Passwords & Security #Finse2011 Per Thorsheim

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.



# 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)

### rtConnect Open

# Examples

me to Airport C	onnect		
	SITA.		
ess Ctrl-/	Alt-Delete	to be	gin.
	3		
-			
Line	CONTRACTOR OF	_	-
The second			-
		The set L at the	
		the second se	and the second se

Pease us	e new logins	
Username	Password Prev	iously
sas	383	iban
cal	cal	(bgo-
cod	cod	(bgo-
dy	dy	(bgo-

-

sas

# 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)**

Password	Account Management
Your password is no longer valid. You must change your password.	Enter your sign-in ID and date of birth to reset your password. Sign-In ID
	(E-mail Address)
O Back X Enter	Cancel Continue

# PS3 Policy #1 Revealed

#### Playstation

Password		
Enter the new pas	ssword.	
* Use at least	Password ( eight characters consis Password (Re-enter)	ting of both numbers and letters.
Cancel	Confin	m
× Enter		



**Online** (web)

Reset Using E-mail

# PS3 Policy #2 Revealed

#### Playstation

### **Online (web)**

#### Password

The information you entered is not valid. When creating a password, note the following:

- The password must contain at least eight characters.
- The password must contain at least one letter and at least one number.
- The password must not contain a letter or a number used three or more times in a row.
- The password must not be the same as your sign-in ID or online ID.
- · You must enter the password correctly in two fields.
- Letters are case-sensitive.
- The password must be different than your previous password.

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

pe

### Web Password Reset CAPTCHA

**Online (web)** 

Sian In / Sian Up

### Playstation





# **#PSN Partial CC Data Stored**

#### Playstation

**Online (web)** 

Billing Information	
Enter your credit card inf	ormation.
Card Type	Olympic de la construcción de
Cardholder's Name	
Card Number	4
Expires On	No hyphens required Solution
Card Security Code	
	This is the 3 or 4 digit code on your card
	the second secon
Delete Billing Information	
	Cancel Continue

Edit the password for	
Eun me password for	
New Password •	
Re-Enter New Password	
Contin	ue

### PS3 vs Web – Policy Comparison Playstation Online (web)

#### Password

The information you entered is not valid. When creating a password, note the following:

- The password must contain at least eight characters.
- The password must contain at least one letter and at least one number.
- The password must not contain a letter or a number used three or more times in a row.
- The password must not be the same as your sign-in ID or online ID.
- You must enter the password correctly in two fields.
- Letters are case-sensitive.
- The password must be different than your previous password.

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's May, so far: 1) PSN hack 2) SOE hack 3) Sweepstakes hack 4) PSN password glitch 5) Phishing site on sony.co.th... #bettersafethansony

# Sony BGM Greece

PAST	EBIN	#1 PASTE TO	DOL SINCE 200	)2		CRE	ATE NEW PASTE	TOOLS	
010110 11001 10100	P	ASTE	BIN						sear
000	- <mark></mark>	REATE NEW	PASTE 📲 T	RENDING PAS	TES				SIGN UP   LO
5	B	Sony BG Y: A GUEST   N OPY TO CLIPE	M Greece MAY 22ND, 20: 30ARD   DOW	HACK 11   SYNTAX: N 'NLOAD   RAW	ONE   SIZE: 40.10   EMBED   REPOR	) KB   VIEWS: 5,93 RT ABUSE	3   EXPIRES: NEVE	R	∎ 9K
Bui	ld an	d rule you	r dream k	¦ingdom ₹	Enter Pla	as: Lady y Free Fore	Lord ever		
1. 2. 3.	DB De Metho Type: Data	tection: d: GET Integ Base:	MsSQL n er (Auto D SONYBMG	o error (Au etected)	to Detected)				
5	Table	· LISER	S						
6	Total	Rows -	8385						
7.	····		0000						
8.	u_id u	u_usr _lname	u_name	u_pwd	u_company	u_email	u_tel	FOREIGN_DOMAIN	N u_regdate
9.	8	aggelinaa	a Alex	004994	02@n	ail.gr	0 a	lex	
10.	8	aggela	Alex	001996	<3	Θ	Alba		
11.	8	aggelika albandis	Alex	002369	¶	íí	á Â8	#223;ó	31; 0
12.	8	affirmati	on agg	elika 0	0006974010101	- 1	Θ	ADANIS	
13.	8	abakas	1218	00000	-	0 -			
14.	8	abg a	00000	9 -	Θ				
15.	8		-	Θ					
16.	8	agapaki9	Akis	0001981	-	Θ	agelopoulou		
17.	8	agapy	akis46	000890	-	Θ	aggelakopoulo	S	
18.	8	aces2402	abram	000000	-	Θ	0886775434		

# Bergen Bompengeselskap AS

# Login (https)

Log in New customer Forgot password Forgot customer number		
AutoPASS - Bergen Bompengeselskap AS		
Log in		<b>**</b> **
(i) Enter your customer id and password to log in.		
Customer Id:		
Password:		
	Log in	euto PASS

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.

# I Forgot My Password!

Log i	n New customer	Forgot password	Forgot customer number	
Auto	PASS - Bergen Bomp	engeselskap AS		
			Forgot Password	
	If you enter you still hav	your email address or yo en't activated your custo	our customer id, you will receive an email with your username and password. If omer relation, you will instead receive a new activation mail.	
		Em	ail/Customer id: 4	
			Send	<u>الا</u>
				auto PASS

# 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...

Log in N	ew customer	Forgot password	Forgot customer number	
AutoPASS -	Bergen Bomp	engeselskap AS		
			Forgot customer Id and/or password	
	To get custo	mer Id and password, y	ou must enter tag id and license number for one of your vehicles	
	You will rece will receive working day	vive an e-mail with your a letter from the tolling s.	customer Id and password it your e-mail address is registered. If it is not, you containing information about your customer Id and password withing a few	
			License plate:	
			Tag Id:	PASS
	How do I fin	d the tag Id?		
			Sand	
			Send	
1				

# **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:



#### Sikkerhet ( vis forklaring )

- Dette er en offentlig eller delt datamaskin
- Dette er en personlig datamaskin

#### Bruk Outlook Web Access Light

Light-klienten har færre funksjoner og er iblant raskere. Bruk Light-klienten hvis du har en treg tilkobling eller bruker en datamaskin med uvanlig strenge sikkerhetsinnstillinger for webleseren. Hvis du bruker en annen webleser enn Internet Explorer 6.0 eller senere, kan du bare bruke Light-klienten.



#### **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 <u>code injection</u> technique that exploits a <u>security</u> <u>vulnerability</u> occurring in the <u>database</u> layer of an <u>application</u>. The vulnerability is present when user input is either incorrectly filtered for <u>string literal escape characters</u> embedded in <u>SQL</u> statements or user input is not <u>strongly typed</u> 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 😳

12	S	nkil	<b>Ie</b>	CC	om						
ð	14	ashi	kill	ler			Did yo May 24	u miss your a 4, 2011, 10:4 Donate	ctivation e 6:28 am	mail?	
Webc	rack	Opencrack	Forum	Hashes	Downloads	Chat	About	Stats			
										Pagistan	a gip
lashki ages:	iller » : 123	English » Hash 3 [4] 5 6 37	icracking				Stautod ku	Deed		Last post	
l Mem	ber an	Subject d 4 Guests are view	wing this boa	ard.			Started by	кері	ies views	Last post 🗸	
	•	Wordpress has	sh - please	help crack			bugn3t	0	59	May 02, 2011, 08:33:46 am by bugn3t	ľ
Î	•	1 LM:NTLM has	sh				geocine	1	40	May 02, 2011, 08:11:00 am by geocine	- 27
î.	•	msql4/5 hash	×4				BON3	0	37	May 02, 2011, 02:36:31 am by B0N3	- 2
Î.	-	mysql5 passwo	ord Do rea	dable?			yang	0	42	May 01, 2011, 20:11:23 pm by yang	1
î.	-	Please Crack :	)				1337	3	108	May 01, 2011, 15:03:06 pm by AbakBarama	ť
<b>1</b> 11	•	806077 uncra	cked hash	es! « 1 2 »			BlandyUK	15	634	May 01, 2011, 13:44:26 pm by fuzen	1
Î.	٠	Vbulletin Hard	:S				1337	0	35	May 01, 2011, 09:23:55 am by 1337	. 2
-	-	MD5 x 4 vBulle	etin				BON3	0	41	May 01, 2011, 01:39:49 am by B0N3	1
									24	April 30, 2011, 22:37:06 pr	n f
	-	5 x phpbb3					cneezy	U	34	by cheezy	

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

<u>566Gb (1400+ files) table set: charset coverage:</u> <u>!"#\$%&'()\*+,-./0123456789:;<=>?@</u> ABCDEFGHIJKLMNOPORSTUVWXYZ[\]^\_ abcdefghijklmnopqrstuvwxyz{|}~¢£¤¥ µAAAAAAÆÇÈÉÊËÌÍÍĨÐÑÒÓÔÕÖØÙÚÜÜÝÞß àáâãäåæçèéêëìíîîðñòóôõöøùúûüýþÿ1f

> !"#\$%&'()\*+,-./0123456789:;<=>?@ ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^\_ abcdefghijklmnopqrstuvwxyz{|}~¢f¥ 掏ÆÇÉŇÖÜßàáâäåæçèéêëìíîîñòóôöùúûüÿ ƒΓΘΣΦΩαδεπστφ‰

### ntlm\_mixalpha-numeric#1-8\_40000

- Windows NTLM Mixalpha\_numeric\_1-8
- 453Gb, covers A-Z,a-z,o-9

# Hybrid Rainbowtables

- ntlm\_hybrid2(alpha#1-1,loweralpha#5-5,loweralphanumeric#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/enoug h-with-the-rainbow-tables-what-you-need-to-knowabout-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**



![](_page_44_Picture_2.jpeg)

# **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\_Passwords 10.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**

![](_page_49_Picture_1.jpeg)

iPod		
= 7 <b>=</b> 4	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 søk	(er
	automatisk etter oppdateringer igjen 25.01.2011.	
Gienopprett	Hvis du har problemer med iPod, kan du gjenopprette	
	originalinnstillingene ved å klikke på Gjenopprett.	
Valg		
t dig		
$\checkmark$	Åpne iTunes når denne iPod-enheten kobles til	
	Synkroniser kun avkryssede sanger og videoer	
	· · · · · · · · · · · · · · · · · · ·	
Knynter iDod-s	ikkorbotskoni Eng	Iro paccord
Kiypter iPou s	ikkemetskopi ( End	ne passoru
	Konfigurer Særlige behov	

Elcomsoft Phone Password Breaker		Device Backups	
ile Recovery Help			
Backup:		É Familien Thorsheim	10.01.2011 14:30:01
Click 'Open' to select file	Open	🔒 🗯 iPod touch	15.11.2010 17:15:53
Attacks			
Task		Device Name:	Product Type
english.dic: no mutations		Device Name:	Product Type:
		Phone Number:	
		Open another	OK Cancel
		Keychain Explorer	
Progress			
rigicas		Access Group	apple
	Start	E webmail.edb.com (EDB3	DCet 1953)
Estimated time left:		Account	EDB%5Cat1953
Esumated une left:		Data	Dettetarikke Jan Fredrik Levers und
Attack rate:		Protocol	HTTPS
Current password:		Port	443
		Authentication Type	Default
Time Message		Access Group	apple
21:37:51 Starting EPPB		Path	/Microsoft-Server-ActiveSync
21:37:51 EPPB v. 1.45 r837 [PROFESSIONAL EDITION]			

-----

# **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/prwe b8470927.htm

# **Password Usability**

![](_page_54_Picture_1.jpeg)

# 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		
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

![](_page_58_Figure_1.jpeg)

## 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!

![](_page_64_Picture_1.jpeg)

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