Password Policy Considered Harmful

Andrew Findlay
LDAPCon 2019

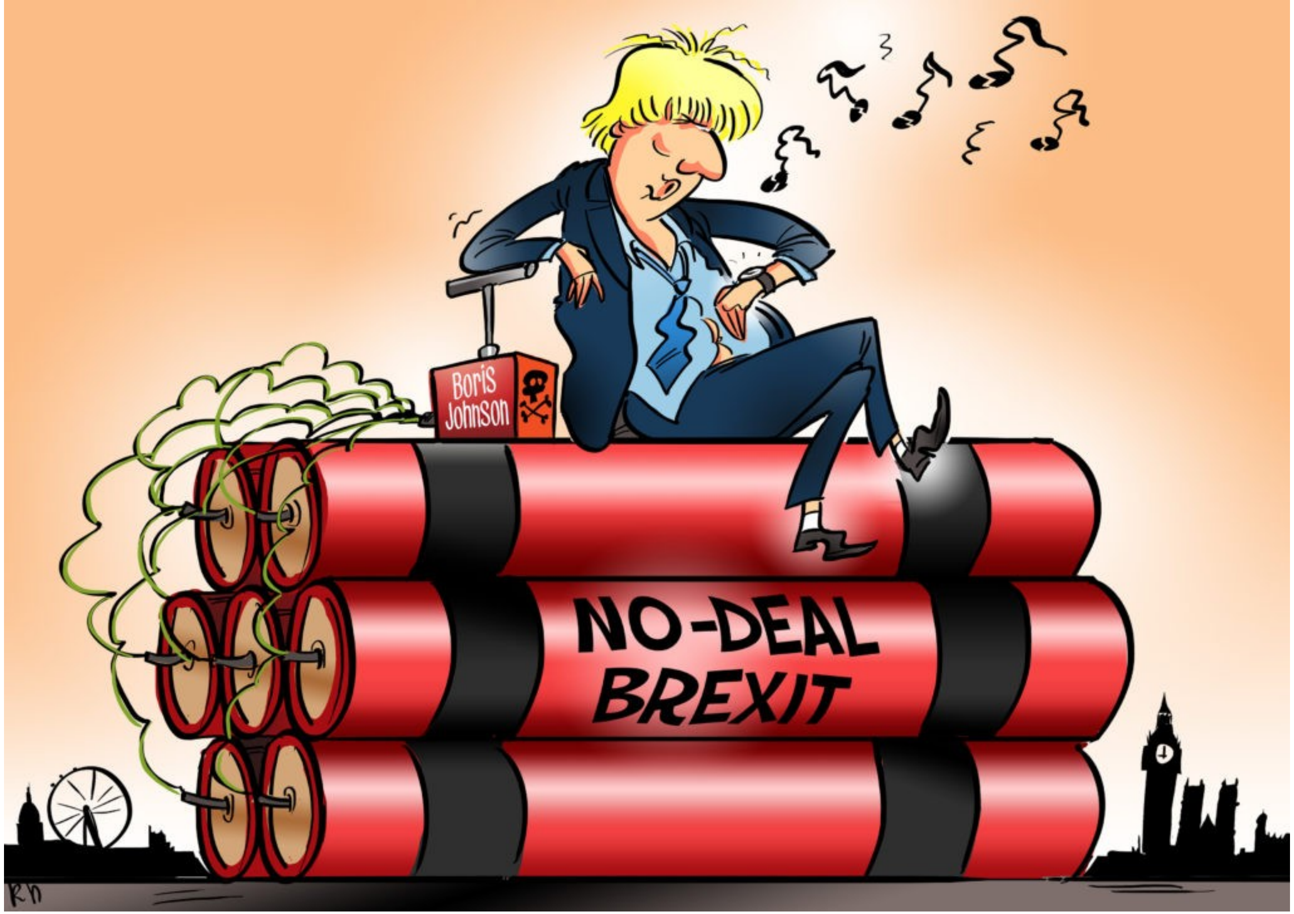
We still use passwords?!?

- Worst possible solution
  - Apart from most of the others
- Policy is supposed to mitigate the risks
  - But often adds new ones
  - Especially if you still follow the DoD Orange Book
- Consider some alternative ideas...

But first

Some Good Advice
From the British Government

Maybe not...



politico.eu

Some Good Advice
From the British Civil Service

Hmm…

Some Good Advice From the British Spooks

Yes!

- The house-trained ones anyway
- Specifically:
  The National Cyber Security Centre (NCSC)
- www.ncsc.gov.uk

Password Policy: Updating Your Approach

- No routine expiry
- No complexity rules
  - *Just Three Words* campaign
- Users are allowed to write down passwords
- Use password blacklists
- Use attempt throttling
- Be careful with lockout

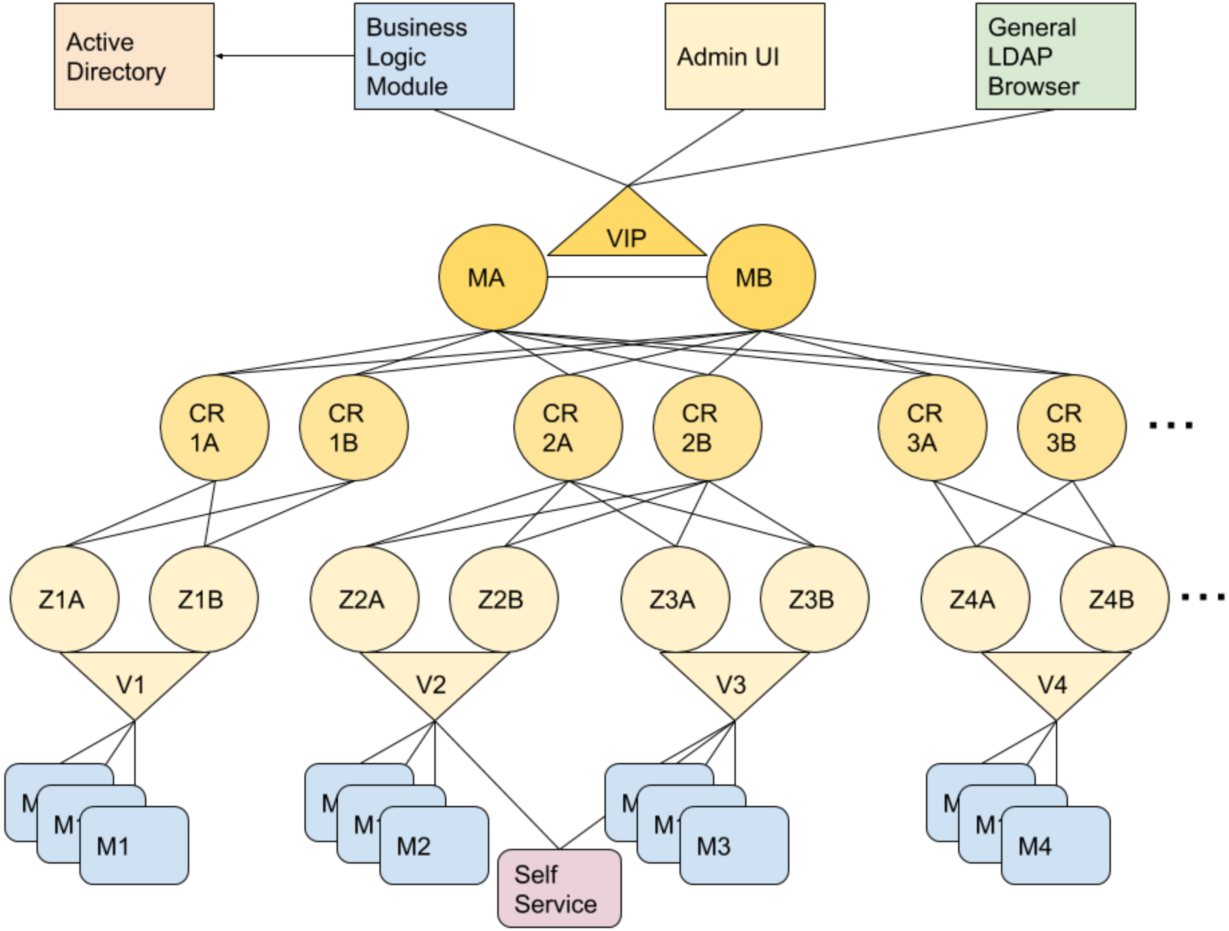
Policy vs LDAP

Do you really *want* lockout?

- Be careful what you wish for:
- Every login failure becomes an update to LDAP
  - Entries grow
  - Easy DDoS
- Can block any chosen user with a few failed logins
  - Consider the phone you left at home…

    on the day you changed your password while abroad

Replication makes this worse



Shawn’s replication scenario

Every PW failure gets relayed to the top

Lockout or Throttle

- Lockout invites DDoS
- Can we just slow down instead?
- How do we identify attacks?
  - LDAP may be the wrong place to do this
- Client-facing code has more information
  - And more options to counter attacks

Attack Detection Service

- Separate from LDAP servers
- Distributed / replicated
- Does not need ACID semantics
- Incorporate data from LDAP and non-LDAP sources
- Detection heuristics
- Output alerts to services in real time

Component ideas

- LMDB or even memcached
- Message queues
- Session tracking control helps with richer data
- Fail2ban – IP-level protection
- Services (IMAP, web, etc) to support variable slowdown