SECURITY CHALLENGES IN VIVO

ADAPTING THE BSI IT SECURITY STANDARDS

GLOBAL SECURITY STATISTICS

1/3 of organizations is attacked on a weekly basis

47% growth in SSL-based attacks against European organizations

40% growth in ransom motivated attacks in 2017

*Global Application & Network Security Report 2017-2018

Bundesamt für Sicherheit in der Informationstechnik

- German Federal Office for Information Security
- IT Baseline Protection Manual[1]
- Creating IT security concepts
- IT security management

1 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

// PASSWORD HASHING

- In 2015 **11 million** MD5 hashed passwords were compromised within a single week[2]
- Argon2 is a key derivation function
- Winner of **Password Hashing Competition** 2015
- Argon2i is optimized to resist side-channel attacks

Checklist	MD5	Argon2i
Salted	✗	✓
Configurable (memory, time, parallelism)	✗	✓
Vulnerable (brute force, GPU attack, hash collision)	✓	✗
Time (hash generation)	Fast	Slow
Hash Length	128 bit	Configurable 2^{32} bytes

MD5 Hash

4BBA69E66998C59F03530EE02C406CB0

Argon2i Hash

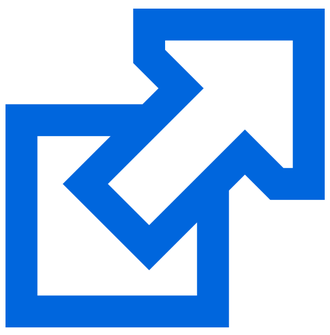
version memory time parallelism

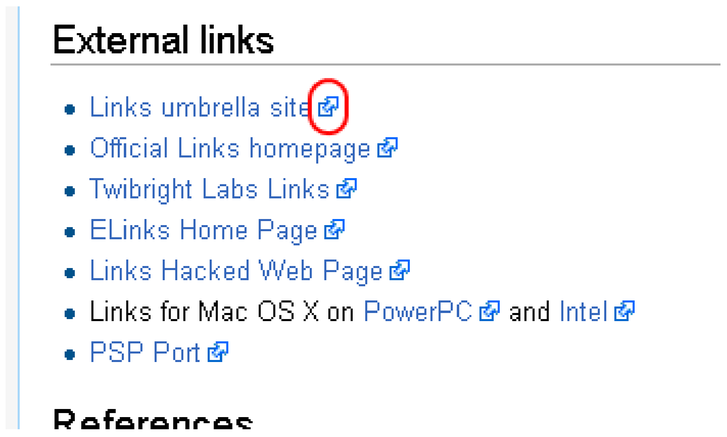
$argon2i$v=19$m=1024,t=1000,p=1$YGRB2tUxW2POXdL/nd85TA$auNkQocp9gFlhypoog/OQLREyJQ7PmpmrpU8T5yE6K0

encoded random salt and hash

2. https://en.wikipedia.org/wiki/Ashley_Madison_data_breach

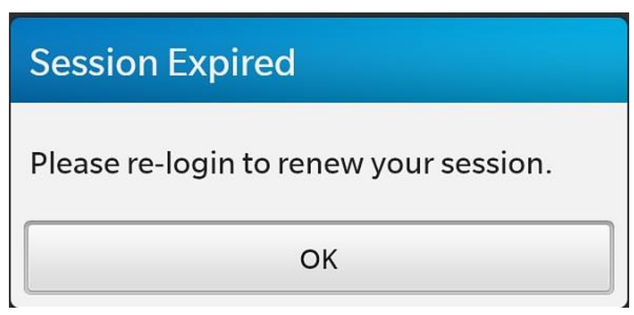
// LABELING OF EXTERNAL LINKS





Is exclusive labeling of external URLs necessary?

// BROWSER SESSION EXPIRATION



Setting an expiration time for browser session

Qazi Asim Ijaz Ahmad https://orcid.org/0000-0001-8959-6370
Martin Barber https://orcid.org/0000-0001-7924-0741
Christian Hauschke https://orcid.org/0000-0003-2499-7741

DURASPACE MEMBER

TIB LEIBNIZ-INFORMATIONSZENTRUM TECHNIK UND NATURWISSENSCHAFTEN UNIVERSITÄTSBIBLIOTHEK