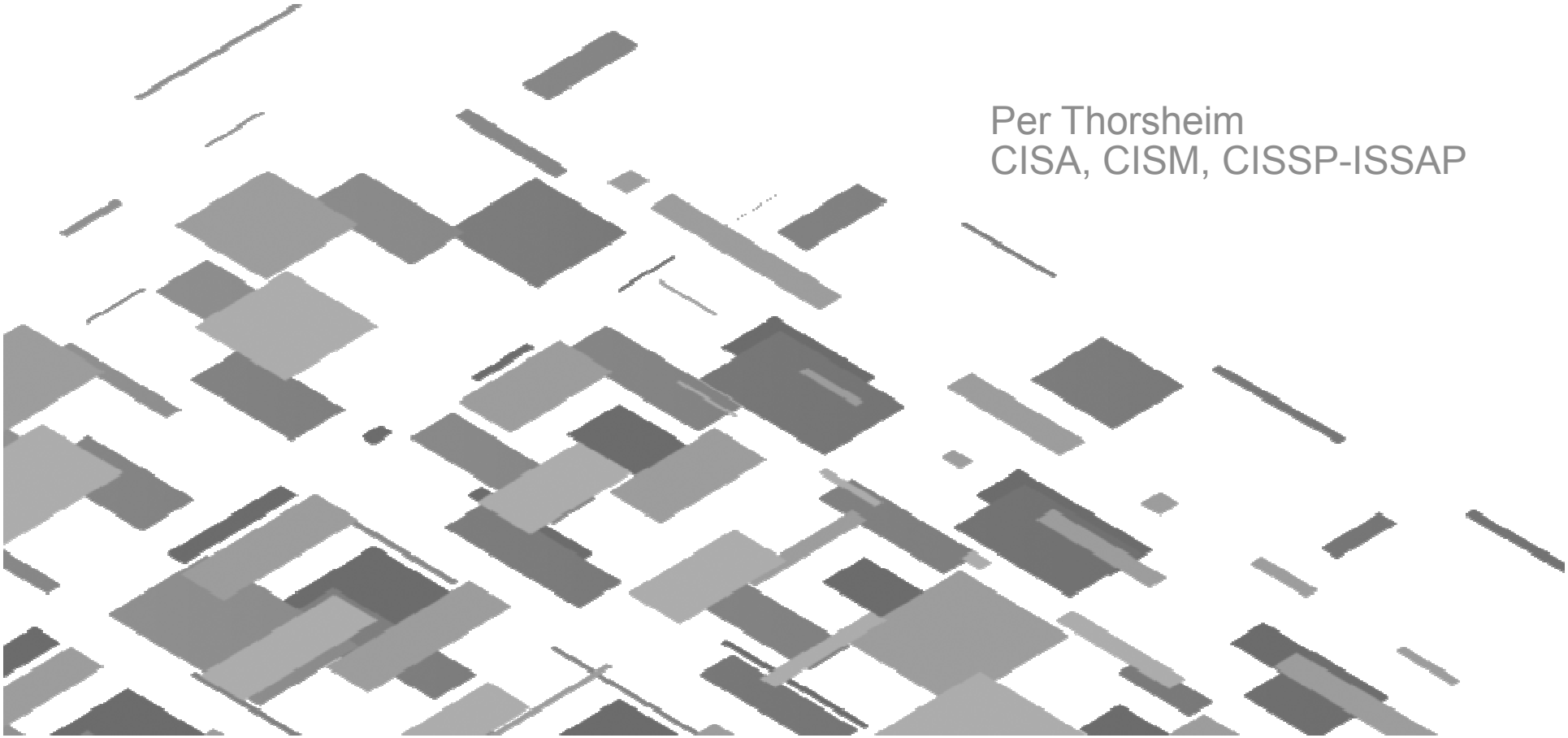
EDB

Passwords

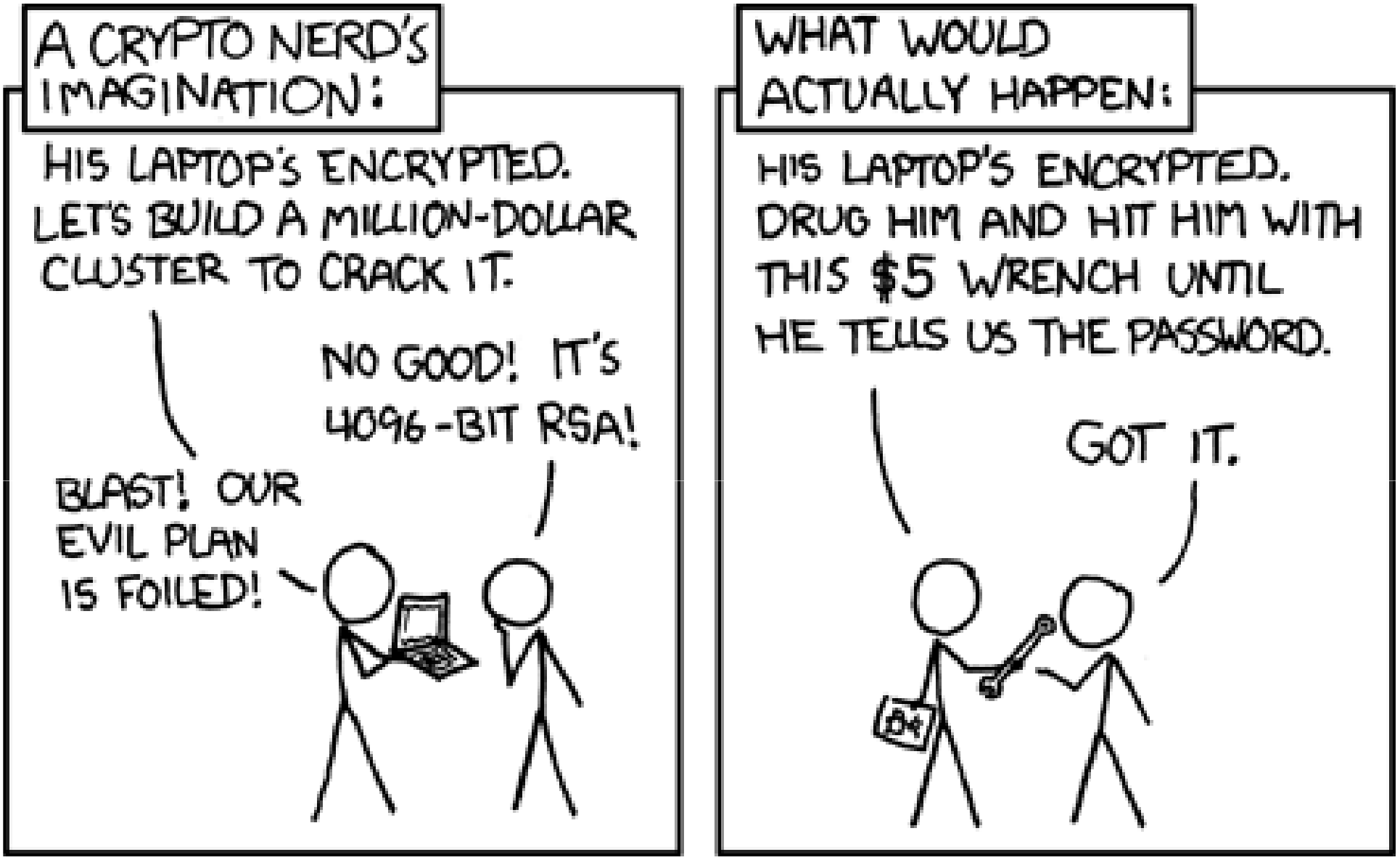


Per Thorsheim
CISA, CISM, CISSP-ISSAP

Agenda

- Basics
- Password policies
- Some tech stuff
- Tools
- Findings
- More tech stuff (and attacks)
- Password alternatives?
- Recommendations

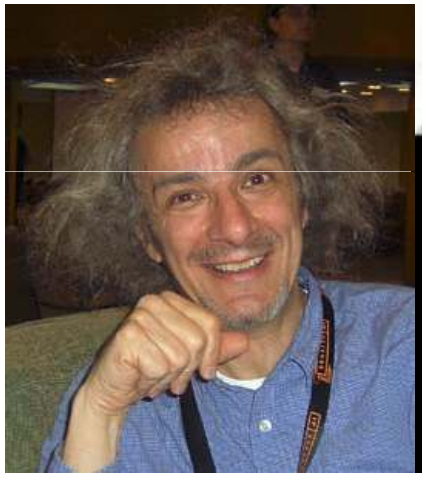
EDB

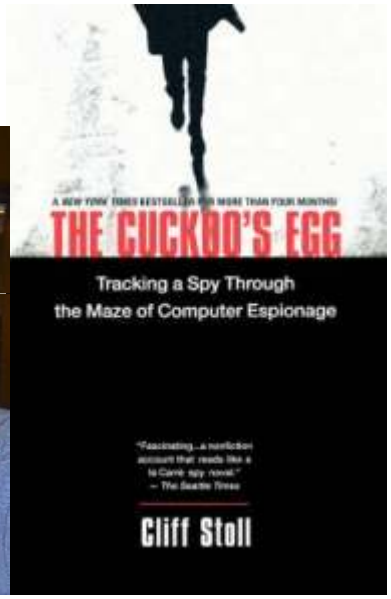

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

EDB

Background

- Commodore 64 & Amiga 1000 (Your computer is alive)
- Wargames, Sneakers, and Terminator (Skynet)
- Chaos Computer Club

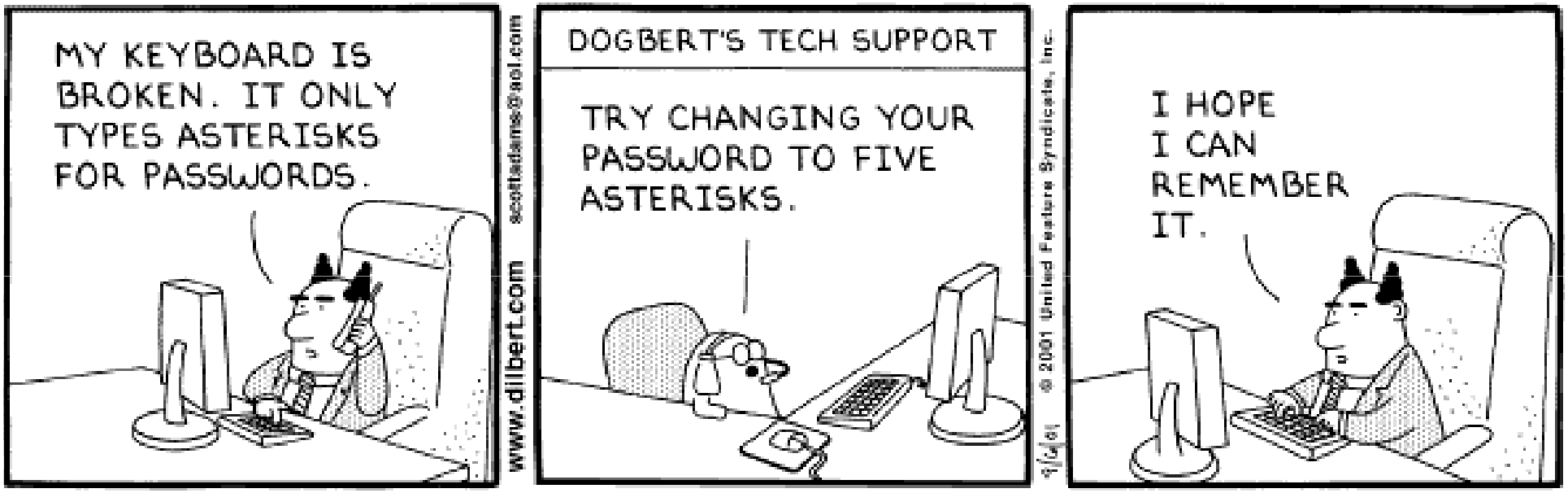




- Working/playing/investigating passwords for 9 years

EDB

Basics


MY KEYBOARD IS BROKEN. IT ONLY TYPES ASTERISKS FOR PASSWORDS.
DOGBERT'S TECH SUPPORT
TRY CHANGING YOUR PASSWORD TO FIVE ASTERISKS.
I HOPE I CAN REMEMBER IT.
www.dilbert.com scottadams@aol.com
© 2001 United Feature Syndicate, Inc.

EDB

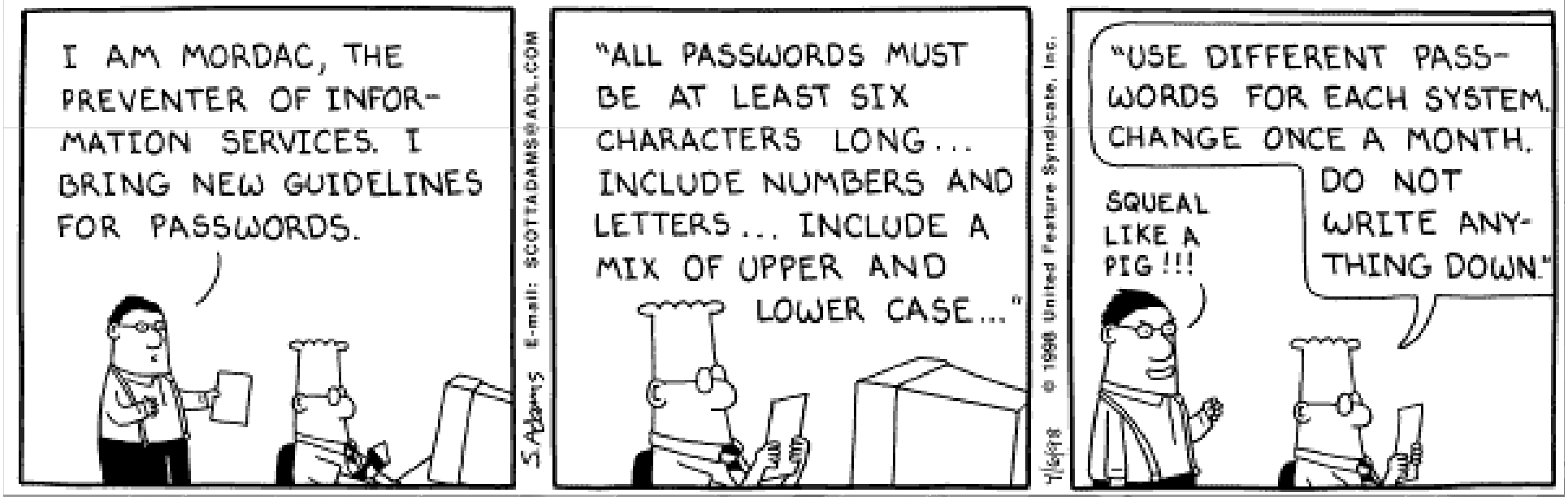
Basics

- Online vs Offline attacks
  - Limits vs almost no limits
- Evil maid attack (that's vandalism & cheating ☺)
- Attack methods:
  - Blank password (press enter)
  - Password = username
  - Wordlist attack
  - Dictionary attack
  - Hybrid attack
  - Bruteforce attack
    - Using CPU and GPU, multi-cores and distributed solutions
  - Rainbowtable attack
- Character classes?

EDB

Password policies

”Thou shalt not…”

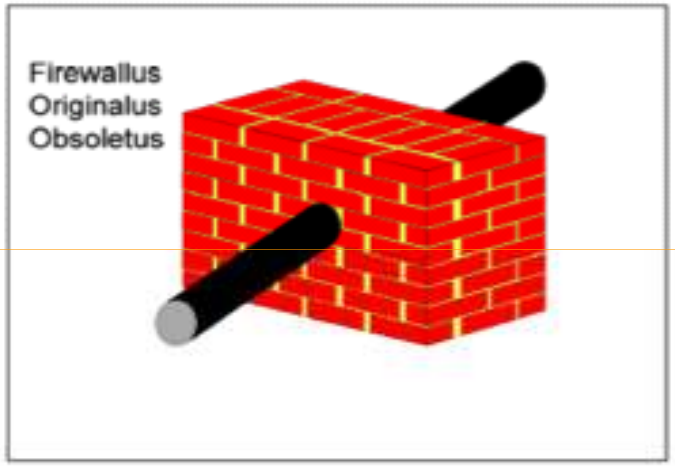


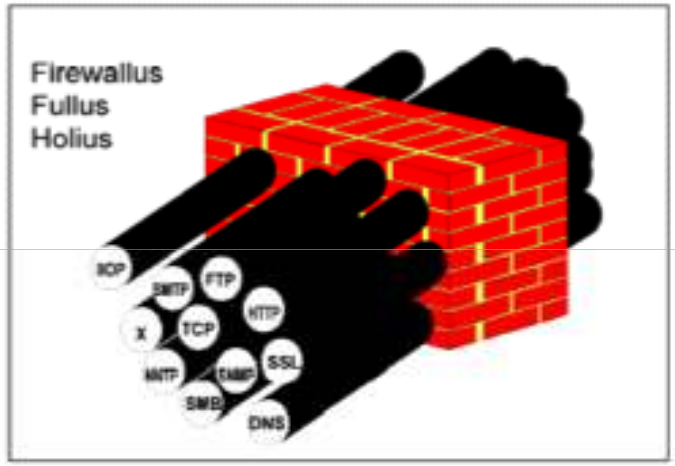
Password policies

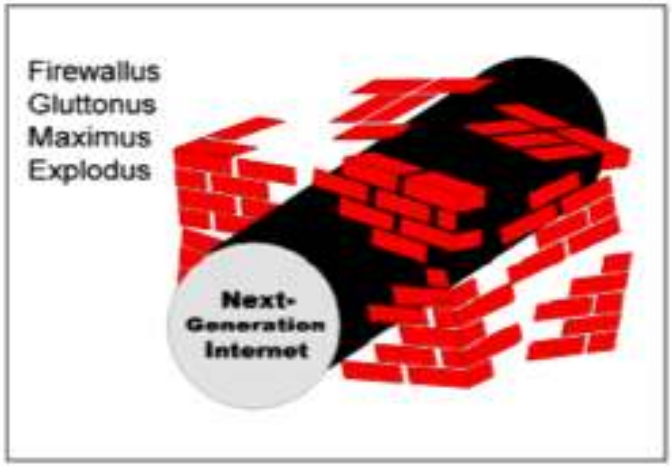
- Examples from the real world
- Security recommenders vs service providers
- Password history
- Change frequency
- Passwords are secret, but usernames?
- Password meters

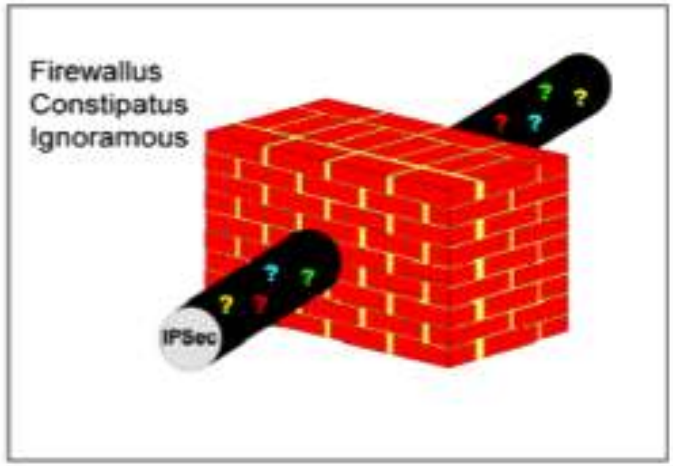
Some tech stuff

Tools,
attacks,
techniques









On/Offline password crackers

- Online
  - No names, no demos (i'm sorry)
- Offline
  - L0phtCrack
  - Cain & Abel
  - LCP
  - Elcomsoft Distributed Password Recovery
  - Ophcrack
  - John the Ripper
  - And many more….

EDB

Nobody is perfect…

- Virus/trojan/hacktools
  - AV vendors are NOT consistent in this area!
- No support for historical hash dumps
- Problems with historical hash dumps

Findings

More tech stuff

NOT to be exploited!

Windows password basics

- LM hash
- NTLM hash
- Windows security policy

Alternatives?

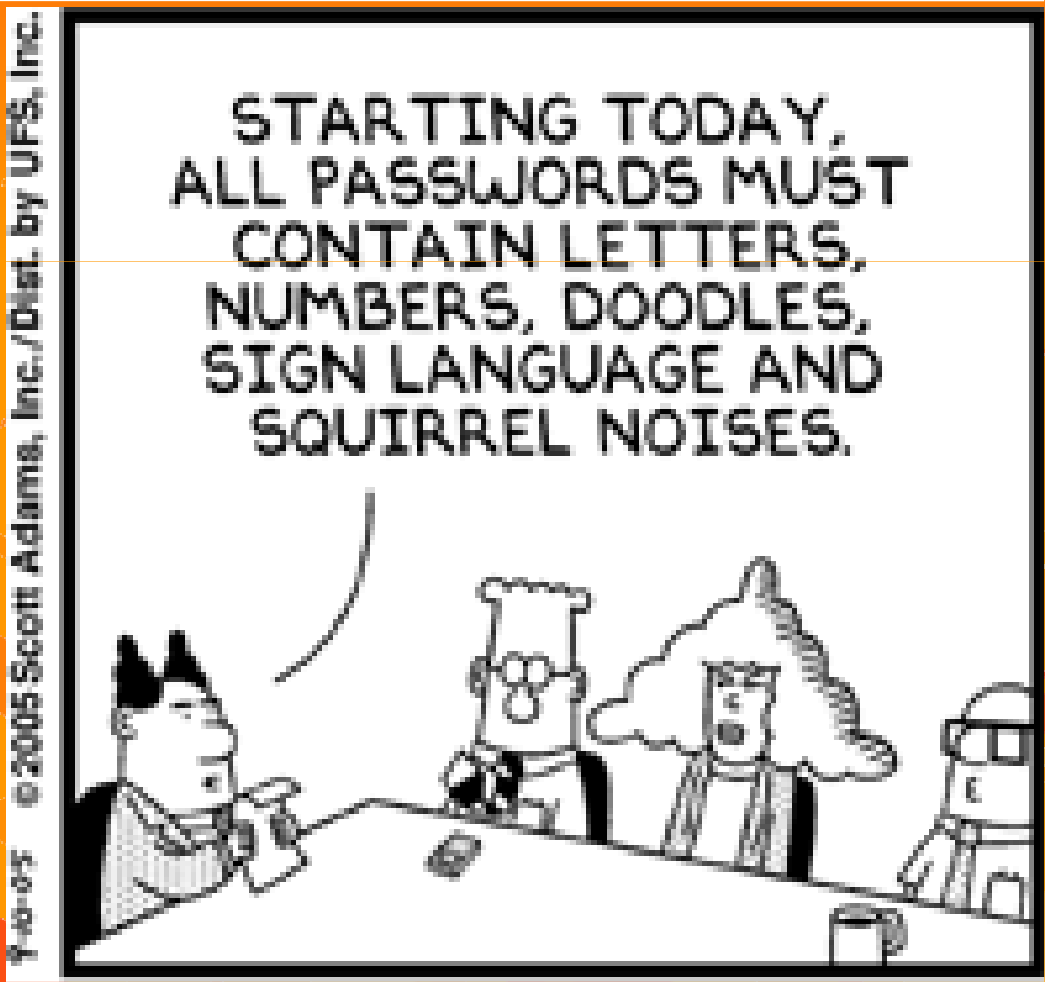
Alternatives?

- Identity Management
- 2 factor authentication
  - SecurID, mobile phones, BankID (!)
- Biometrics
  - Sure. What about Skynet and the Terminator?

EDB

Recommendations

Ordo ab chao



Feature requests

- Working command line password dumper with history support
- Rule-based configuration (John) for better control of hybrid/bruteforce attacks
- per-position charset support

- Goal #1: reduce time needed to crack ”crackable” passwords
- Goal #2: improve chances of cracking ”uncrackable” passwords based on statistics etc.

Recommendations

- Length 10 – change every 13 months
- One policy to rule them all
  - User training
  - Training technicians (Mordac, go away!)
  - Death by <insert-your-choice-here> for not complying with policy
- Do NOT reinvent the wheel (Ptacek)
  - http://chargen.matasano.com/chargen/2007/9/7/enough-with-the-rainbow-tables-what-you-need-to-know-about-s.html
- Write down your password

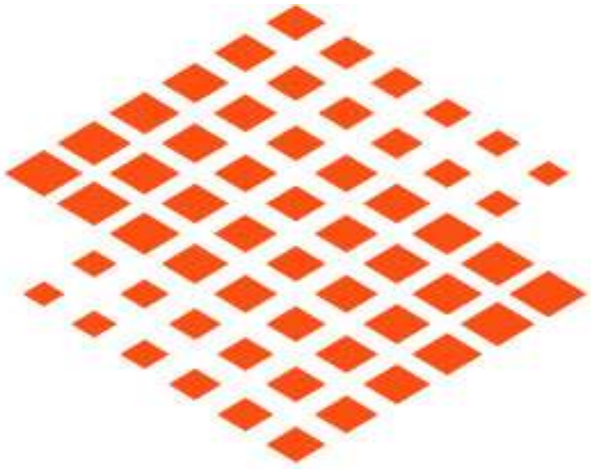
EDB

Thank you!

- Visit us at www.edb.com
- per.thorsheim@edb.com

- twitter.com/thorsheim
- linkedin.com/in/thorsheim
- securitynirvana.blogspot.com

EDB



EDB

More from IT™