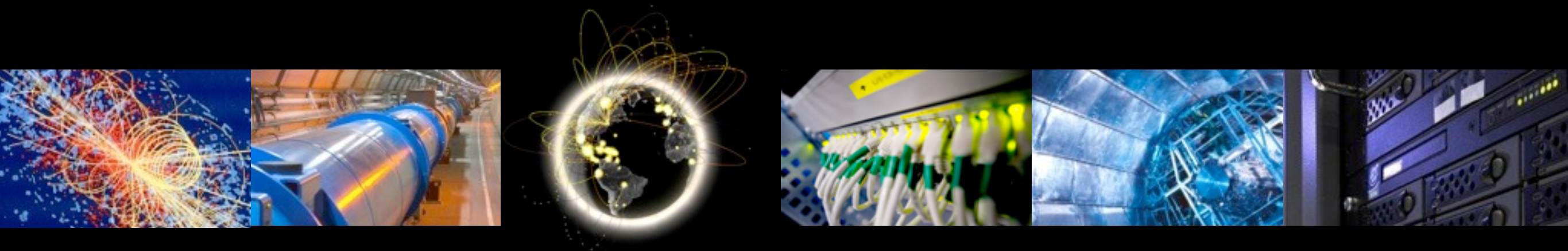


Be a lot safer and prepared in 6 steps

HEPiX Fall 2013 Meeting, Ann Arbor, R. Wartel





Motivation

- HEP sites often have a large and distributed community
- Monitoring pre-intrusion is very costly and rarely works
 - Typically: direct SSH login with a valid user account
- Root escalation is extremely difficult to prevent
- Many heterogenous services with direct Internet access
- The attack surface is very large
- Yet, it is possible to significantly reduce your chances of disaster in 6 steps!





Once they're in...

- There are always compromised user accounts
- Make root escalation slightly more difficult
 - Keep up-to-date with security patches from your vendors
 - Many “basic” incidents could be prevented
- However:
 - Decent attackers come with 0-days or private exploits
 - A number of attacker do not need root privileges
- Eventually, motivated or patient attackers will get root
 - “Game over”
 - Disable LKM loading on runtime to break a number of rootkits
 - Run “rpmverify” to detect a number of user space rootkits



Traceability

- How did they get root?
 - Via a valid user used in conjunction with a 0-day
 - Via stolen admin credentials (SSH) from infected Windows desktops
 - etc.
- It may take a while (months/years) before the compromise is discovered
- **Traceability** then becomes the most important asset
 - Essential to understand how the compromised occurred
 - Else, containing and fully resolving the incident is impossible
 - ...and the attacker will almost immediately come back



What data will you need?

- Keep all your (sys)logs, untampered if possible
 - Use remote syslog and safely archive your logs for a long time
 - There are probably legal requirements
 - Storing is easy, data mining is difficult
 - Some important services don't use syslog (e.g. Apache)
 - Make sure the data is accessible only by appropriate staff!
- Keep a record of user actions
 - Keep shell history, including commands and options
 - Accounting information is insufficient (often, argv is missing)
 - e.g. <https://github.com/a2o/snoopy/releases> (Snoopy, LD Preload)
- Keep a detailed record of network traffic
 - Match network traffic with a PID/UID
 - Netlog: <https://github.com/CERN-CERT/netlog>
 - Auditd can also be a good alternative
 - `iptables -I OUTPUT -p tcp -m tcp --sport 22 --tcp-flags SYN,ACK SYN,ACK -j LOG --log-prefix newtcp-out: --log-uid --log-level debug`

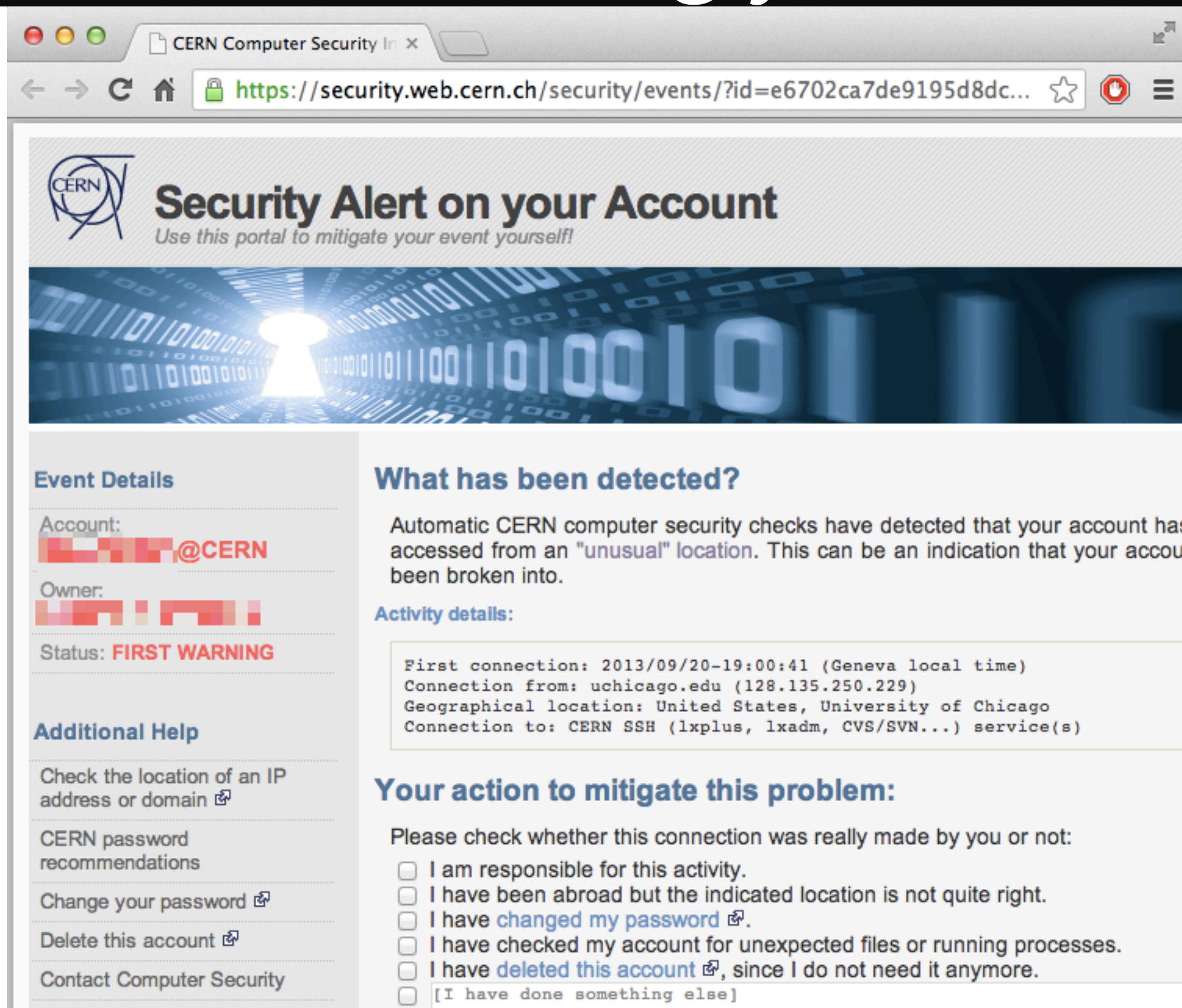


Summary

- How to be a lot safer and prepared?
 - Keep up-to-date with security patches
 - Disable LKM loading on runtime
 - Use “rpmverify” or any package integrity verification tool
 - Use remote syslog and safely archive your logs
 - Keep shell history, including commands and options
 - Match network traffic with a PID/UID
- Know your limits. If you don't have the expertise:
 - Call the experts! Liaise with other security teams/groups
 - Otherwise in all likelihood the attacker will come back shortly
 - Someone probably has precious intel to share
 - Stand-alone incidents are history



Crowd-sourcing your IDS



The screenshot shows a web browser window with the address bar displaying <https://security.web.cern.ch/security/events/?id=e6702ca7de9195d8dc...>. The page title is "Security Alert on your Account" with the subtitle "Use this portal to mitigate your event yourself!". The main header features a CERN logo and a background image of binary code with a glowing keyhole. The page is divided into several sections:

- Event Details:**
 - Account: [redacted]@CERN
 - Owner: [redacted]
 - Status: **FIRST WARNING**
- Additional Help:**
 - Check the location of an IP address or domain
 - CERN password recommendations
 - Change your password
 - Delete this account
 - Contact Computer Security
- What has been detected?:**

Automatic CERN computer security checks have detected that your account has accessed from an "unusual" location. This can be an indication that your account has been broken into.
- Activity details:**

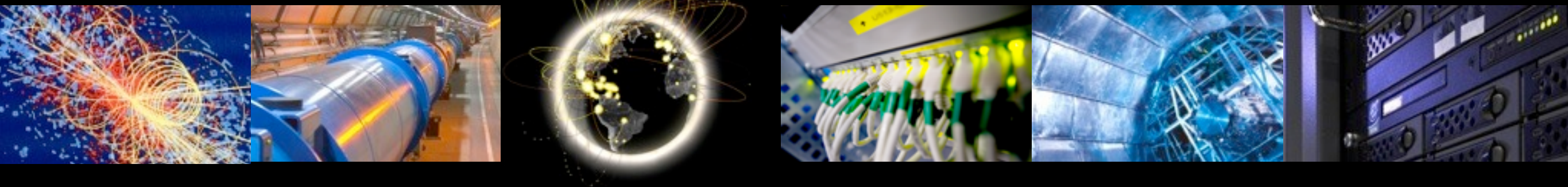
First connection: 2013/09/20-19:00:41 (Geneva local time)
Connection from: uchicago.edu (128.135.250.229)
Geographical location: United States, University of Chicago
Connection to: CERN SSH (lxplus, lxadm, CVS/SVN...) service(s)
- Your action to mitigate this problem:**

Please check whether this connection was really made by you or not:

 - ☐ I am responsible for this activity.
 - ☐ I have been abroad but the indicated location is not quite right.
 - ☐ I have **changed my password**.
 - ☐ I have checked my account for unexpected files or running processes.
 - ☐ I have **deleted this account**, since I do not need it anymore.
 - ☐ [I have done something else]

<https://security.web.cern.ch/security/services/en/receipts.shtml>

Questions?





Home

Products

Resellers

Affiliates

Order Tracking

Renewals

Payments

Support

Switch to Trustico®

Contact Us

Order Now

Our Ordering System
Is Fully Automated
**Get Your SSL Certificate
Within Minutes**



Are You
New To
**Online
Security?**

[Click Here To Get Started](#)

Why Should I Choose Trustico?



- » 7 Day Money Back Guarantee
- » All Certificates Work Globally
- » VeriSign® Platinum Partner
- » We'll Match Competitor Prices
- » Automated Ordering System
- » We Don't Require A CSR
- » 24 Hour Sales & Support
- » Wide Range Of SSL Products
- » Reseller Program Available

[View Even More Reasons](#)

Which SSL Certificate? SSL Product Wizard

Find The Best
SSL Certificate
For Your Website
With Our



Certificate Key Matcher

You can use this Certificate Key Matcher to check whether a private key matches a certificate. When you are dealing with lots of different certificates it can be easy to lose track of which certificate goes with which private key was used to generate which certificate. The Certificate Key Matcher tool makes it easy to determine whether a private key matches a certificate.

Paste your **CERTIFICATE** here

Paste your **PRIVATE KEY** here

[Chat Now](#)



Check if your CSR and Private Key match

GlobeSSL
in SSL we trust

Manage SSL Verify SSL CSR Decoder AutoCSR Convert SSL **Key Matcher**

What to Check

- ☒ Check if a Certificate and a Private Key match
- ☐ Check if a Certificate and CSR match

Certificate Text ⓘ

GlobeSSL
trusted & secure
Extended Validation



[IIS 7](#)

[How to Create A Self Signed Certificate](#)

[More Discussion About How Firefox 3 Handles SSL Certificates](#)

SSL Quick Search

- [Cheap SSL Certificates](#)
- [Cheapest Unchained Certificates](#)
- [Cheapest EV Certificates](#)
- [UC Certificates](#)
- [Special Deals](#)
- [Best SSL Wildcard Certificates](#)
- [Code Signing Certificates](#)

Your private key is intended to remain on the server. While we try to make this process as secure as possible by using SSL to encrypt the key when it is sent to the server, for complete security, we recommend that you manually check the modulus of the private key on your server using the OpenSSL commands above.

What to Check

☒ Check if a Certificate and a Private Key match

☐ Check if a CSR and a Certificate match

Enter your Certificate:

Enter your Private Key:

Results will be displayed here after both boxes are filled.

Your private key is intended to remain on the server. While we try to make this process as secure as possible by using SSL to encrypt the key when it is sent to the server, for



Trade without Bureaucracy™

Login Create Account iG

About iGolder

Buy Gold

Sell Gold

Join Now!

Contact

Home

PGP Decryption Tool

Related
[PGP Fre](#)
[PGP Ke](#)
[PGP En](#)
[PGP En](#)

This tool is simple to use: enter your private PGP key, your PGP passphrase, and the PGP-encrypted message you wish to decrypt, then click on the **Decrypt Message** button. If you supply the proper PRP private key and passphrase/password, then you will be able to read the decrypted message, otherwise you will see an error message the tool is unable to decrypt the message.

iGolder respects your privacy and does not log nor monitors any activity (decryption) done on this web page.

PGP Private Key (paste your private key - you also need to supply your PGP passphrase to unlock your private key)

PGP-Key Password / Passphrase:



PGP-Encrypted Message (paste the PGP-encrypted message you received)

Decrypt Message

Decrypted Message

