Passwords & Security #Finse2011

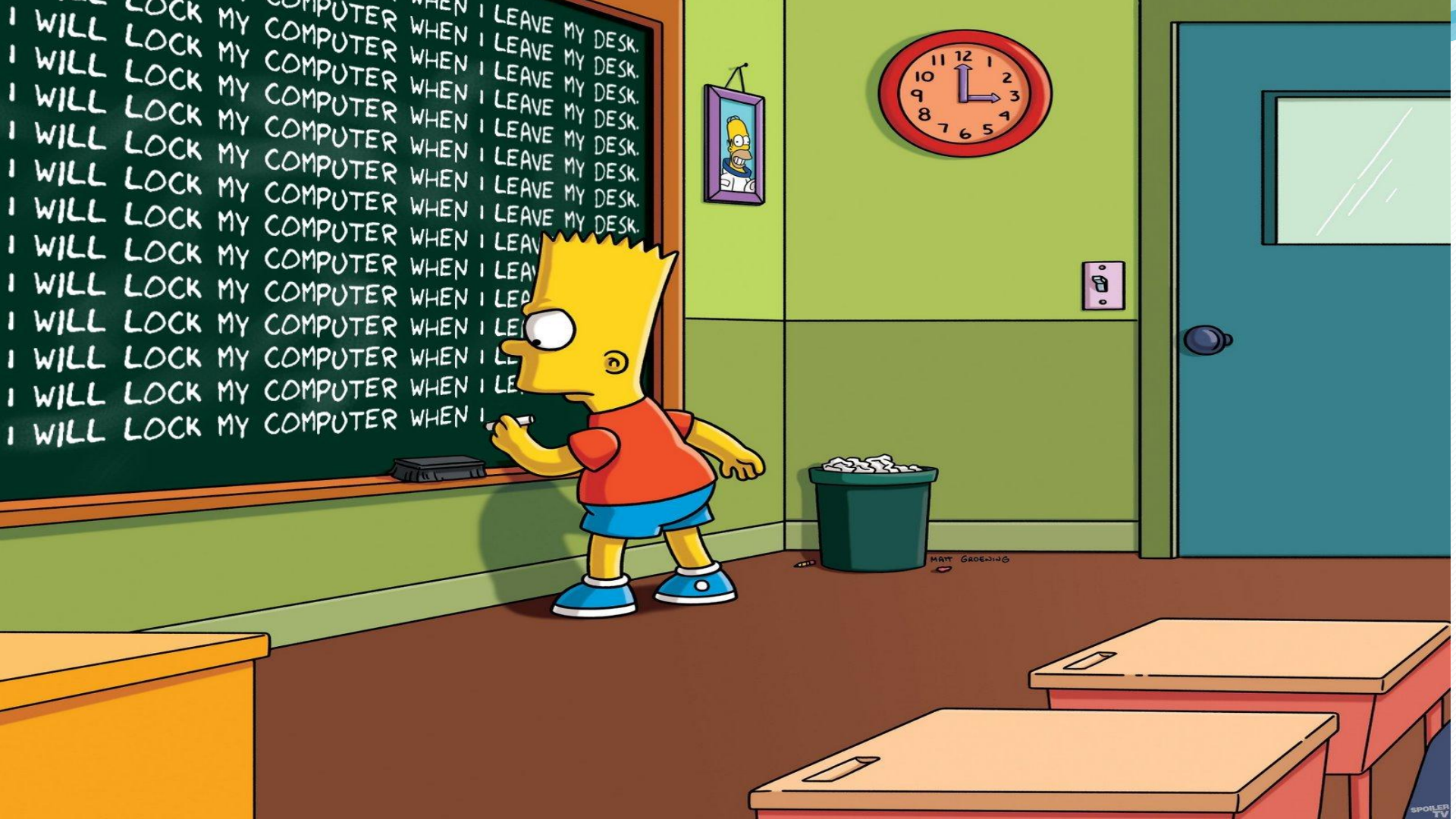
Per Thorsheim
CISA, CISM, CISSP-ISSAP
securitynirvana.blogspot.com

Disclaimer

My presentation, as well as anything I say, do, show, demonstrate, give away *or try to sell you* is my personal stuff & opinions.

My employer have chosen not to be a part of this in any way, as such my employer cannot and will not be held liable. My opinions does not necessarily reflect that of my employer, our customers or partners.

Etc etc.


I WILL LOCK MY COMPUTER WHEN I LEAVE MY DESK.
MATT GROENING

About me

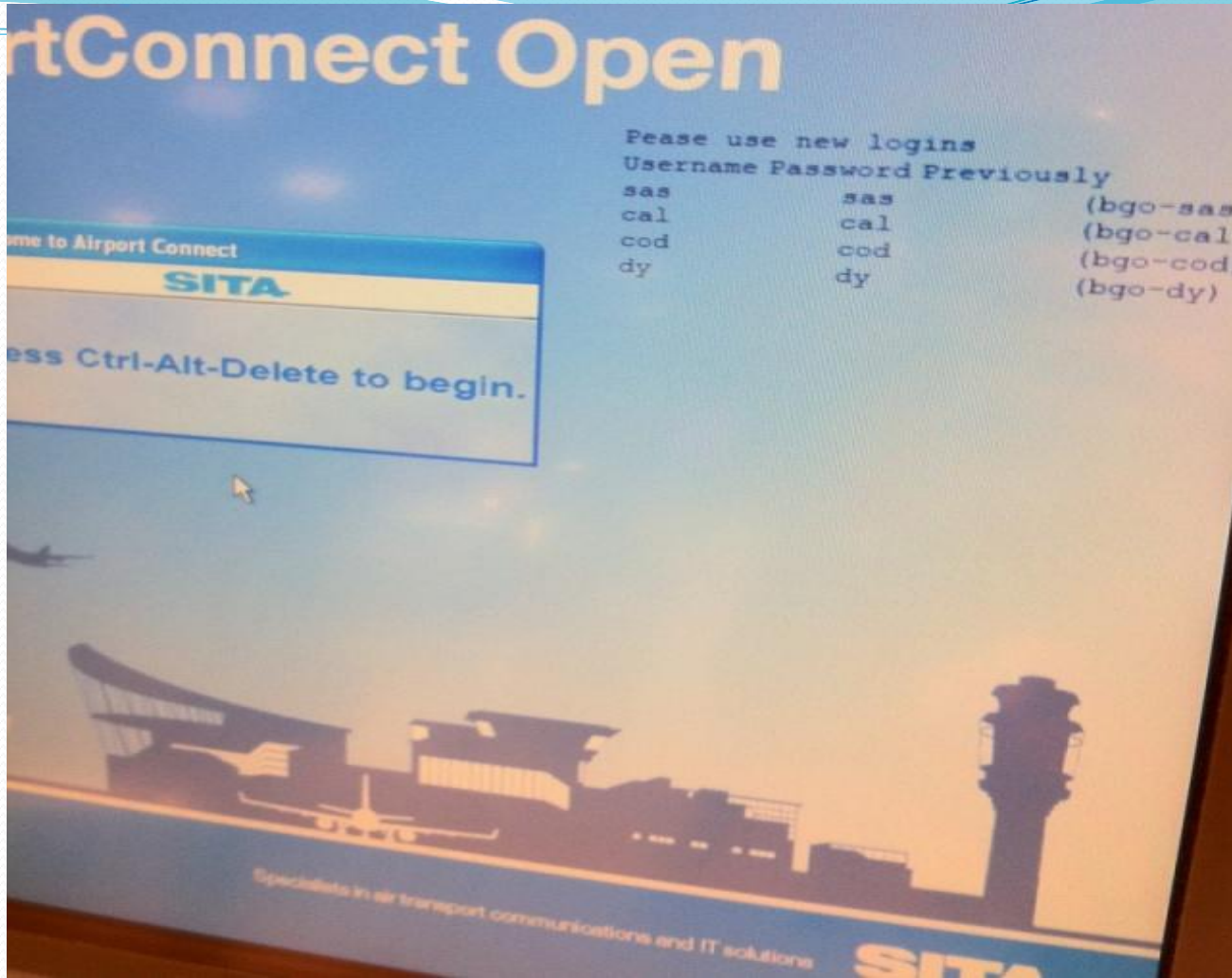
- Valid certifications:
  - Certified Information Systems Auditor
  - Certified Information Security Manager
  - Certified Information Systems Security Professional
  - Information Systems Security Architecture Professional
  - ITIL v3 Foundations

- Passwords^10 conference in December 2010
  - Videos: http://ftp.ii.uib.no/pub/passwords10/

Passwords^11, June 7-8, Bergen

- Prof. Frank Stajano (Cambridge)
- Prof. Kirsi Helkala (Gjøvik)
- Simon Josefsson (Head of R&D, Yubico)
- Bendik Mjaaland (Accenture)
- John Arild M. Johansen (CSO, Buypass)
- Erlend Dyrnes (CSO, Nextgentel)
- ~~Chris Lyon (Mozilla)~~
- James Nobis (Freerainbowtables.com)
- Dmitry Sklyarov (Elcomsoft)

Examples


rtConnect Open
Pease use new logins
Username Password Previously
sas sas (bgo-sas
cal cal (bgo-cal
cod cod (bgo-cod
dy dy (bgo-dy)
me to Airport Connect
SITA
ess Ctrl-Alt-Delete to begin.
SITA

Sony Playstation Network

- 70+ million accounts compromised
- #PSN unavailable for 3 weeks
- Playstation store unavailable for 4 weeks
- New firmware: v3.61
- All passwords must be changed

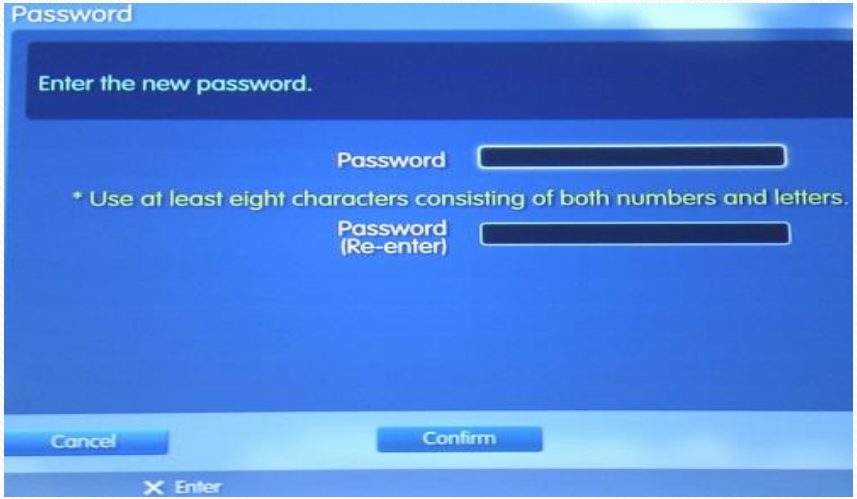
#PSN Password Reset

Playstation

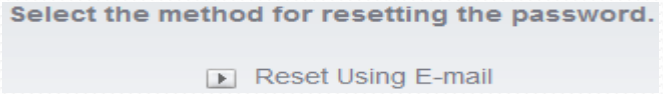
Online (web)

PS3 Policy #1 Revealed

Playstation

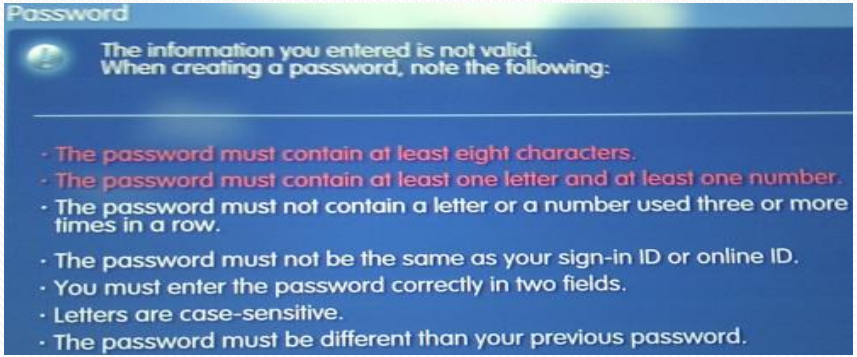


Online (web)



PS3 Policy #2 Revealed

Playstation



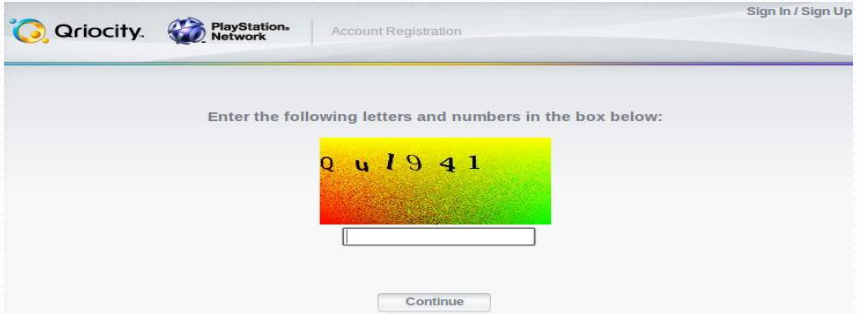
Online (web)

An e-mail message has been sent from PlayStation®Network to the following e-mail address:
pe

Web Password Reset CAPTCHA

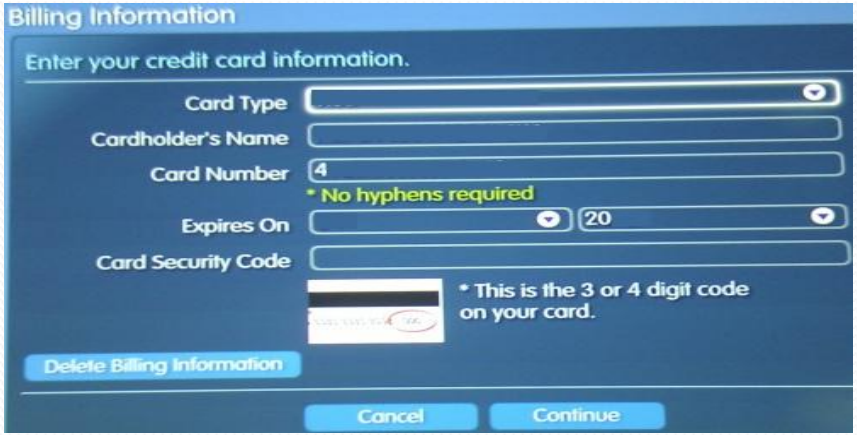
Playstation

Online (web)

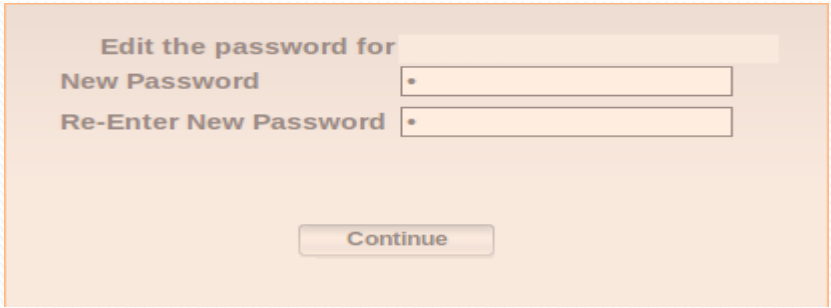


#PSN Partial CC Data Stored

Playstation

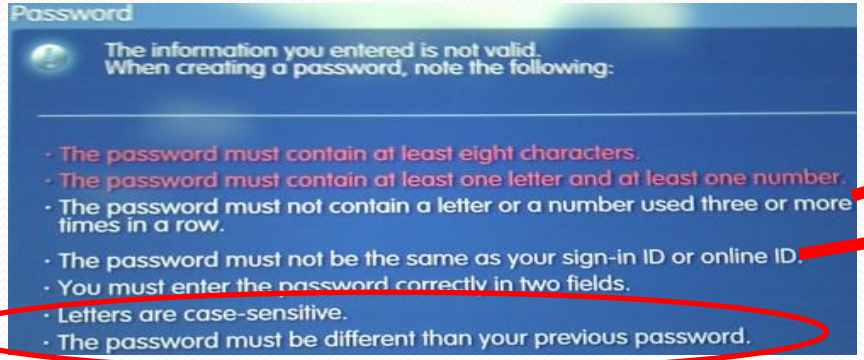


Online (web)



PS3 vs Web – Policy Comparison

Playstation



Online (web)

Your password must:
- contain at least eight characters
- contain at least one letter and one number
- not contain any character used more than two times in a row
- not match the sign-in ID

Please try again.

#PSN Password Reset

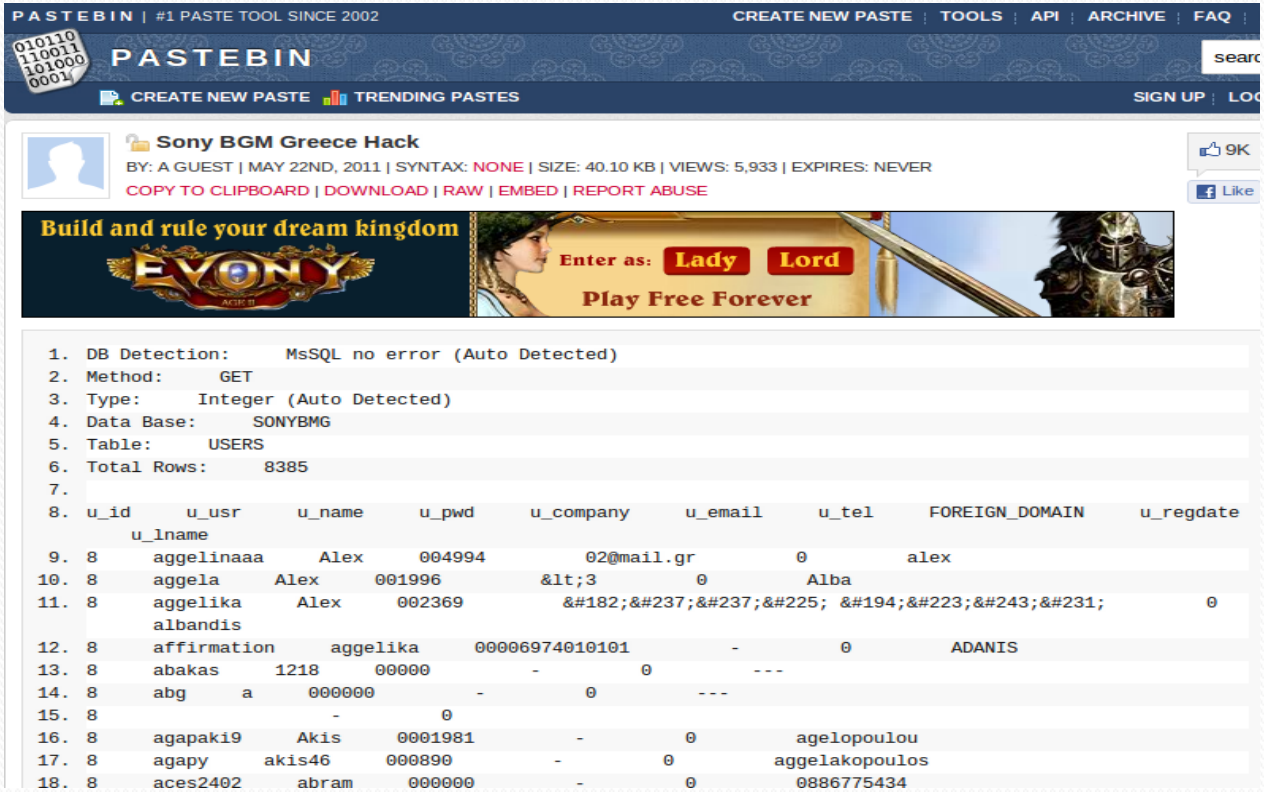
Playstation

Online (web)

The account password for has been updated.

#PSN – There's more!

Sony BGM Greece



PASTEBIN | #1 PASTE TOOL SINCE 2002 — CREATE NEW PASTE | TOOLS | API | ARCHIVE | FAQ

PASTEBIN

CREATE NEW PASTE | TRENDING PASTES — SIGN UP | LOG

Sony BGM Greece Hack

BY: A GUEST | MAY 22ND, 2011 | SYNTAX: NONE | SIZE: 40.10 KB | VIEWS: 5,933 | EXPIRES: NEVER

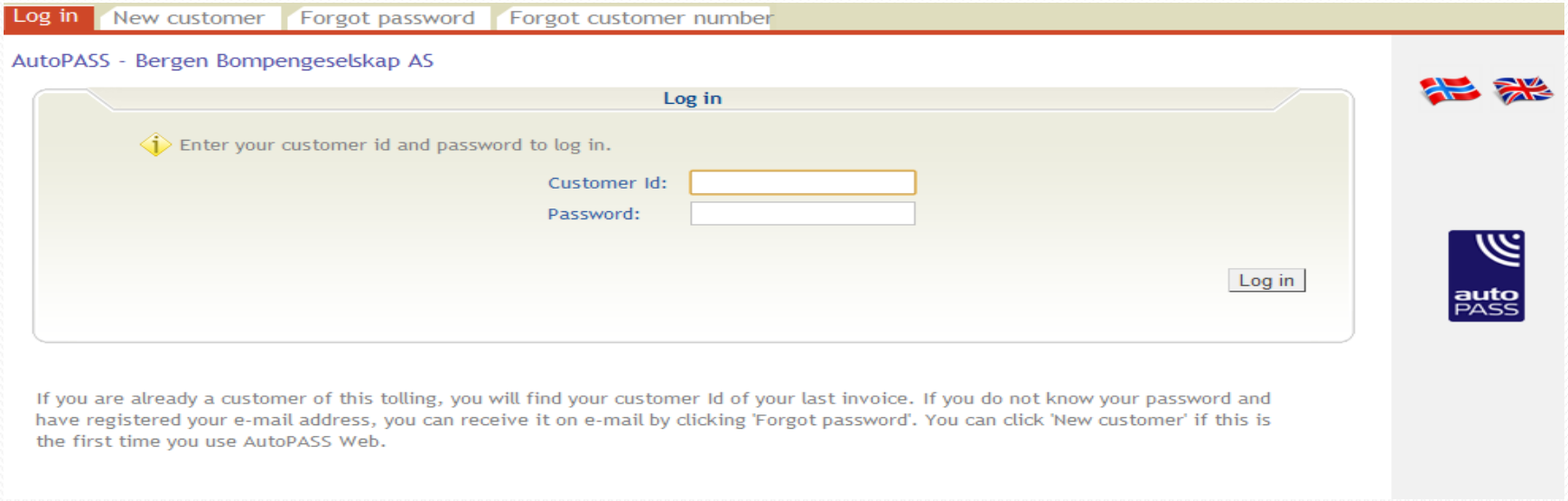
COPY TO CLIPBOARD | DOWNLOAD | RAW | EMBED | REPORT ABUSE

9K Like

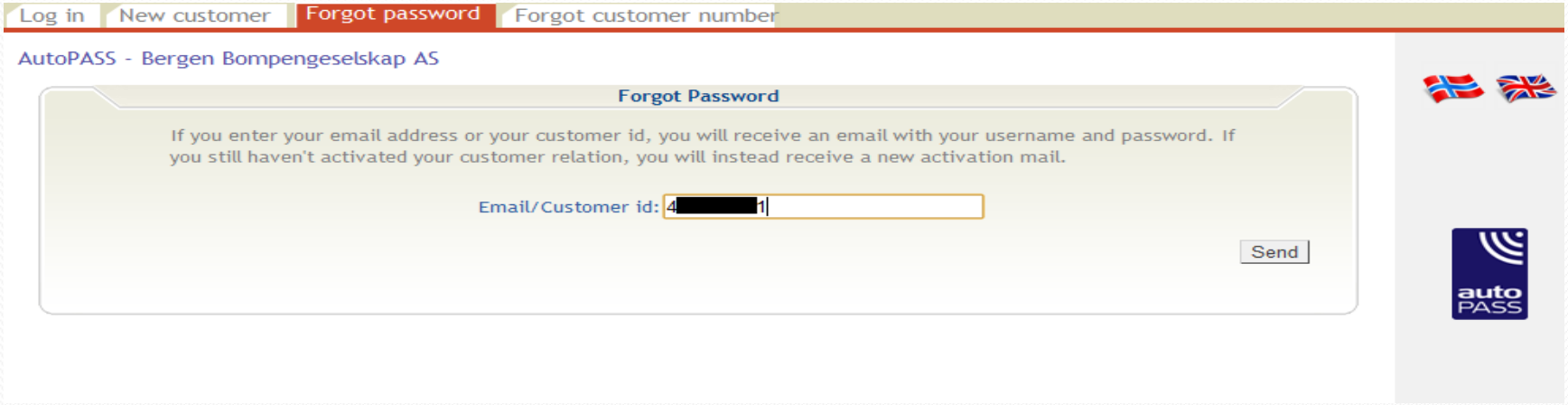

```
1.  DB Detection:     MsSQL no error (Auto Detected)
2.  Method:     GET
3.  Type:     Integer (Auto Detected)
4.  Data Base:     SONYBMG
5.  Table:     USERS
6.  Total Rows:     8385
7.
8.  u_id     u_usr     u_name     u_pwd     u_company     u_email     u_tel     FOREIGN_DOMAIN     u_regdate
        u_lname
9.  8     aggelinaaa     Alex     004994         02@mail.gr         0         alex
10. 8     aggela     Alex     001996         &lt;3         0         Alba
11. 8     aggelika     Alex     002369         &#182;&#237;&#237;&#225; &#194;&#223;&#243;&#231;         0
        albandis
12. 8     affirmation     aggelika     00006974010101         -         0         ADANIS
13. 8     abakas     1218     00000         -         0         ---
14. 8     abg     a     000000         -         0         ---
15. 8                     -         0
16. 8     agapaki9     Akis     0001981         -         0         agelopoulou
17. 8     agapy     akis46     000890         -         0         aggelakopoulos
18. 8     aces2402     abram     000000         -         0         0886775434
```

Bergen Bompengeselskap AS

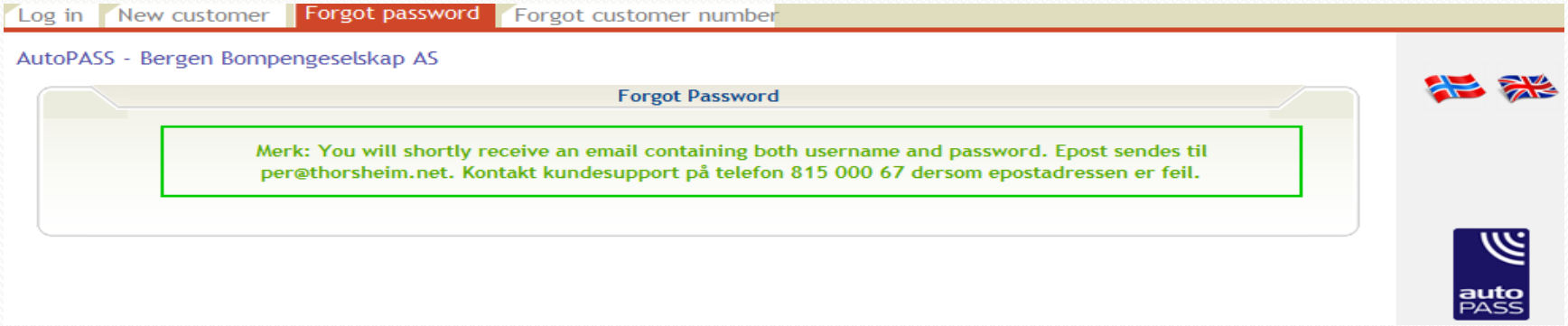
Login (https)


Log in
New customer
Forgot password
Forgot customer number
AutoPASS - Bergen Bompengeselskap AS
Log in
Enter your customer id and password to log in.
Customer Id:
Password:
Log in
If you are already a customer of this tolling, you will find your customer Id of your last invoice. If you do not know your password and have registered your e-mail address, you can receive it on e-mail by clicking 'Forgot password'. You can click 'New customer' if this is the first time you use AutoPASS Web.
auto PASS

I Forgot My Password!



Which Language Sir?



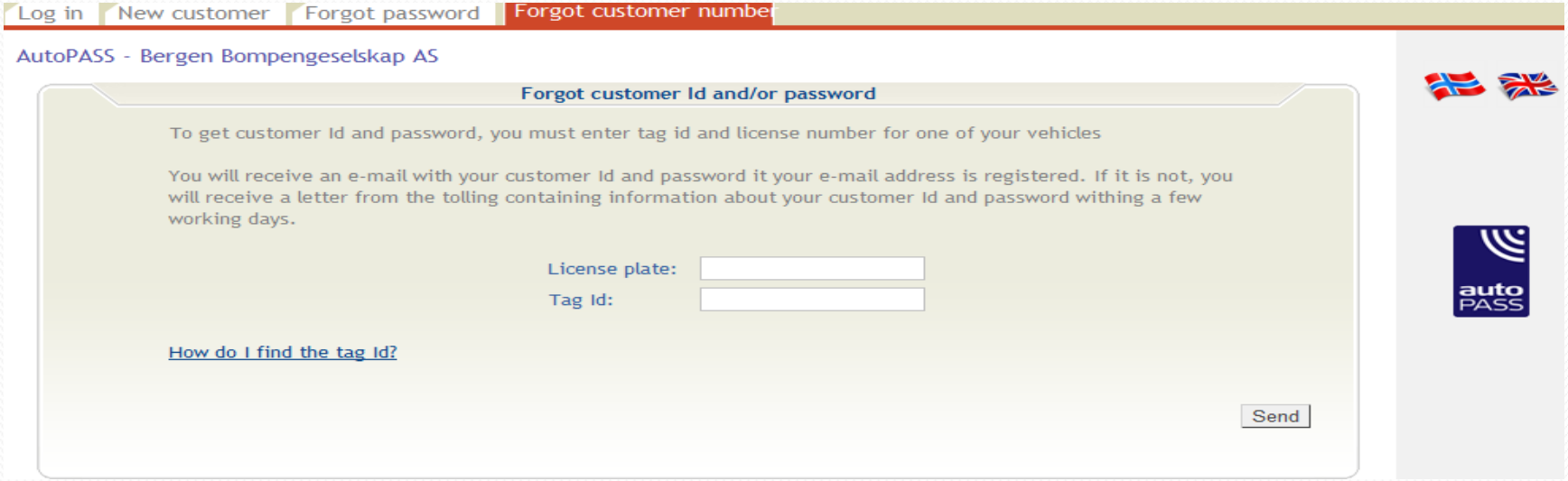
E-mail received:

Your customer id is 400210881 where the password is PMOsT;FxGuNBp`&EA4%L`Sp;

If support is needed, please use email address bergen@brotunnel.no or phone number 815 000 67

Best regards
Bergen Bompengeselskap AS
http://www.brotunnel.no/Default.aspx?tabid=584&subtabid=592

Or: License Number + Tag ID…



Breaking in – online attacks

Todo List

- We need:
  - Usernames and/or username algorithm at targetcorp
  - Windows domain (if applicable)
  - Account lockout policy
  - FQDN to webmail service
  - Online password cracker
  - Some passwords *(statistics are your friend!)*
  - *(Google is your friend…)*

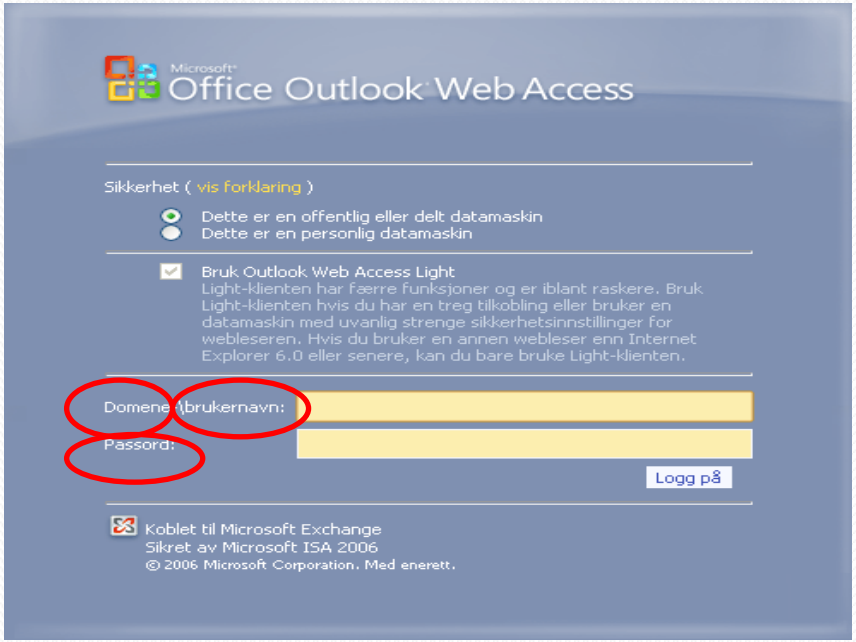
- And patience… ☺

Online Password Attacks

THC Hydra **Medusa** **Ncrack**

http://www.thc.org/thc-hydra/network_password_cracker_comparison.html

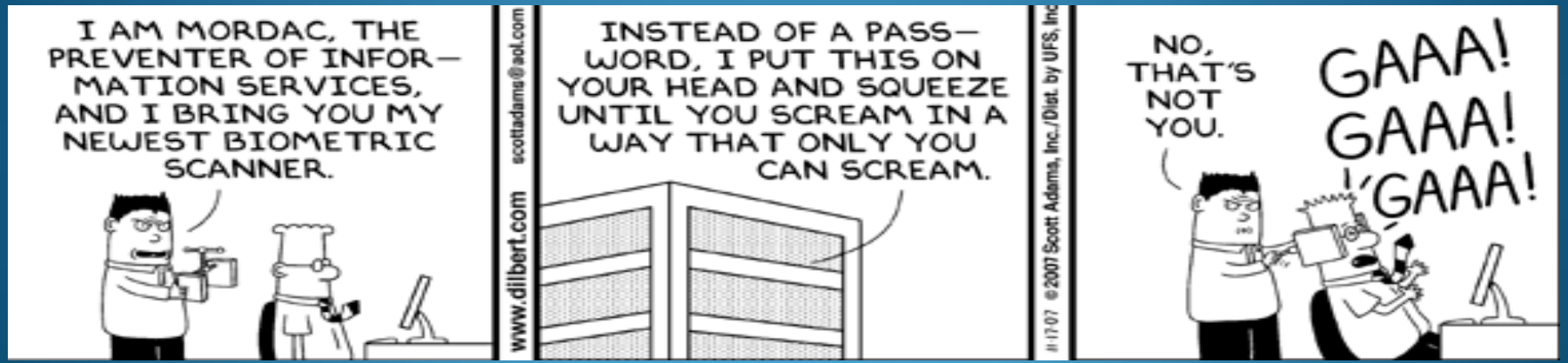
Possible targets found:



Potential targets:

- Webmail.ntnu.no
- Webmail.inbox.com
- Webmail.nr.no
- Webmail.uib.no
- Webmail.unik.no
- Webmail.uia.no
- Webmail.uni.lu

Offline Password Attacks



Got Hash?

SQL Injection Attacks:

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. It is an instance of a more general class of vulnerabilities that can occur whenever one programming or scripting language is embedded inside another.

Source: Wikipedia ☺

Hashkiller.com

Cracking Passwords

Offline password cracking

A wide number of tools & techniques available:

- Rainbowtables
- Dictionary attacks
- Various hybrid/logical attacks
- Bruteforce

- **Time is on your side!**

Rainbow Tables (wikipedia)

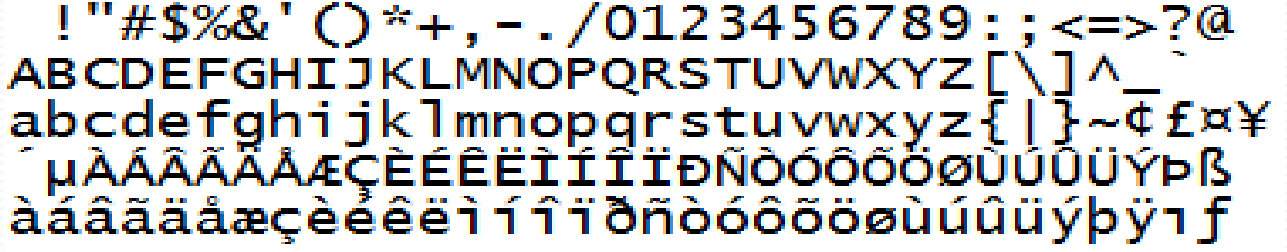
A **rainbow table** is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering the plaintext password, up to a certain length consisting of a limited set of characters. It is a form of time-memory tradeoff, using less CPU at the cost of more storage. Proper key derivation functions employ salt to make this attack infeasible. Rainbow tables are a refinement of an earlier, simpler algorithm by Martin Hellman that used the inversion of hashes by looking up precomputed hash chains.

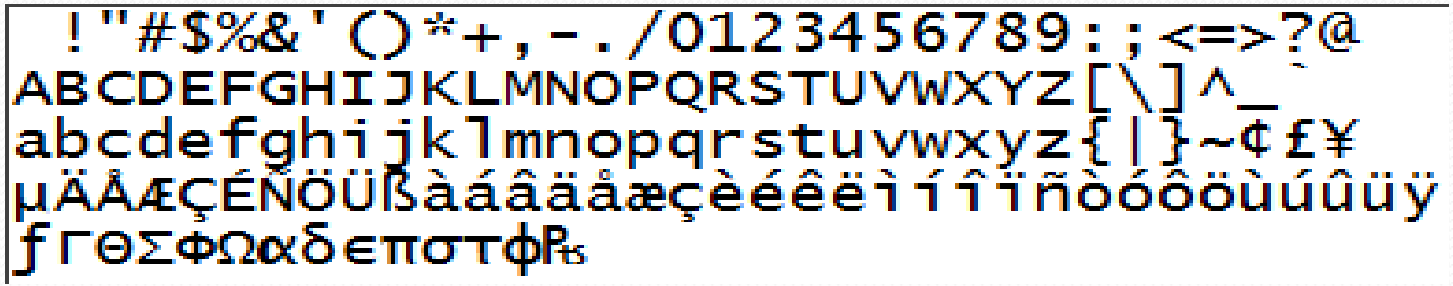
Rainbow Tables available:

- Freerainbowtables.com (99.9% hitrate)
  - LM/NTLM, MD5, SHA-1, HALFLMCHALL
    - CPU/GPU generation, CPU cracking (for now)
- Project-rainbowcrack.com
  - LM/NTLM, MD5, SHA-1 (CPU/GPU)
- Cryptohaze.com
  - MD5, NTLM
    - (Full US charset, chainlength 200k, GPU only!)

lm_lm-frt-cp437-850#1-7_20000

- Windows LM passwords length 1-14
- 566Gb (1400+ files) table set: charset coverage:





ntlm_mixalpha-numeric#1-8_40000

- Windows NTLM Mixalpha_numeric_1-8
- 453Gb, covers A-Z,a-z,0-9

Hybrid Rainbowtables

- ntlm_hybrid2(alpha#1-1,loweralpha#5-5,loweralpha-numeric#2-2,numeric#1-3)
- is currently being finished by freerainbowtables.com

- *With more to come!*

Hybrid attacks

- John the Ripper (JtR)
  - www.openwall.com/john/
- Hashcat family (lite, plus, ocl)
  - Hashcat.net
- Cain & Abel
  - www.oxid.it

- …
- *And many, many more!*

Bruteforce

- Bruteforcing is increasingly hard to do;
- Graphics Processing Units (GPUs) to the rescue!

Password Statistics

Time to show some cool/interesting/boring numbers!

Password Resets

Storing passwords

«I'm using MD5, so I'm safe.»

Response from web application developer after I talked about storing passwords in cleartext being a bad idea.

Thomas Ptacek

Enough With The Rainbow Tables: What You Need To Know About Secure Password Schemes

http://chargen.matasano.com/chargen/2007/9/7/enough-with-the-rainbow-tables-what-you-need-to-know-about-s.html

Lastpass.com

If you have a strong, non-dictionary based password or pass phrase, this shouldn't impact you - the potential threat here is brute forcing your master password using dictionary words, then going to LastPass with that password to get your data. Unfortunately not everyone picks a master password that's immune to brute forcing.

To counter that potential threat, we're going to force everyone to change their master passwords. Additionally, we're going to want an indication that you're you, by either ensuring that you're coming from an IP block you've used before or by validating your email address. The reason is that if an attacker had your master password through a brute force method, LastPass still wouldn't give access to this theoretical attacker because they wouldn't have access to your email account or your IP.

We realize this may be an overreaction and we apologize for the disruption this will cause, but we'd rather be paranoid and slightly inconvenience you than to be even more sorry later.

We're also taking this as an opportunity to roll out something we've been planning for a while: PBKDF2 using SHA-256 on the server with a 256-bit salt utilizing 100,000 rounds. We'll be rolling out a second implementation of it with the client too. In more basic terms, this further mitigates the risk if we ever see something suspicious like this in the future. As we continue to grow we'll continue to find ways to reduce how large a target we are.

Source: http://blog.lastpass.com/2011/05/lastpass-security-notification.html

Chris Lyon

- “SHA-512 w/ per User Salts is Not Enough”
- http://cslyon.net/2011/05/10/sha-512-w-per-user-salts-is-not-enough/

Bypassing Password Security

Bypassing Password Security

- Microsoft Windows Pass-the-Hash attacks
- Microsoft Windows Pass-the-Ticket attacks
- Forensic toolkits
  - Passware – «bypassing» Microsoft Bitlocker
  - Elcomsoft EPPB
- Smartphone (in)security

Pass-the-Hash / Pass-the-Ticket

- Windows Credentials Editor v1.2:
  - http://www.ampliasecurity.com/research.html

Scenario description:

Eve just started in Alices company. Bob, the domain admin guy, gives you your brand new laptop, ready to use. You have local admin rights. Bob's login credentials are cached on your computer. Extract, send credentials (username + hash value), get access.

Passware Kit Forensic

vs Microsoft Bitlocker:

- Live memory dump from target system using Firewire, utilizing Direct Memory Access. Search dump, get decryption keys, get access
- Remove disk from hibernated computer. Physical memory is written to disk, parts of it unencrypted. Search and find decryption keys, mount volume, get access.

- Video demonstration:
  - http://ftp.ii.uib.no/pub/passwords10/Passware_at_Passwords10.mp4

Corporate Android Security

- Android devices: no hardware encryption
- Nitro software – software encryption
  - But only for Microsoft Activesync data
    - (Mail, Calendar, Contacts)

- Samsung Galaxy S II
  - Hardware device encryption
  - 90% of all MS Activesync policies supported
    - Not even Microsoft does that!

Corporate iOS Security

iPod

Navn: iPod touch
Kapasitet: 59,42 GB
Programvareversjon: 4.2.1
Serienummer: 9C9465RX6K4

Versjon

Søk etter oppdateringer

iPod-enheten har nyeste versjon av programvaren. iTunes søker automatisk etter oppdateringer igjen 25.01.2011.

Gjenopprett

Hvis du har problemer med iPod, kan du gjenopprette originalinnstillingene ved å klikke på Gjenopprett.

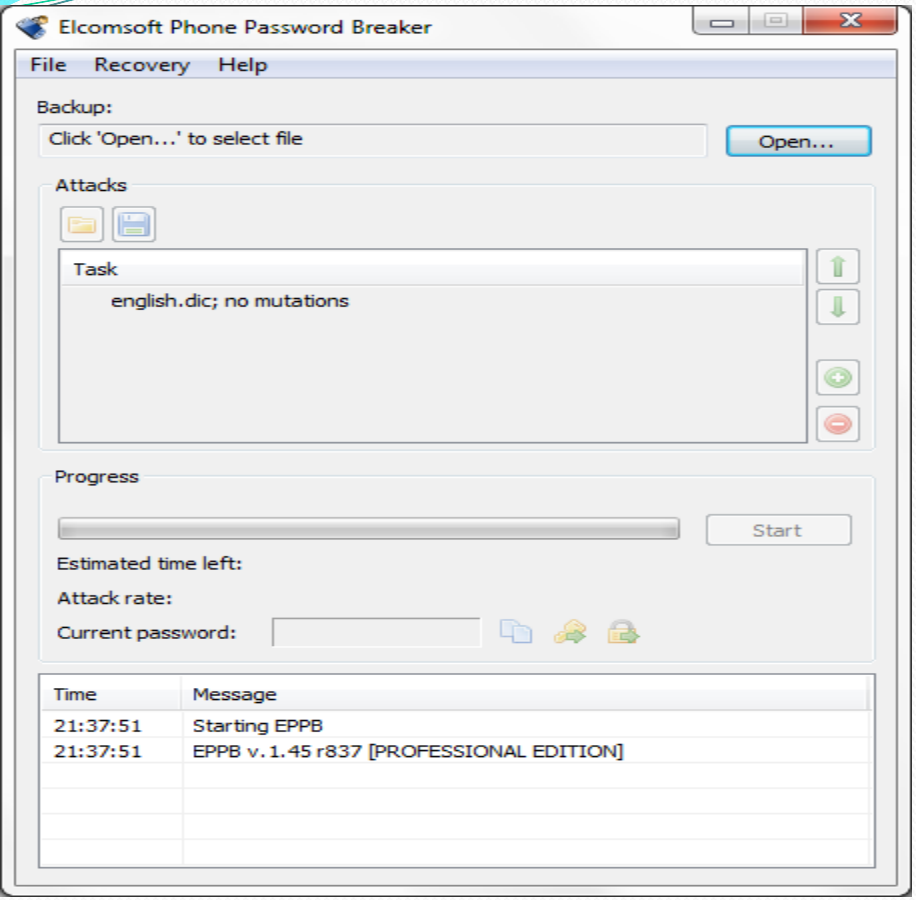
Valg

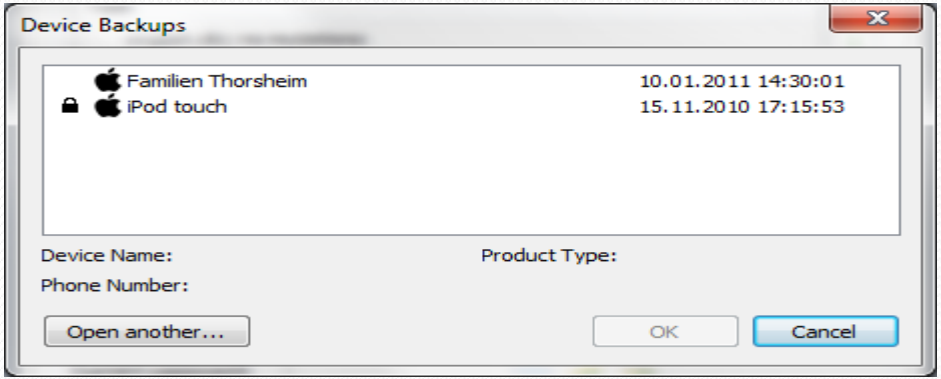
- [x] Åpne iTunes når denne iPod-enheten kobles til
- [ ] Synkroniser kun avkryssede sanger og videoer

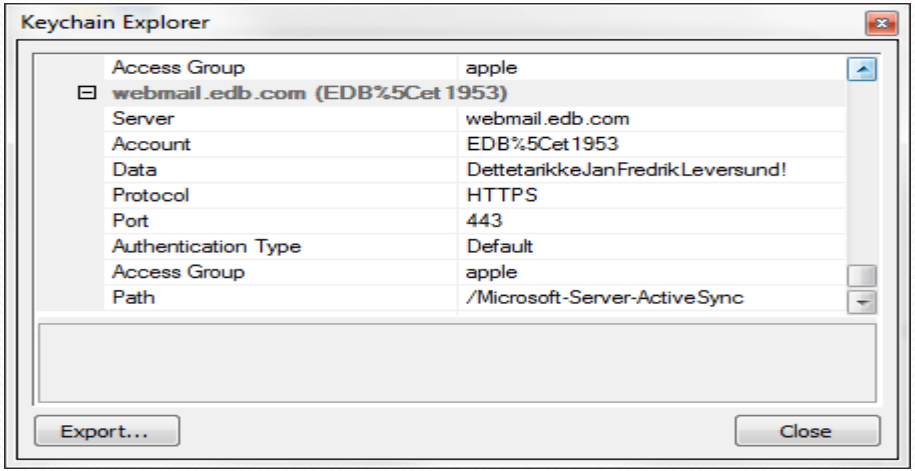
- [x] Krypter iPod-sikkerhetskopi

Endre passord...

Konfigurer Særlige behov...


Elcomsoft Phone Password Breaker
File Recovery Help
Backup:
Click 'Open...' to select file
Open...
Attacks
Task
english.dic; no mutations
Progress
Start
Estimated time left:
Attack rate:
Current password:
Time Message
21:37:51 Starting EPPB
21:37:51 EPPB v.1.45 r837 [PROFESSIONAL EDITION]


Device Backups
Familien Thorsheim 10.01.2011 14:30:01
iPod touch 15.11.2010 17:15:53
Device Name:
Product Type:
Phone Number:
Open another...
OK
Cancel


Keychain Explorer
Access Group apple
webmail.edb.com (EDB%5Cet1953)
Server webmail.edb.com
Account EDB%5Cet1953
Data DettetarikkeJanFredrikLeversund!
Protocol HTTPS
Port 443
Authentication Type Default
Access Group apple
Path /Microsoft-Server-ActiveSync
Export...
Close

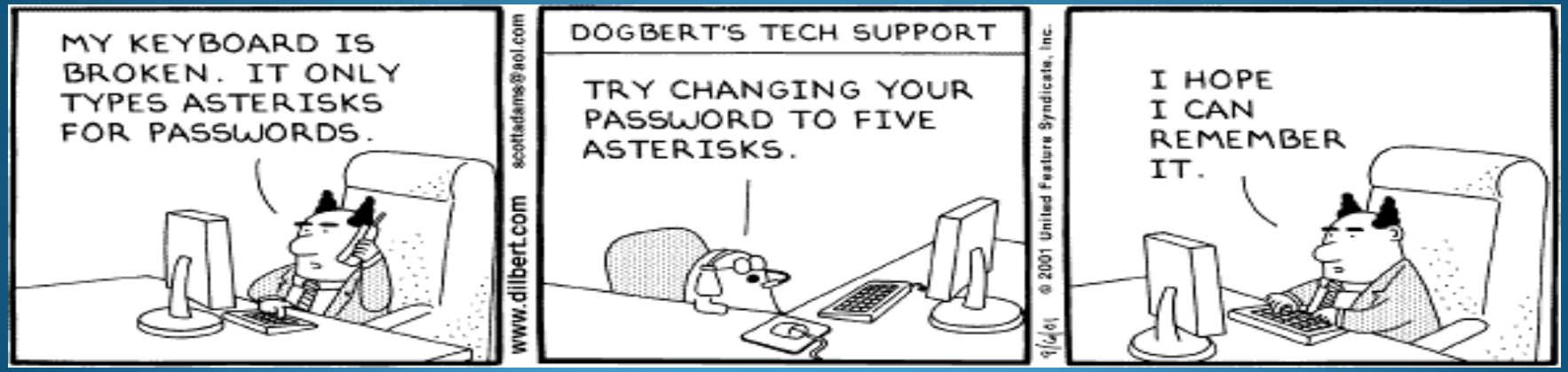
Corporate iOS Security

- AES hardware device encryption is good, *but*..
  - iTunes configuration issues
    - Frequent updates *(Quicktime + Safari + iTunes)*
    - Backup password protection
    - Hardware Device has «password protect» flag
- Without password protection:
  - Device-specific encryption key is used to protect keychain
  - Almost all other data available unencrypted in backup

Elcomsoft, Tuesday, May 24th:

http://www.prweb.com/releases/iPhone/forensics/prweb8470927.htm

Password Usability



NorSIS / nettvett.no (Norway)

Anbefaling	NorSIS	Nettvett
Bruk kombinasjon av tall og bokstaver		Y
Passordet må være lett å huske		Y
Passordet må være lett å huske, men vanskelig for andre å gjette		Y
Passordet bør bestå av en kombinasjon av små og store bokstaver, tall og spesialtegn		Y
Vær forsiktig med å bruke det samme passordet på flere tjenester		Y
Unngå bruk av ord som finnes i ordlister eller knyttet til personlig informasjon		Y
Passordet bør ikke inneholde bokstavene Æ, Ø eller Å		Y
Tips: Bruk L33T språk (bokstav <-> tall erstatninger)		Y
Minstelengde	8	8
Bruk store og små bokstaver	Y	Y
Tips: forkortede setninger (5rEftd7M)	Y	Y
Baser ikke passord eller PIN-koder på personlig informasjon	Y	
Unngå ord som finnes i ordbøker (gjelder alle språk)	Y	
Unngå bokstavkombinasjoner som ligner på ord	Y	
Passord bør være så langt som mulig, og minst 8 tegn	Y	
Benytt ulike passord for ulike tilganger	Y	
Bytt passord med jevne mellomrom	Y	
Bruk passfraser (setninger)	Y	
Oppgi aldri passord eller koder til noen – selv ikke banken	Y	
Passord skal være på minimum åtte tegn, og skal inneholde både bokstaver, tall og eventuelt spesialtegn	Y	
Alle standard brukeridenter og passord fra leverandører skal endres før produktet settes i produksjon	Y	

Password Usability

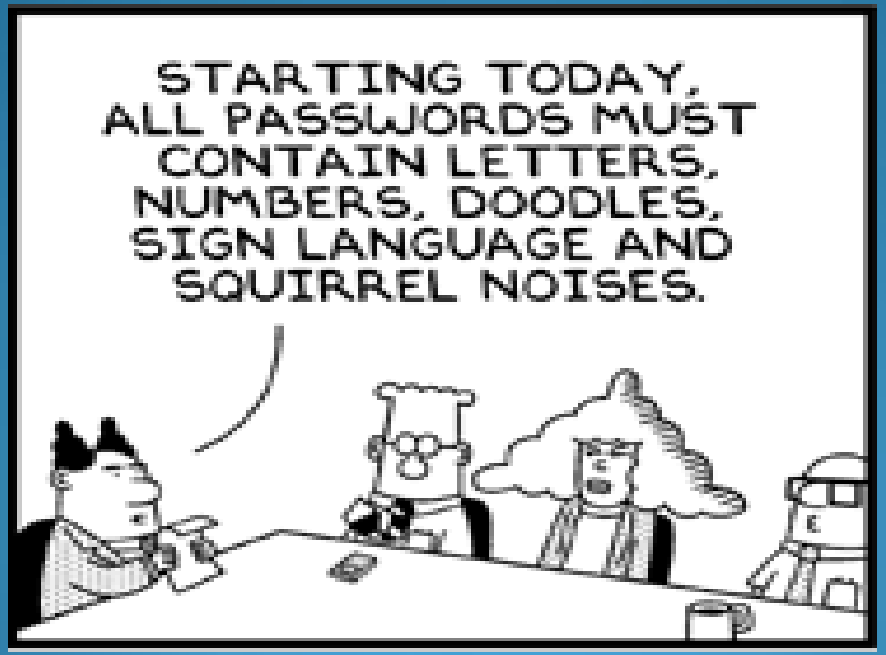
- Minimum/Maximum Length
- Complexity requirements
- Password History
- Change Frequency
- Lost Password (Password Reset)
- Reauthentication (BankID)
- Single Sign-On

Usability vs Security

- Minimum/Maximum Length
- Complexity requirements
- Password History
- Change Frequency
- Lost Password (Password Reset)
- Reauthentication (BankID)
- Single Sign-On

- Use passphrases / implement support for it!
- Length = complexity
- Pattern detection
- «Window of opportunity»
- VERY hard to do in real-life environments!
- «Dear mom…»
- Good idea, but…

Recommendations



My User Recommendation:

Use a normal sentence as your password.

Change it when you think it is necessary.

My Policy Recommendation:

Use a normal sentence as your password.

It must be changed every 13 months.

Technical Recommendation

- Has to be a little more complex then the previous slides, but;
  - Do NOT tell your end-users or others about the actual rules implemented!
- Provide **useful feedback** when passwords are rejected
- Do 100% **technical** implementation of **written** policy
- SSO: store password hashes at the **strongest** system

Dynamic Prevention of Common Passwords

- Some websites have static lists of «forbidden» (common) passwords
- Can be found & documented (Twitter…)
- Does not provide better security
- Easily circumvented (blocking bad passwords is hard!)

Dynamic Prevention of Common Passwords

My suggestion:

- A custom DLL for Windows. It receives a users requested password. Check against rules (length, complexity, history etc).
- If OK, then hash and store hash with counter = 1
- DLL config has a threshold value
  - Any given password can only exist on X accounts at the same time

Thank you!

And do not forget: Passwords^11, June 7-8, UiB, Bergen.
2 days, only about passwords.