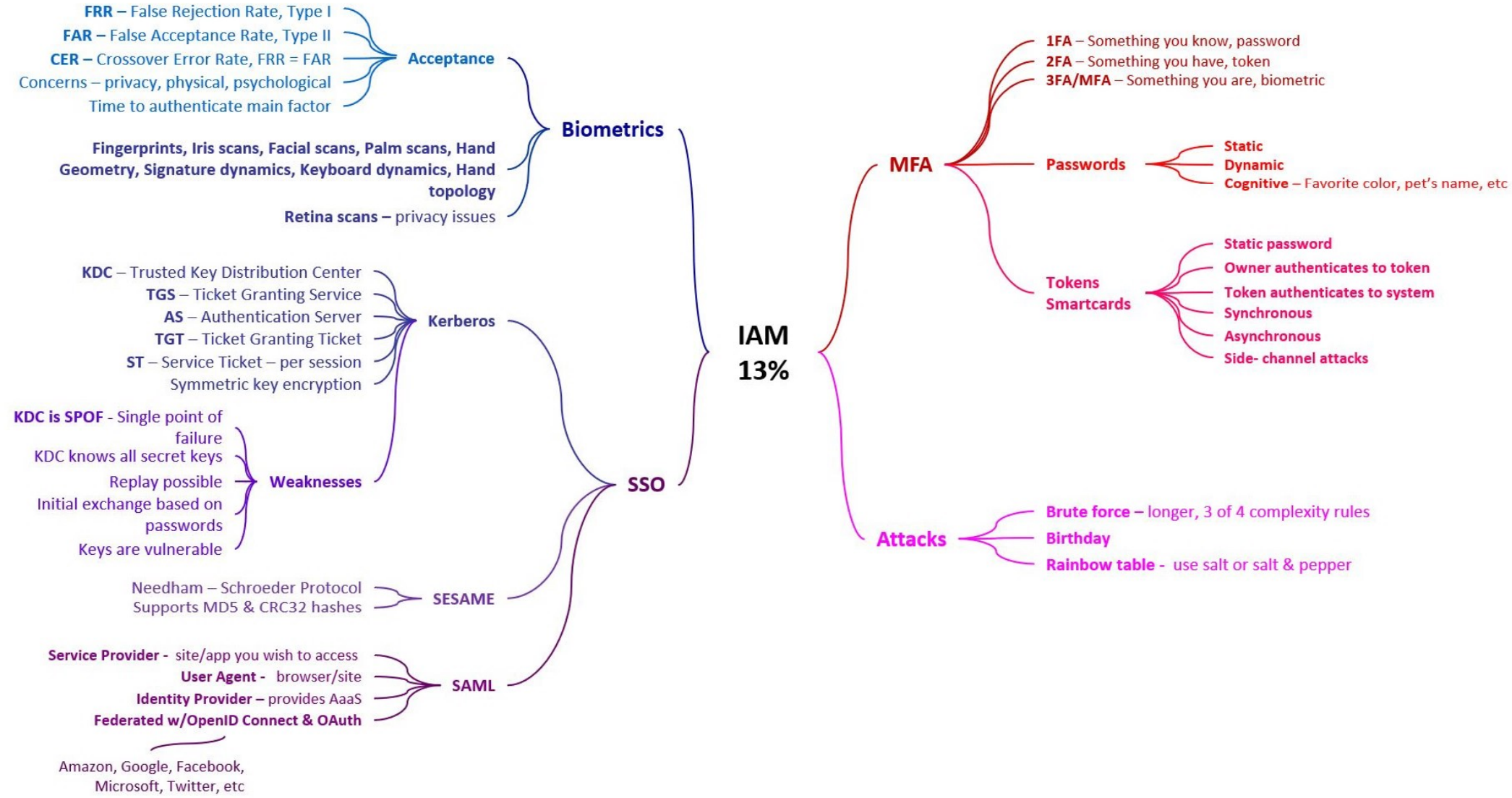
IAM
13%
Biometrics
FRR – False Rejection Rate, Type I
FAR – False Acceptance Rate, Type II
CER – Crossover Error Rate, FRR = FAR
Concerns – privacy, physical, psychological
Time to authenticate main factor
Acceptance
Fingerprints, Iris scans, Facial scans, Palm scans, Hand Geometry, Signature dynamics, Keyboard dynamics, Hand topology
Retina scans – privacy issues
SSO
KDC – Trusted Key Distribution Center
TGS – Ticket Granting Service
AS – Authentication Server
TGT – Ticket Granting Ticket
ST – Service Ticket – per session
Symmetric key encryption
Kerberos
KDC is SPOF - Single point of failure
KDC knows all secret keys
Replay possible
Initial exchange based on passwords
Keys are vulnerable
Weaknesses
Needham – Schroeder Protocol
Supports MD5 & CRC32 hashes
SESAME
Service Provider - site/app you wish to access
User Agent - browser/site
Identity Provider – provides AaaS
Federated w/OpenID Connect & OAuth
Amazon, Google, Facebook, Microsoft, Twitter, etc
SAML
MFA
1FA – Something you know, password
2FA – Something you have, token
3FA/MFA – Something you are, biometric
Passwords
Static
Dynamic
Cognitive – Favorite color, pet's name, etc
Tokens
Smartcards
Static password
Owner authenticates to token
Token authenticates to system
Synchronous
Asynchronous
Side- channel attacks
Attacks
Brute force – longer, 3 of 4 complexity rules
Birthday
Rainbow table - use salt or salt & pepper