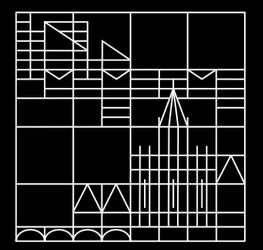
SIEGE

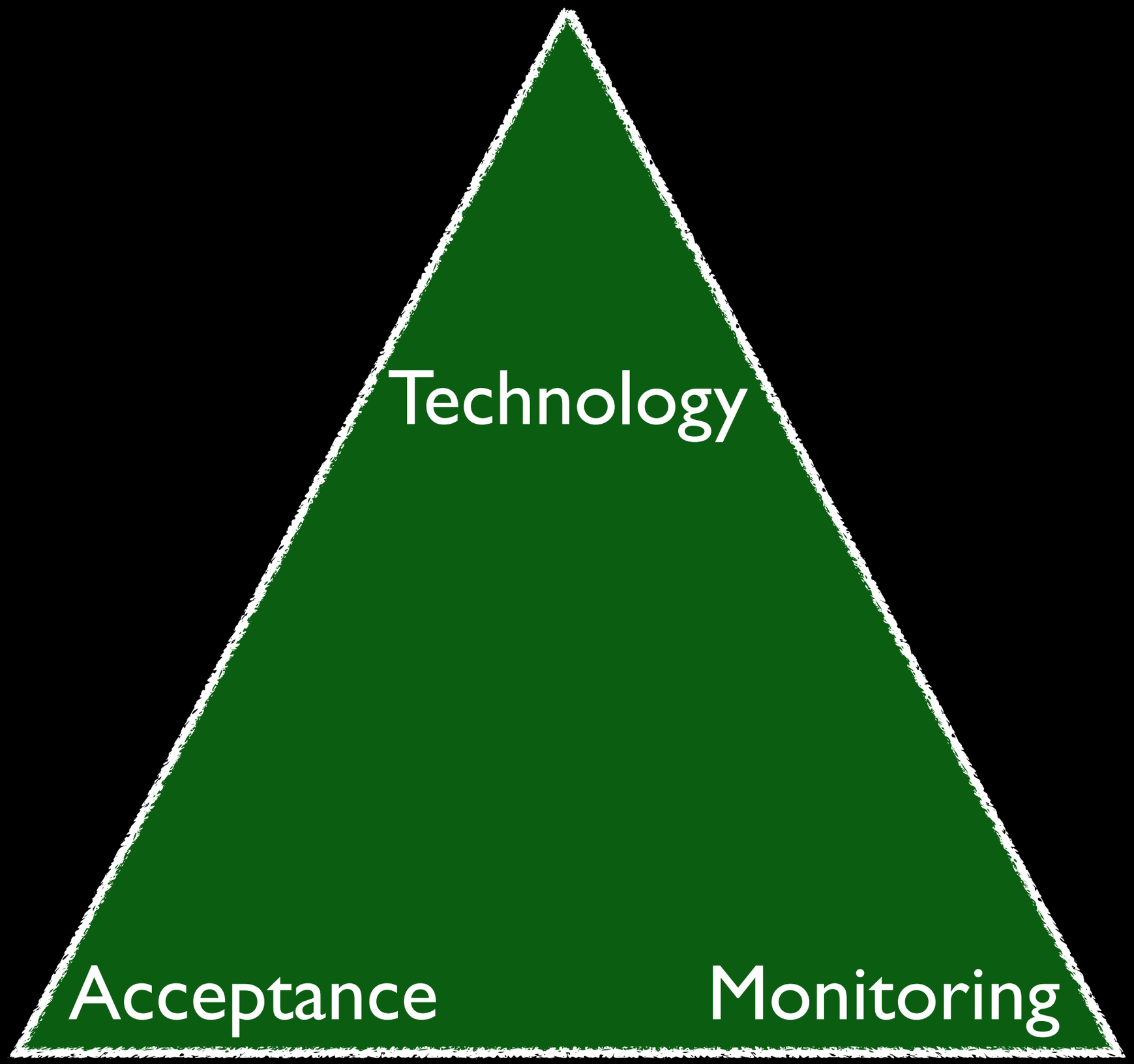
Service-Independent Enterprise-Grade Protection Against Password Scans

Marcel Waldvogel and Jürgen Kollek

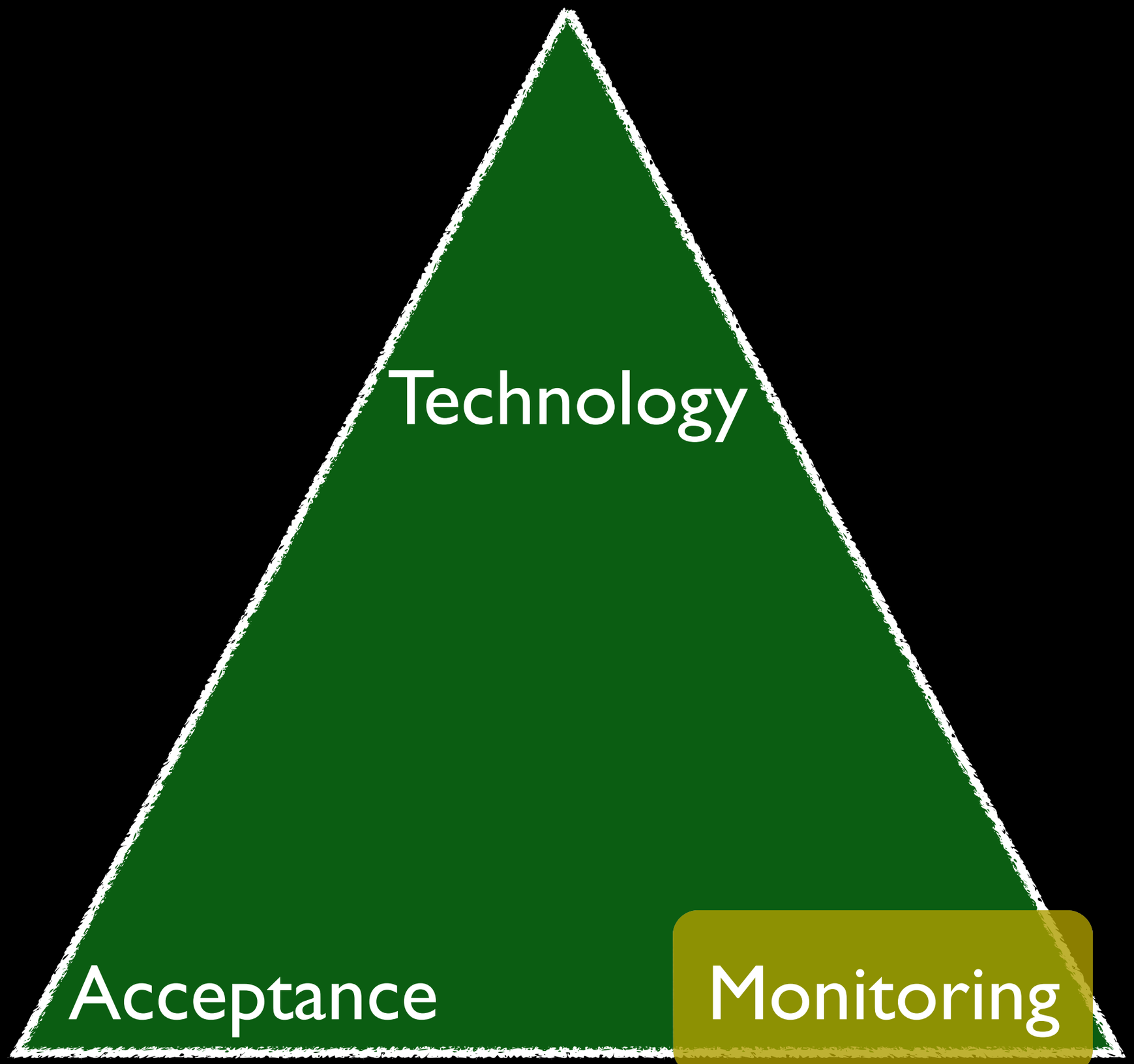
Universität Konstanz



Security Triangle



Security Triangle



Traditional

- Single host
- Per application
- Log file parsing

```
Jan 08 13:39:55 testhost sshd[555]:↴
Invalid user test from 1.2.3.4
```

Traditional

- Single host
- Per application
- Log file parsing

```
Jan 08 13:39:55 testhost sshd[555]:↴
Invalid user test from 1.2.3.4
```

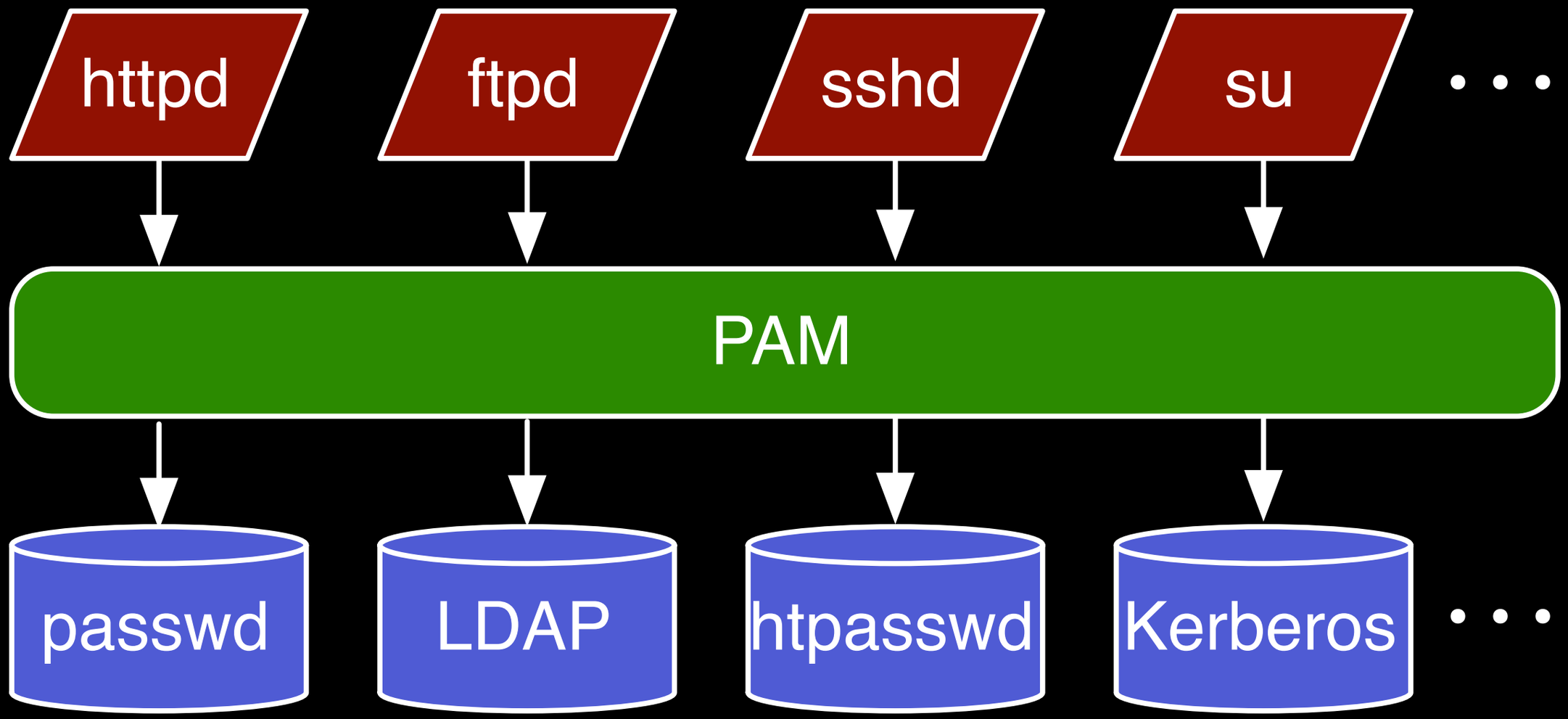
```
Jan 08 13:39:55 testhost sshd[555]:↴
Invalid user test from 4.5.6.7 from 1.2.3.4
```

Goals and Mechanisms

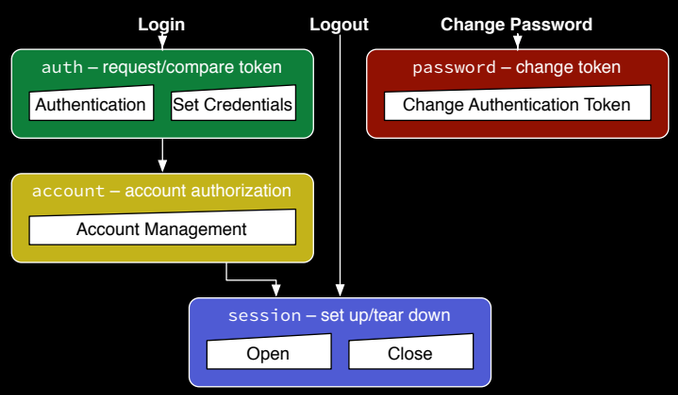
- Lock out bad guys
- Allow good guys

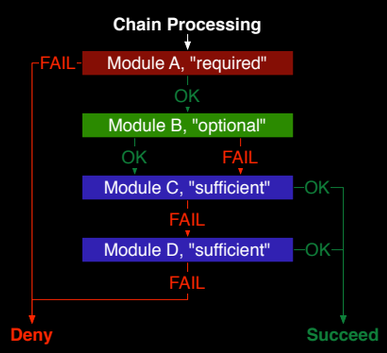
1. Modularity — Modularity
2. CooRdinated Organization-Wide Defense — CROWD
3. Geographical Risk Differentiation — Geo
4. Dictionary-based botnet identification — Dict
5. User/bot password differentiation — Typo

Modularity

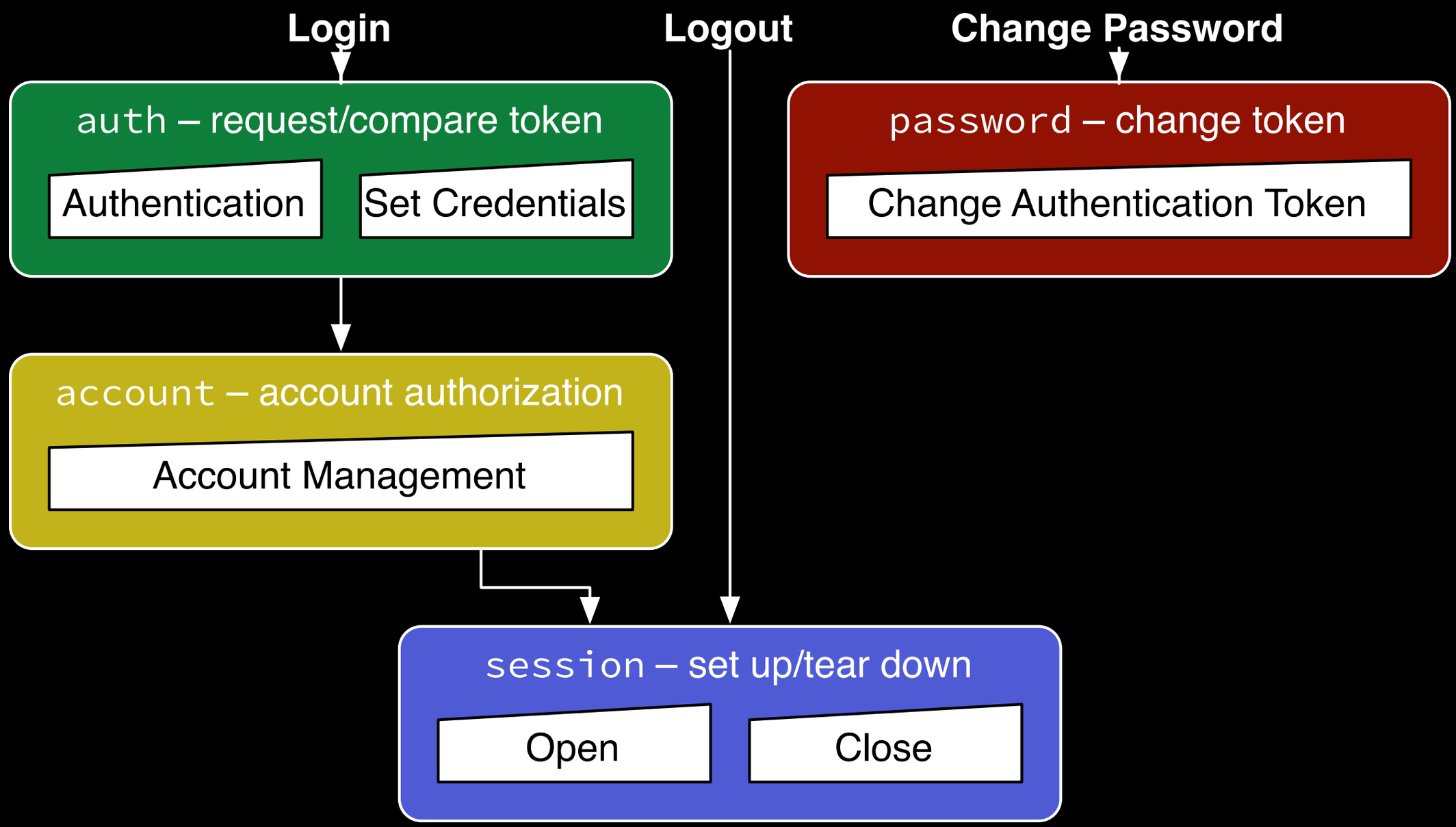


PAM

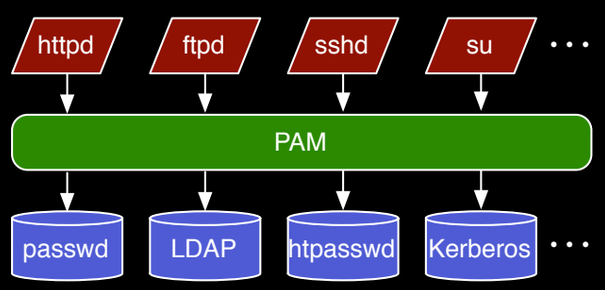


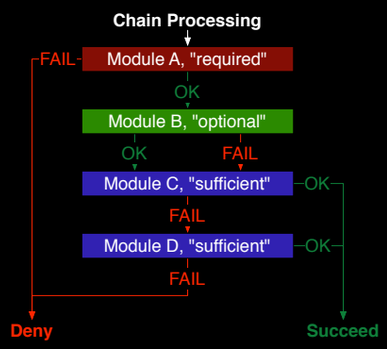


Modularity



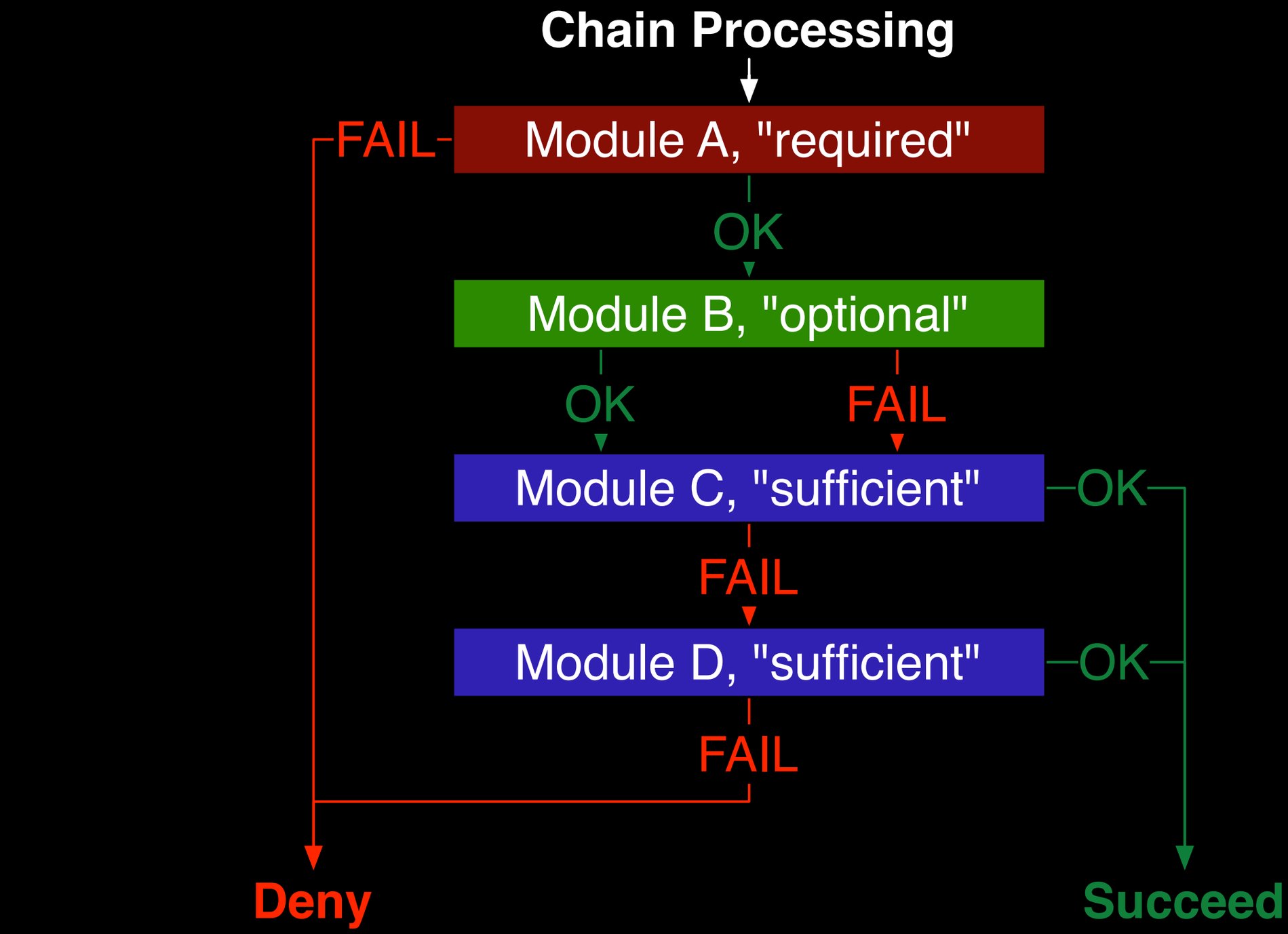
PAM

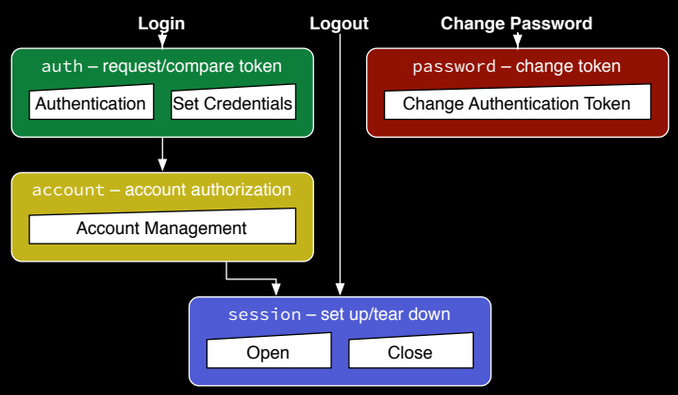


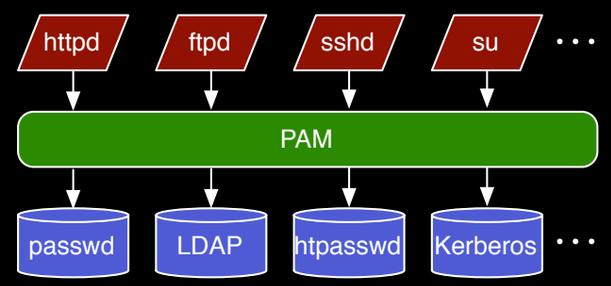


Modularity

PAM

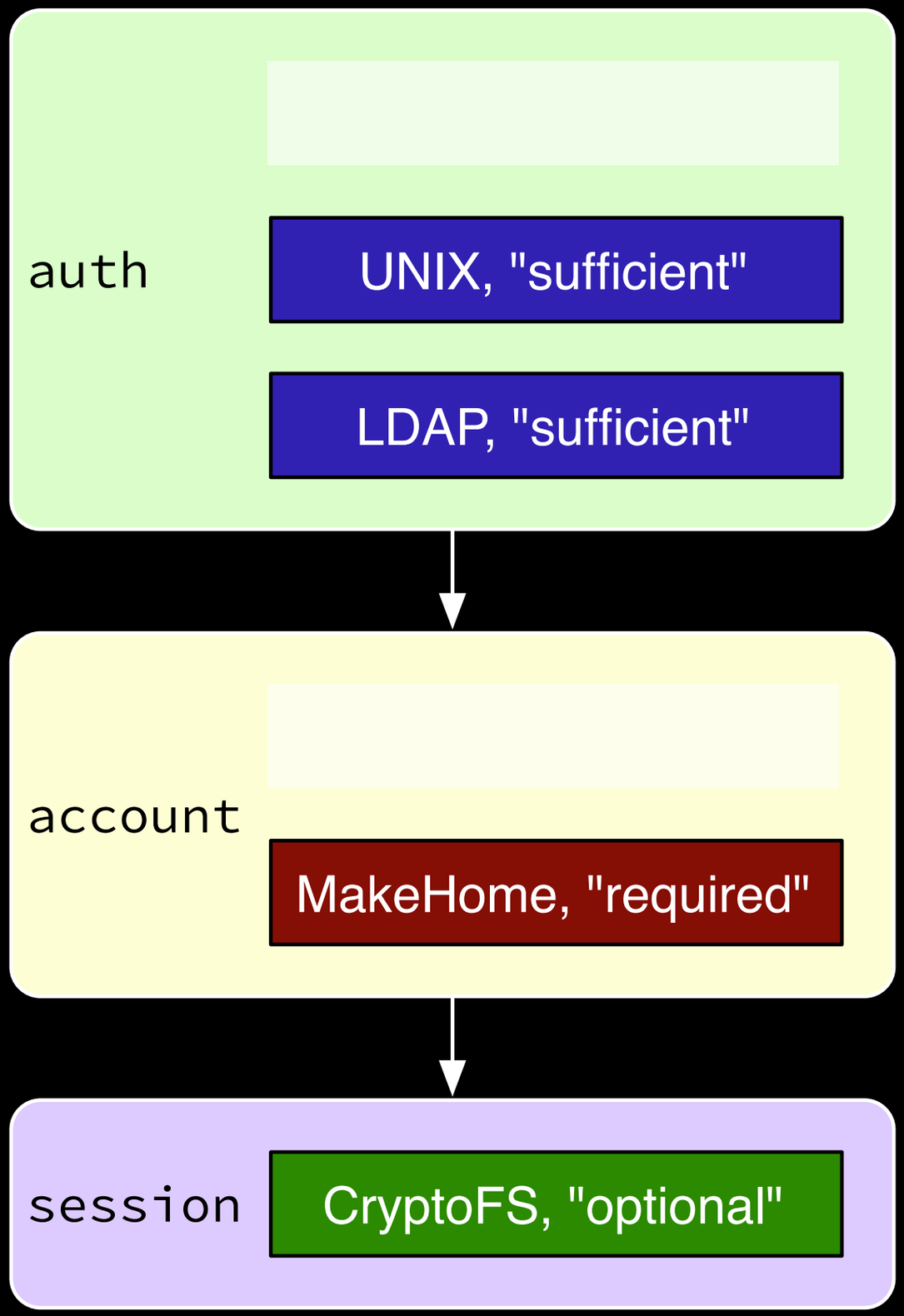




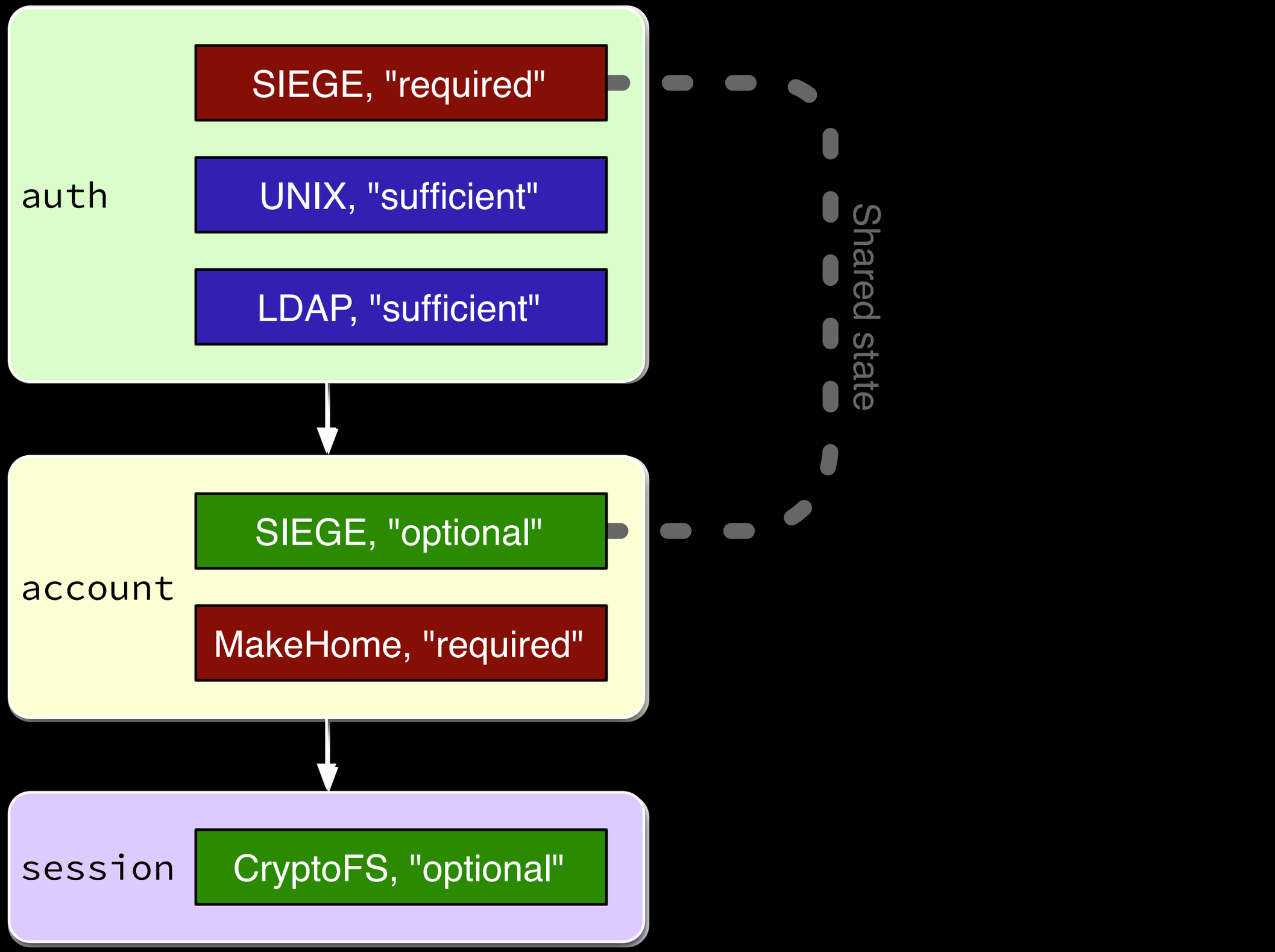


Modularity
CROWD

SIEGE in PAM

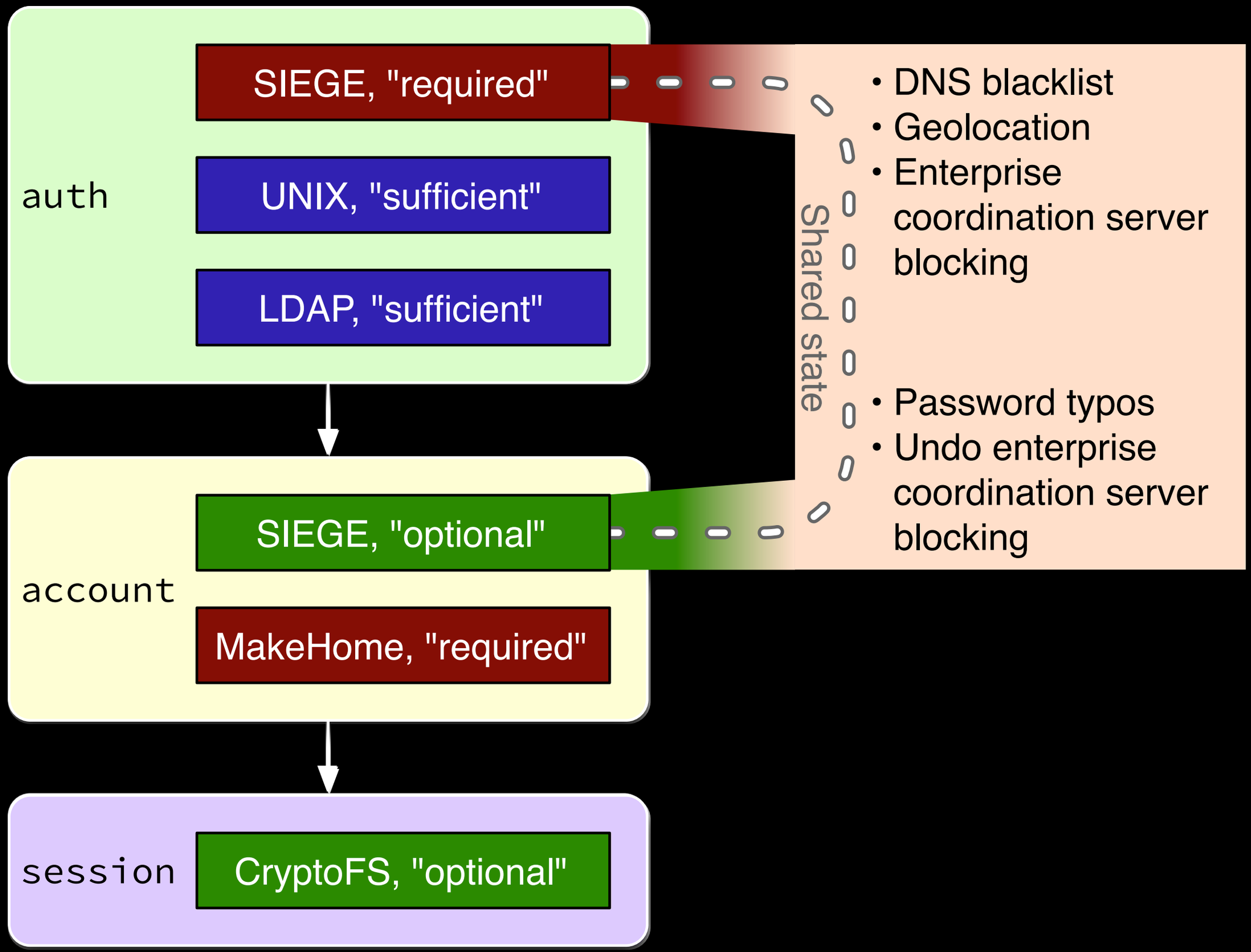


SIEGE in PAM


auth
SIEGE, "required"
UNIX, "sufficient"
LDAP, "sufficient"
account
SIEGE, "optional"
MakeHome, "required"
session
CryptoFS, "optional"
Shared state

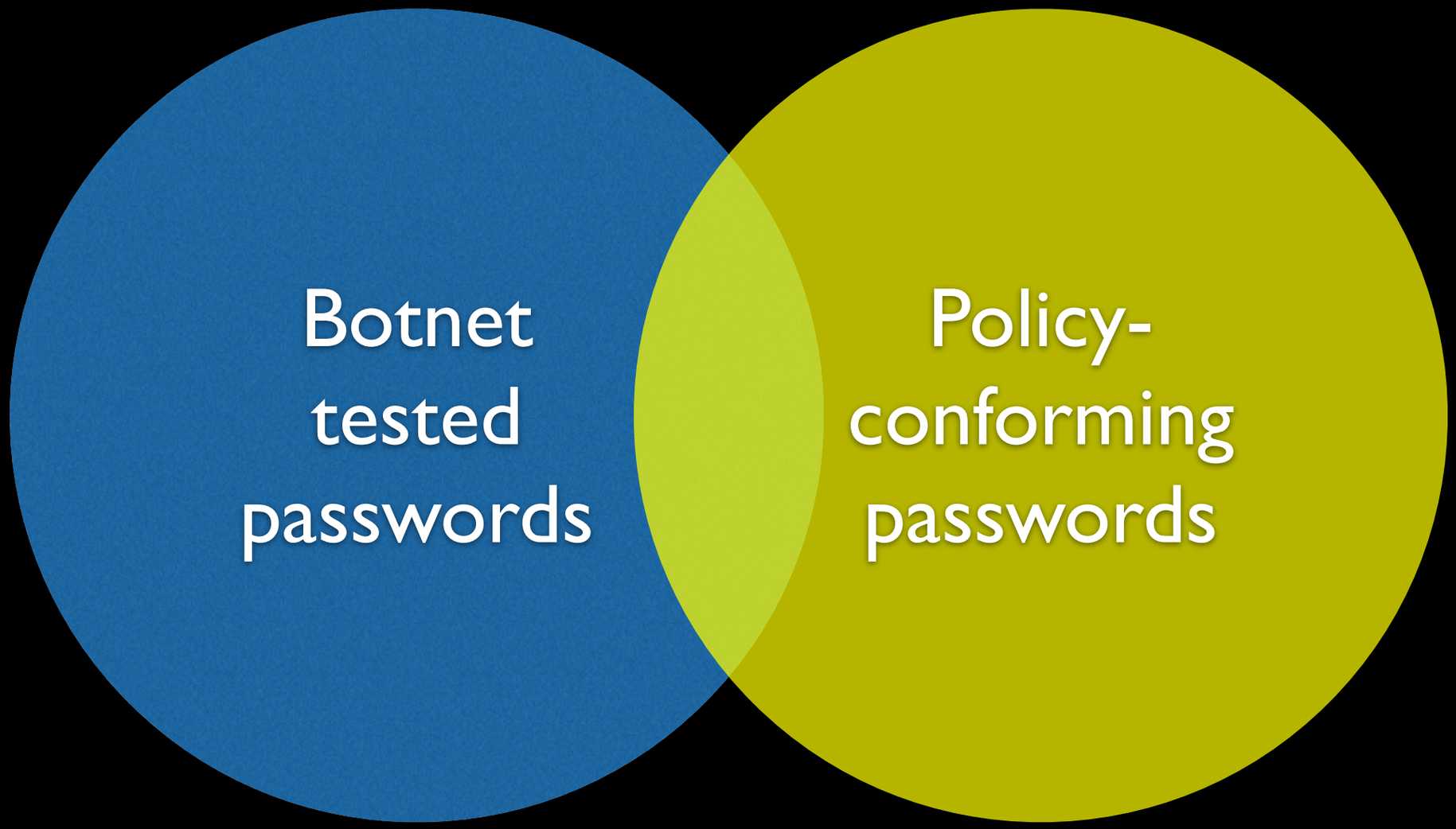
Modularity CROWD

SIEGE in PAM



Password Policy

Dict



Typo

User or bot?

Wurst-brot1

- Wurts-brot1 — ℓ-1
- Wurrst-brot1 — ≪ℓ
- Wurst-brot1 — (ℓ+1)A

Geo Risk Differentiation

- Good? Bad?
- Network aggregation

Password trials

Geo CROWD

Password guesses/s

10'000M
1'000M
100'000K
10'000K
1'000K
100'000
10'000
1'000
100
10
1

Unpro-tected

Single Host

1 Home 5 Neighbors 250 Others Total

SIEGE

10k against 1

Geo CROWD

Password trials

Passwords/s

10'000M
1'000M
100'000K
10'000K
1'000K
100'000
10'000
1'000
100
10
1

Unpro-tected	Single Host	1 Home	5 Neighbors	250 Others	Total
10'000	164	1	2	32	35

SIEGE

1M against 1

Geo CROWD

Password trials

Passwords/s

10'000M
1'000M
100'000K
10'000K
1'000K
100'000
10'000
1'000
100
10
1

Unpro-tected	Single Host	1 Home	5 Neighbors	250 Others	Total
1'000K	16'393	64	161	447	672

SIEGE

100M against 1

Geo CROWD

Password trials

Passwords/s

10'000M
1'000M
100'000K
10'000K
1'000K
100'000
10'000
1'000
100
10
1

Unpro-tected	Single Host	1 Home	5 Neighbors	250 Others	Total
100'000K	1'639K	5'548	535	446	6'529

SIEGE

10k against 10k

Geo CROWD

Password trials

Passwords/s

10'000M
1'000M
100'000K
10'000K
1'000K
100'000
10'000
1'000
100
10
1

Unpro-tected	Single Host	1 Home	5 Neighbors	250 Others	Total
10'000K	163'934	1	2	32	35

SIEGE

1M against 10k

Geo CROWD

Password trials

Passwords/s

10'000M
1'000M
100'000K
10'000K
1'000K
100'000
10'000
1'000
100
10
1

1'000M
16'393K
64
161
447
672

Unpro-tected
Single Host
1 Home
5 Neighbors
250 Others
Total

SIEGE

100M against 10k

Geo CROWD

Password trials

Passwords/s

10'000M
1'000M
100'000K
10'000K
1'000K
100'000
10'000
1'000
100
10
1

100'000M
1'639M
5'548
535
446
6'529

Unpro-tected
Single Host
1 Home
5 Neighbors
250 Others
Total

SIEGE