

Report about **Stefan Lueders** presentation on

**CERN computer
security : Abuse Blunder
& Fun** (CERN 24 Nov 2014)



By **Elena Gianolio**

Slides credits : Stefan Lueders

There is no 100% security.

Hackers have time, knowledge and sometime money

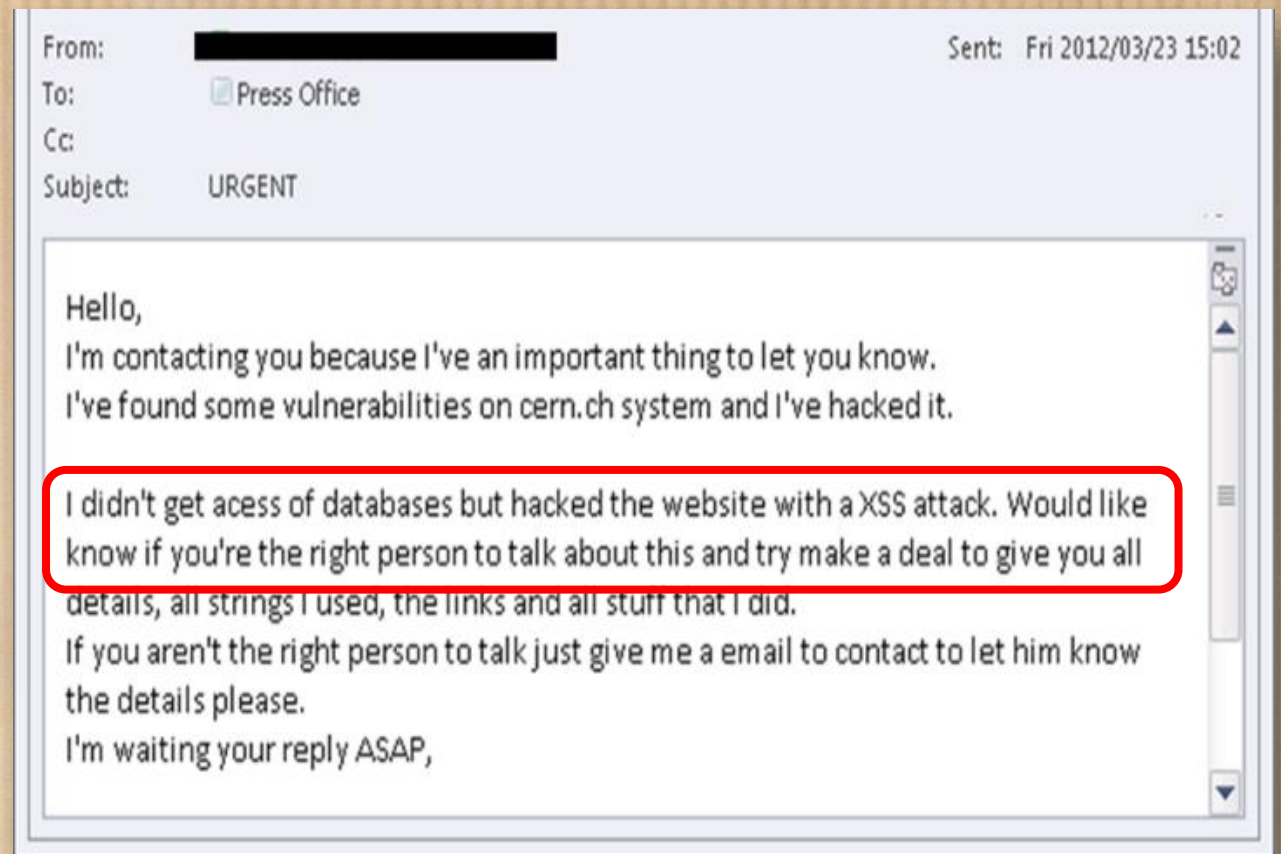
We (CERN) are target

PART 1: HACKING THE LARGE HADRON COLLIDER (XSS VULNERABILITY)

Published by camilla c. | Filed under [General, News, Spreadin'](#)

PART 2: HACKING THE LARGE HADRON COLLIDER (AUTHORIZATION BYPASS)

Published by camilla c. | Filed under [General, News](#)



```
<sc0rp> nice
```

```
<MLT> using the exploit on CERN would be win, hacking the people who created the internet :P
```

```
<sc0rp> haha
```

Mandate:

**Protect the operations and reputation
of CERN against cyber-threats**

Protect CERN/your assets

IN OUR MAILS

Date: Fri, 5 Sep 2008 15:53:42 -0700
From: Webmail IT Service <sandward@charterinternet.com>
Reply-To: webITService@live.com
To:
Subject: Important: Email Account Verification Update

Dear Staff/Student

This message is from the Webmail IT Service messaging center mail center due to an unusual activities identified in our email. Please verify your webmail account by confirming your Webmail identity.

In order to confirm your Web-Mail identity, you are to provide the following information:

Full Names:
Username/ID:
Password:
Domain Name:
Important

Please provide all these information completely and correctly.

We thank you for your prompt attention to this matter. Please verify your Webmail Account. We apologise for any inconvenience.

Regards,

From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal The way to send and receive money online

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

[Click here to verify your account](#)

If you choose to ignore our request, we will temporarily suspend your account. Please visit the following page as we try to verify your identity.

Thank you for using PayPal!

Please do not reply to this e-mail as it cannot be answered. For assistance, please contact your account and choose the "Help" page.

To receive email notifications in plain text instead of HTML, update your preferences [here](#).

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at [http://www.paypal.com/security](#)

[Click here to verify your account](#)

http://211.248.156.177/.PayPal/cgi-bin/webcmd_login.php



Wed 24/06/2015 14:09

Emilie M Bogart <Emilie.Bogart@jiscs.com>

RD78 Collaboration Meeting June 29/30 2015, Jones Institute, 1st announcement

To Stefan Lueders

i You replied to this message on 24/06/2015 15:07.

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Collaborator:

On the last meeting in Amsterdam we decided to have the next RD78 Collaboration meeting at Jones Institute. The date is now fixed (as we proposed in Amsterdam)

time:

Monday, June, 29. and Tuesday, June, 30. in 2015

location:

CERN, 1211 Geneva 23, Switzerland

For the Collaboration meeting you find the following information:

accomodation:

Do a reservation at the CERN hostel and send mail to Emilie.Bogart@jiscs.com or look into our web-page to find a list of other hostels in Geneva or France.

further information:

<http://RD78.JISCS.COM/RD78/RDCERN45252GL.PDF>

Please inform us, wheather you attend the meeting, and if you like to report a topic or want to have it discussed.

In case you are missing a colleague on this mailing list, please forward it and let us know about the missing address, to be included in the list in future.



Rechnung

Bestellnummer: MGFWF25VGX
Lfd. Nummer: 2-12674277
Bestellung gesamt: CHF 27.00
Rechnung an: Visa

Artikel	Interpret	Art	Preis pro Stück
(Justin Bieber)	NBC	Playlist	

Wenn sie nicht berechtigt diese Zahlung melden Sie dies bitte in den untenstehenden Link:

[Abbrechen Zahlungs](#)

Bitte bewahren Sie eine Kopie für Ihre Unterlagen auf.


Die Bedingungen und Konditionen, die an diese Bestellung geknüpft sind, finden Sie weiter unten.

iTunes S.à r.l.

Sie finden die Verkaufsbedingungen und Verkaufsrichtlinien, indem Sie Ihr iTunes-Programm starten und auf diesen Link klicken: [Verkaufsbedingungen](#)

Antworten auf häufige Fragen zum iTunes Store finden Sie hier:
<http://www.apple.com/chde/support/itunes/musicstore/>

Bestellung ge



Justin Bieber
Singer, songwriter · justinbiebermusic.com

Justin Drew Bieber is a Canadian singer and songwriter. Bieber released his debut EP, My World, in late 2009. It has been certified platinum in the United States. [Wikipedia](#)

Born: March 1, 1994 (age 21), London, Canada
Height: 1.75 m
Parents: Pattie Mallette, Jeremy Bieber

Songs

What Do You Mean?	2015	Purpose
Baby	2010	My Worlds
Boyfriend	2012	Believe
As Long As You Love Me	2012	Believe
Never Say Never	2010	My Worlds

Bestellnummer: MGFWF25VGX
Lfd. Nummer: 2-12674277
Bestellung gesamt: CHF 27.00
Rechnung an: Visa

<https://server44.abstractdns.com/~maxwellk/ch>

Artikel	Interpret
Justin Bieber	NBC

Wenn sie nicht berechtigt diese Zahlung melden Sie dies bitte in den untenstehenden Link:

[Abbrechen Zahlungs](#)

Bitte bewahren Sie eine Kopie für Ihre Unterlagen auf.

Die Bedingungen und Konditionen, die an diese Bestellung geknüpft sind, finden Sie weiter unten.

iTunes S.à r.l.

Sie finden die Verkaufsbedingungen und Verkaufsrichtlinien, indem Sie Ihr iTunes-Programm starten und auf diesen Link klicken: [Verkaufsbedingungen](#)

Antworten auf häufige Fragen zum iTunes Store finden Sie hier:
<http://www.apple.com/chde/support/itunes/musicstore/>

[Apple-ID - Übersicht](#) • [Einkaufsstatistik](#)

Apple respektiert Ihre Privatsphäre.
 Informationen zur Verwendung Ihrer persönlichen Daten erhalten Sie hier: <https://www.apple.com/privacy/>

server44.abstractdns.com
 Go to Google Home

All Images Videos Maps News More Search tools

About 196 results (0,43 seconds)

209.188.31.135 IP address information - VirusTotal
<https://www.virustotal.com/en/ip-address/209.188.31.../information/>
 4/65 2015-10-08 09:05:38 http://server44.abstractdns.com/~maxwellk/ch/4144a34700c44de2d5e92598a4464d0d. 5/65 2015-10-08 06:31:00 ...

server44.abstractdns.com - Dnslookup.fr
dnslookup.fr/server44.abstractdns.com
 Attention, il y a 8 ports ouverts : 21/tcp open ftp; 25/tcp open smtp; 53/tcp open domain; 80/tcp open http; 110/tcp open pop3; 143/tcp open imap; 443/tcp open ...

Server44.abstractdns.com - SimilarWeb
www.similarweb.com/website/server44.abstractdns.com
 Server44.abstractdns.com ranking is 0 in the world for Unknown. Get their full traffic statistics with SimilarWeb and uncover their online marketing strategy.

server44.abstractdns.com at WI. Default Web Site Page
website.informer.com/server44.abstractdns.com
 Oct 28, 2015 - server44.abstractdns.com information at Website Informer. Default Web Site Page.

server44.abstractdns.com - Robtex
www.robtx.com/dns/com/abstractdns
 What IP addresses does server44.abstractdns.com use? Server44.abstractdns.com uses the two IP addresses 209.188.24.194 and 209.188.31.135 together ...

PhishTank > Details on suspected phish #3270683
https://www.phishtank.com/phish_detail.php?phish_id=3270683
 Submitted Jun 20th 2015 8:03 AM by GovCERTCH (Current time: Oct 21st 2015 10:28 AM UTC). <https://server44.abstractdns.com/~maxwellk/ch/> ...

server44.abstractdns.com | WOT Reputation Scorecard ...
<https://www.mywot.com/en/scorecard/server44.abstractdns.com>

CONFERENCES !!

"Dear LP2015 conference organ...

I am a registered speaker to
collaboration.

I just received a phone call
inviting me to book an hotel
(given below) instead of the re
the conference web page. [...]"



https://cern.service-now.com/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id= - Internet Explorer - [InP...
InPrivate https://cern.service-now.com/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=37c73964a08d4a406d21ed5d48

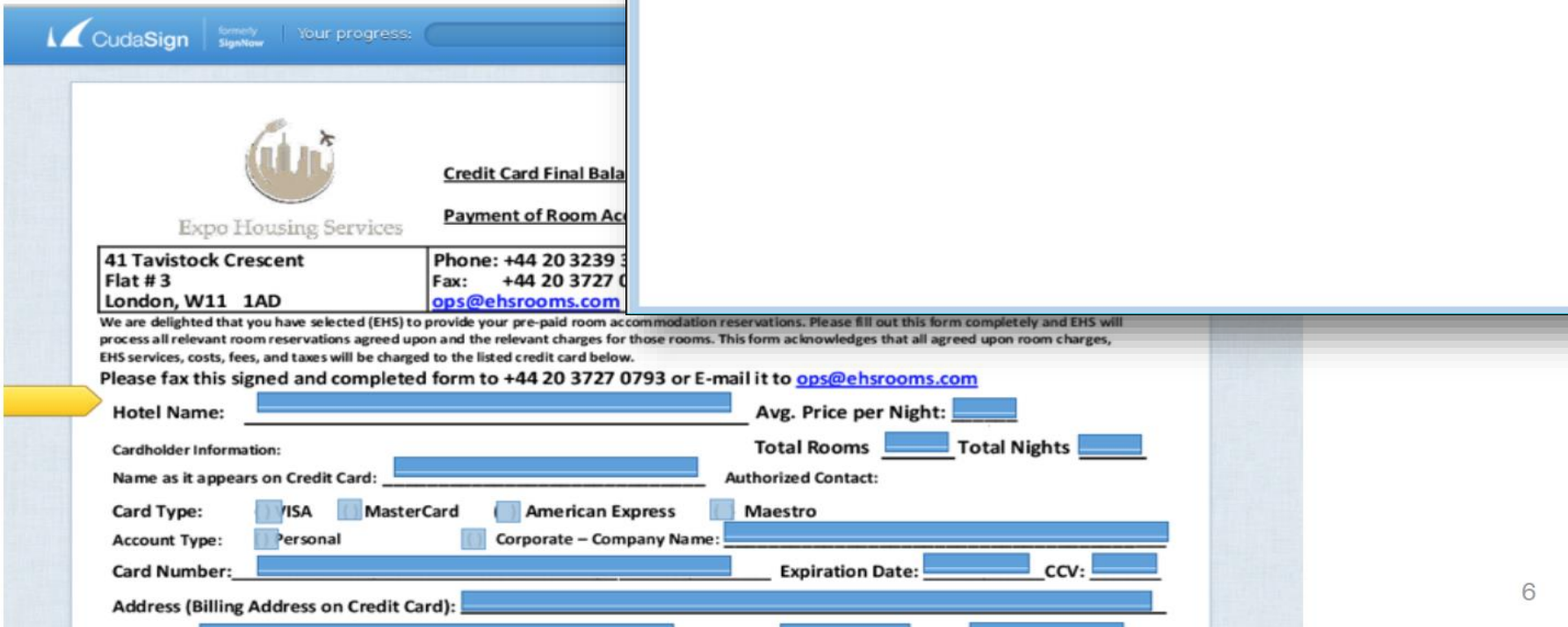
From: <[REDACTED]>
Subject: LP2015 URGENT!!!
Date: 1 Jul 2015 09:22:14 GMT+2
To: <[REDACTED]@cern.ch>

Dear participant of LPH2015 conference

Thanks for registering. We have been warned that there are possible phishing attacks to registrants of the conference. Participants are called by fake representative of the conference and invited to book a hotel directly from a certain web page instead of the recommended reservation from the conference web page. This web page asks to send credit card info through the web interface.

Please do not use this service since this is obviously an attempt to steal your data

Regards
[REDACTED]
for the LP2015 Local Organizing Committee



CudaSign Your progress: [Progress Bar]

Expo Housing Services

41 Tavistock Crescent
Flat # 3
London, W11 1AD

Phone: +44 20 3239 3...
Fax: +44 20 3727 0...
ops@ehsrooms.com

Credit Card Final Balance
Payment of Room Accommodation

We are delighted that you have selected (EHS) to provide your pre-paid room accommodation reservations. Please fill out this form completely and EHS will process all relevant room reservations agreed upon and the relevant charges for those rooms. This form acknowledges that all agreed upon room charges, EHS services, costs, fees, and taxes will be charged to the listed credit card below.

Please fax this signed and completed form to +44 20 3727 0793 or E-mail it to ops@ehsrooms.com

Hotel Name: [REDACTED] Avg. Price per Night: [REDACTED]

Cardholder Information: [REDACTED] Total Rooms [REDACTED] Total Nights [REDACTED]

Name as it appears on Credit Card: [REDACTED] Authorized Contact: [REDACTED]

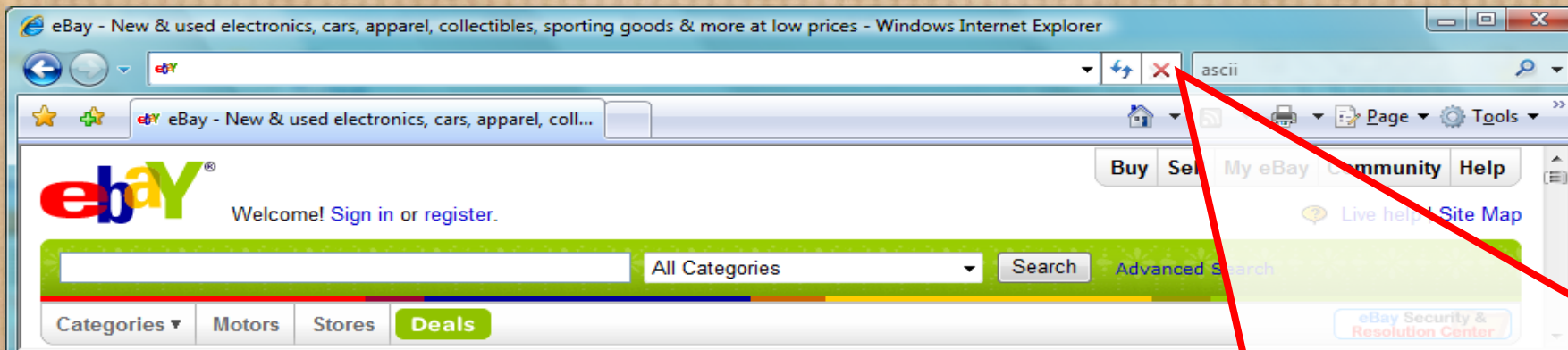
Card Type: VISA MasterCard American Express Maestro

Account Type: Personal Corporate - Company Name: [REDACTED]

Card Number: [REDACTED] Expiration Date: [REDACTED] CCV: [REDACTED]

Address (Billing Address on Credit Card): [REDACTED]

6



Quiz: Which URL leads you to www.ebay.com ?

- ✘ ▶ <http://www.ebay.com/cgi-bin/login?ds=1%204324@%31%33%37%2e%31%33%38%2e%31%33%37%2e%31%37%37/p?uh3f223d>
- ✘ ▶ <http://www.ebay.com/ws/eBayISAPI.dll?SignIn>
- ✔ ▶ http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&rafId=0&encRafId=default
- ✘ ▶ <http://secure-ebay.com>

Why they attach us ?

- **Get informations about us**
- **Get our contacts**
- **Infect our machine**
- **Money extortion (private data encryption)**
- **Join BootNet to attack other system on the Internet**
- **FUN**

Consequences of attacks

- **Send SPAM**
- **Infect other machines on the local network**
- **Host illegal data (software, movies, private data)**
- **Relay confidential work**

free network connection

public machine



<https://medium.com/matter/heres-why-public-wifi-is-a-public-health-hazard-dd5b8dcb55e6#.ntqekzmv7>

We took a hacker to a café and,
in 20 minutes,
he knew where everyone else was born,
what schools they attended,
and the last five things they googled.

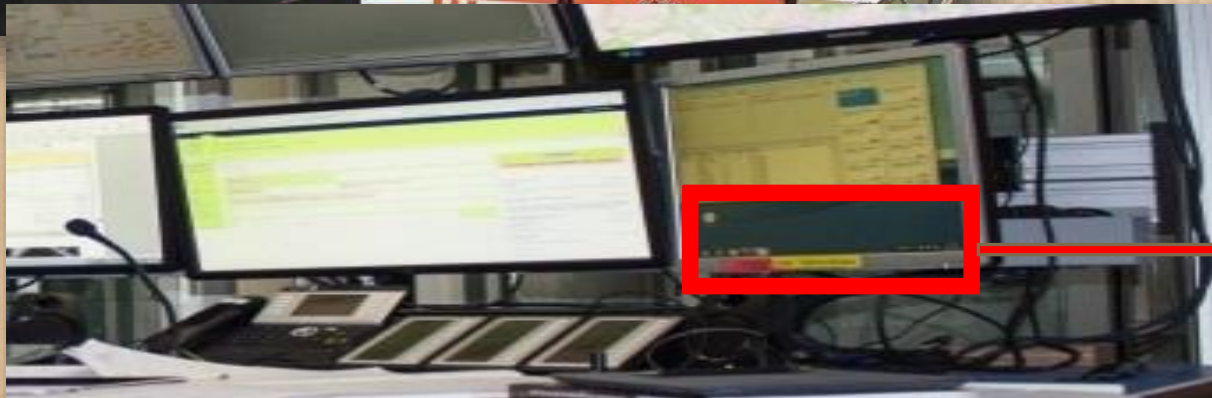
By Maurits Martijn, from *De Correspondent*,
Translated from Dutch by Jona Meijers

Everything, with very few exceptions, can be cracked.

Slotboom's device is capable of registering these searches and appearing as that trusted WiFi network. I suddenly see the name of my home network appear on my iPhone's list of available networks, as well as my workplace, and a list of cafes, hotel lobbies, trains, and other public places I've visited. My phone automatically connects itself to one of these networks, which all belong to the black device.

After Slotboom is connected, he is able to provide all the visitors with an internet connection and to redirect all internet traffic through his little device.

Oooopppsss



CERN Bulletin News Articles Official News Training Announcements Events Staff Association

english | français

Issue No. 20-21/2014 - Monday 12 May 2014
No printable version available - Subscribe: [icon] [icon]



Polarisation confirmed
Celebrating with our neighbours
LSi Report: PS Booster prepares for beam
From the drawing board to the test bench
Data defenders
The "Karma Level Sexy Bottom" awards are back at CERN
Winter Atomiades 2014: CERN skiers win 31 medals!

BEHIND THE SCENES OF GS: NOTHING LEFT TO CHANCE

The AS (Alarm Systems) Section in the GS-ASE Group is, as its name suggests, in charge of the various alarm systems spread across CERN's many sites. Its mission? To install, manage and maintain more than 26,000 alarms of all types located both above ground and in the tunnels.

Detection
Among these systems, the best known are of course the heat and/or smoke detectors, which quickly raise the alarm in the event of a fire. CERN has 8500 of these devices in total. In combination with these, evacuation alarms are also found all over the which is then connected to a transmission unit. From here, the information – for example, which type of alarm has been activated in which building – is transmitted to the Fire Brigade's Safety Control Room (SCR) and to the CERN Control Centre (CCC). "The information is transferred via two channels," explains Henrik Nissen. "The first channel is a basic electrical (wire) network which, by its very nature, ensures a very high level of reliability. The second channel is a computer network which, although it allows more precise information to be transferred, is not as reliable as the first." All of the alarms essential for the safety of people and equipment (level 3 alarms), as well as vital technical alarms (for cryogenics, for example) always use both channels. This redundancy ensures that the information is transmitted whatever happens.

On the maintenance side, each of the 11,000 level 3 alarms is tested every year. This is a mammoth task which requires the expertise of seven people working full time in close cooperation with CERN's Fire Brigade.



Test platform for detecting gas (including ODH). The bottles at the bottom of the image contain different types of gas used for tests.

The Fire Brigade's Safety Control Room, which receives level 3 alarms.

Mandate:

**Protect the operations and reputation
of CERN against cyber-threats**

Protect CERN's reputation

The image shows a screenshot of the Ashley Madison website. The browser address bar displays "http://www.ashleymadison.com/". The website header includes the Ashley Madison logo and the tagline "Life is short. Have an affair.®". A registration form prompts users to "Get started by telling us your relationship status:" with a dropdown menu set to "Please Select" and a "See Your Matches" button. Below the form, it states "Voted the World's #1 Sex Personals with over 39.050.000 members." and "Join FREE! Meet people looking to FUCK tonight!".

Overlaid on the right side of the screenshot is a blue box containing a list of email addresses categorized under "Institutions (basées en Suisse)". The list includes:

- 6 adresses du CERN (@cern.ch)
- 20 adresses (au moins) des Nations Unies (@un.org)
- 11 adresses UNIL (@unil.ch)
- 2 adresses UNIGE (@unige.ch)
- 5 adresses de l'EPFL (@epfl.ch)
- 7 adresses de l'ETHZ (@ethz.ch)
- 1 adresse de la RTS (@rts.ch)

The "6 adresses du CERN (@cern.ch)" entry is highlighted with a red rectangle. The RTS INFO logo is visible in the top right corner of the blue box, and a notification bubble with the number "49" is in the bottom right corner.

...any professional duties here ?

LE FIGARO

ZDNet Government
 Richard Koman

Get ZDNet Government via: [Mobile](#) [RSS](#) [Email Alerts](#)

Pick a blog category

September 12th, 2008

Hackers deface LHC site, came

Le site du Cern piraté

Source : AP
 13/09/2008 | Mise à jour

CyberInsecure.com
 Daily Cyber Threats And Internet Security News: Network Security, Online Safety A

HOME ARCHIVES CONTACT ABOUT EMAIL SUBSCRIBE ADVERTISE

September 13th, 2008

Hackers Attack Large Hadron Collider Network At CERN, Leaving A Message For System Administrators

Hackers have attacked the network of Large Hadron Collider and mocked the IT used on the project, describing the technicians responsible for security as "a bunch of schoolkids." The hackers said they had no intention of disrupting the work of CERN. The website, www.cmsmon.cern.ch, can no longer be accessed by the public as a result of the attack.



SPiegel ONLINE

NACHRICHTEN VIDEO

Home | Politik | Wirtschaft

Nachrichten > Wissenschaft

13.09.2008 Drucken | Se

Telegraph.co.uk

Home News Sport Business Travel Jobs Motoring Telegraph TV

Earth home Earth news Earth watch Comment

Hackers infiltrate Large Hadron Collider systems and mock IT security

News Site of the Year | The 2008 Newspaper Awards

heise online

Home Newsticker 7-Tage-News News-A

heise online > News > 2008 > KW 37 > Webs

12.09.2008 21:26

Webseite des neuen Teilchenbeschleunigers gehackt

TIMES ONLINE

NEWS COMMENT BUSINESS MONEY SPORT LIFE & STYLE TRAVEL DRIVING

UK NEWS WORLD NEWS POLITICS ENVIRONMENT WEATHER TECH & WEB TIMES ONL

Where am I? Home News UK News Science News

From The Times
 September 13, 2008

Hackers break into CERN computer – to show up its ‘schoolkid’ security

SecurityFocus™

IRONKEY THE WORLD'S MOST SECURE FLASH DRIVE

Home Bugtraq Vulnerabilities Mailing Lists Jobs Tools Vista

News
 Infocus
 Foundations
 Microsoft
 Unix

PRINT EMAIL

Hackers defaced collider site, say reports
 Published: 2008-09-12

Mandate:

**Protect the operations and reputation
of CERN against cyber-threats**

Protect CERN's operations

Register FAQ Memberlist Usergroup

Need urgent help with 4.7K DES

New Topic Post Reply InsidePro Software Forum Index -> Unix

Author

dannote
Joined: 18 Jun 2012
Posts: 2
Reputation: 0

Posted: Mon Jun 18, 2012 3:02 am Post subject: Unfortunately, I have very low computer power
<http://pastebin.com/KUEqjxx7>
Thank you!

Back to top Profile PM

dannote
Joined: 18 Jun 2012
Posts: 2
Reputation: 0

Posted: Mon Jun 18, 2012 3:09 am Post subject: Here are 306 found.

Description:	
Filename:	found.txt
Filesize:	5.39 KB
Downloaded:	24 Time(s)

Back to top Profile PM

Display posts from previous

New Topic Post Reply InsidePro Software Forum Index -> Unix

Page 1 of 1

Powered by phpBB © 2001, 2002 phpBB Group

Description:	Left	0 Download
Filename:	dannote4kdes.hash.txt	
Filesize:	45.43 KB	
Downloaded:	15 Time(s)	

Back to top Profile PM

Posted: Tue Jun 19, 2012 8:18 am Post subject: 231 More from the M@LIK left (in pass format)

left.txt		
Description:		0 Download
Filename:	left.txt	
Filesize:	42.27 KB	
Downloaded:	6 Time(s)	

231.txt		
Description:		0 Download
Filename:	231.txt	
Filesize:	1.95 KB	
Downloaded:	8 Time(s)	

Back to top Profile PM

Posted: Tue Jun 19, 2012 9:38 am Post subject: Just a ~2 min attack (with my own wordlist)


Found: 42

KJaWJnd08IpCw:Opera123
2HTRyRgLsDREY:1234%^&*gX1ZsHfMI3Ho:1891Ikap

You cannot delete your posts in this forum
You cannot vote in polls in this forum
You cannot attach files in this forum
You can download files in this forum

Our Phone Book Form (xwho service). - Windows Internet Explorer
ern.ch/xwho/people?<script>alert("This_is_prone_to_cross_site_scripting_(XSS)")</script>

Windows Internet Explorer



This_is_prone_to_cross_site_scripting_(XSS)

<script>alert("This is prone to cross site scripting (XSS)")</script>

Phone book related search terms

Family Name:

Firstname: ([more about search v](#))

Phone number:

Department: CERN group:

Building: Floor-Office:

CERN Accelerating science Sign in Directory

CERN Phonebook

Support | Help | v2.0.1

This<i> is</i> <u>BAD</u>, I suppose.

Advanced Search

Your search **This is BAD, I suppose.** did not match any person or service.

- Check if the searched person appears in the suggestion drop-down list and if yes select it directly.
- Try to refine your search by either using wild cards(**This * is* BAD,* I* suppose.***)
- Sometimes being less specific (reduce the number of searched words and/or characters) can also help finding a person or service.
- Please consider looking at the [Phonebook Help](#) for further details.

100%

Respect Credits and copyrights

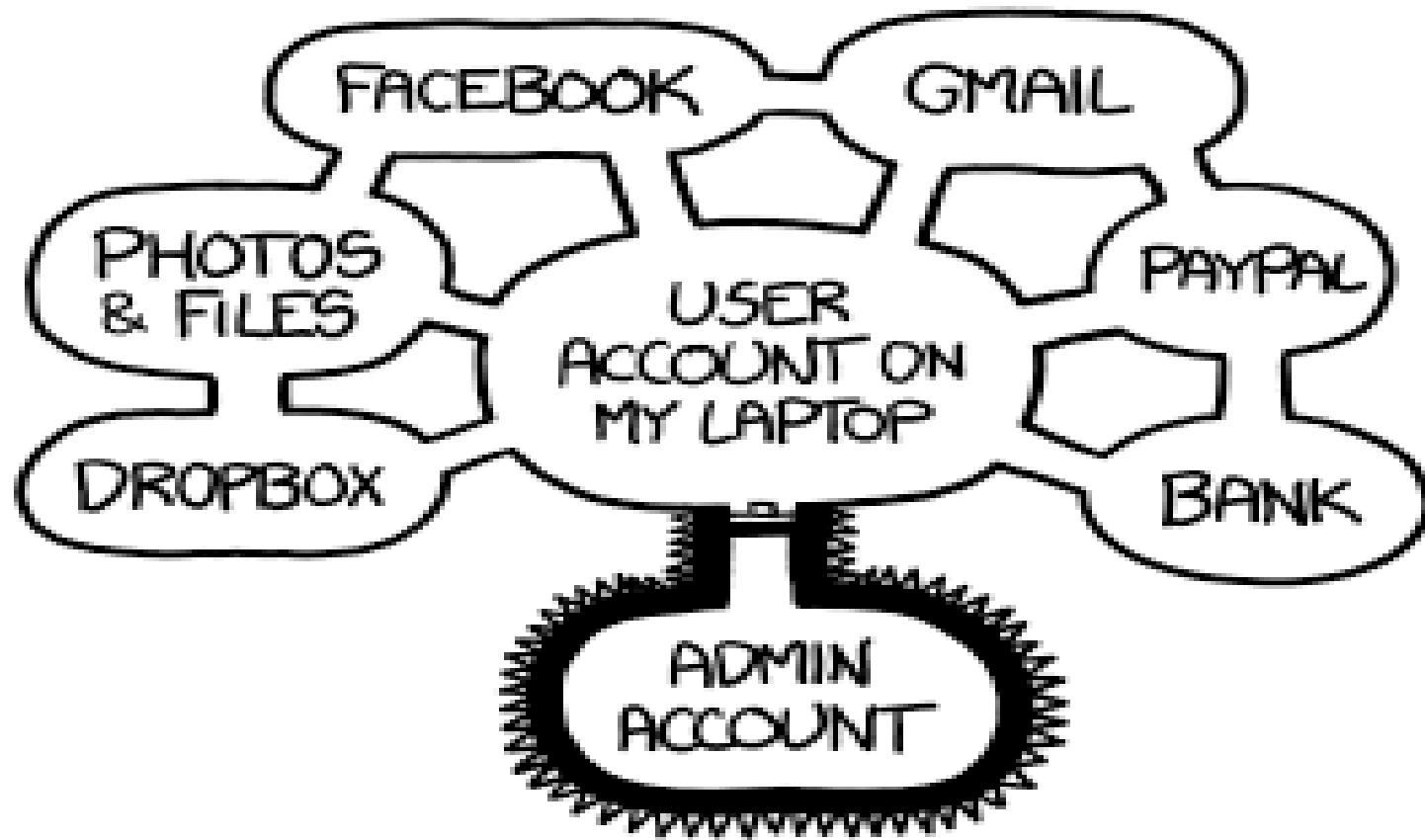
- Images and photos
- Official Documents or assertions
- Programs : respect the license terms



Someone at Cern said this: "We have recorded several videos in advance and it was a mistake that this one went live. We pre-recorded interviews with spokesmen from both experiments [CMS and Atlas] but this went live on the internet due to a technical fault."

What we can do ?

- With (academic) freedom at home and at CERN:
we are responsible for securing our assets
- Choose well our password and protect them Don't use the same
- Keep our devices up-to-date. Install anti-virus software. About less
then 4 minutes a robot scan IPs and send attacks
- Use existing services!
- Respect the rules!
- **Stop! — Think! — Click...? Or maybe not ☺**



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,
BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.



- Home
 - Computing Rules
 - Recommendations
 - Training
 - Services
 - Reports & Presentations
- Vous préférez le français ?
- Emergency Response**
- What to do in an emergency
- Contact**
- How to contact the Computer Security Team
 - Departmental & experiment contacts
- About CERN Computer Security**
- A word from the DG
 - Security is not complete without you

Computer security emergency contact
✉ **Computer.Security@cern.ch** ☎ **70500**
Contact en cas d'incident de sécurité informatique

<http://cern.ch/security>

CERN Accelerating science

Sign In Directory

News Articles Official News Learning Announcements Events Staff Association

english | français

Issue No. 47-48/2015 - Monday 16 November 2015
No printable version available - Subscribe

CERN Bulletin

Of vacuum and gas

COMPUTER SECURITY: CONFIDENTIALITY IS EVERYBODY'S BUSINESS

... was mistakenly made public on one of...
... led for members of an internal...
... someone made a mistake when...
... file accessible to everyone visiting

... minately, this is but one example of...
... mistakes. We have seen other...
... nents made accessible to a much wider...
... quence than originally intended...

... confidentiality is everybody's...
... business

Ombud's Corner: sexual harassment
- who is concerned?

Subscribe by RSS

Subscribe by RSS for this category only

CERN takes serious measures to ensure the confidentiality of data. Confidential or "sensitive" documents (following the nomenclature set out in the CERN Data Protection Policy) deserve professional handling and access protections given only to the people who really need to access them. As such, they must not be widely circulated as attachments in e-mails and, most definitely, must not be stored on random public websites for the sole purpose of sharing them. Instead, these documents should reside in their original storage location (like AFS, Alfresco, CDS, DFS, EDMS, INDICO, Sharepoint) and the corresponding access controls should be adapted so that all people who need access are granted it and everyone else's access is blocked.

The level of protection is clearly marked in EDMS ("Public access", "Restricted access") and INDICO ("public", "restricted" or edit the event and check the "Protection" tab). For AFS and DFS, instructions for properly protecting files can be found here and here.

CTA: mail and web security

Software packages : mail and web security

<http://cds.cern.ch/record/1454932>

You can name her whatever you like but be sure it's something you can remember. You'll be using it as a security question answer for the rest of your life.



© 2012
P. ODEN
BIZARRO
9-27-12