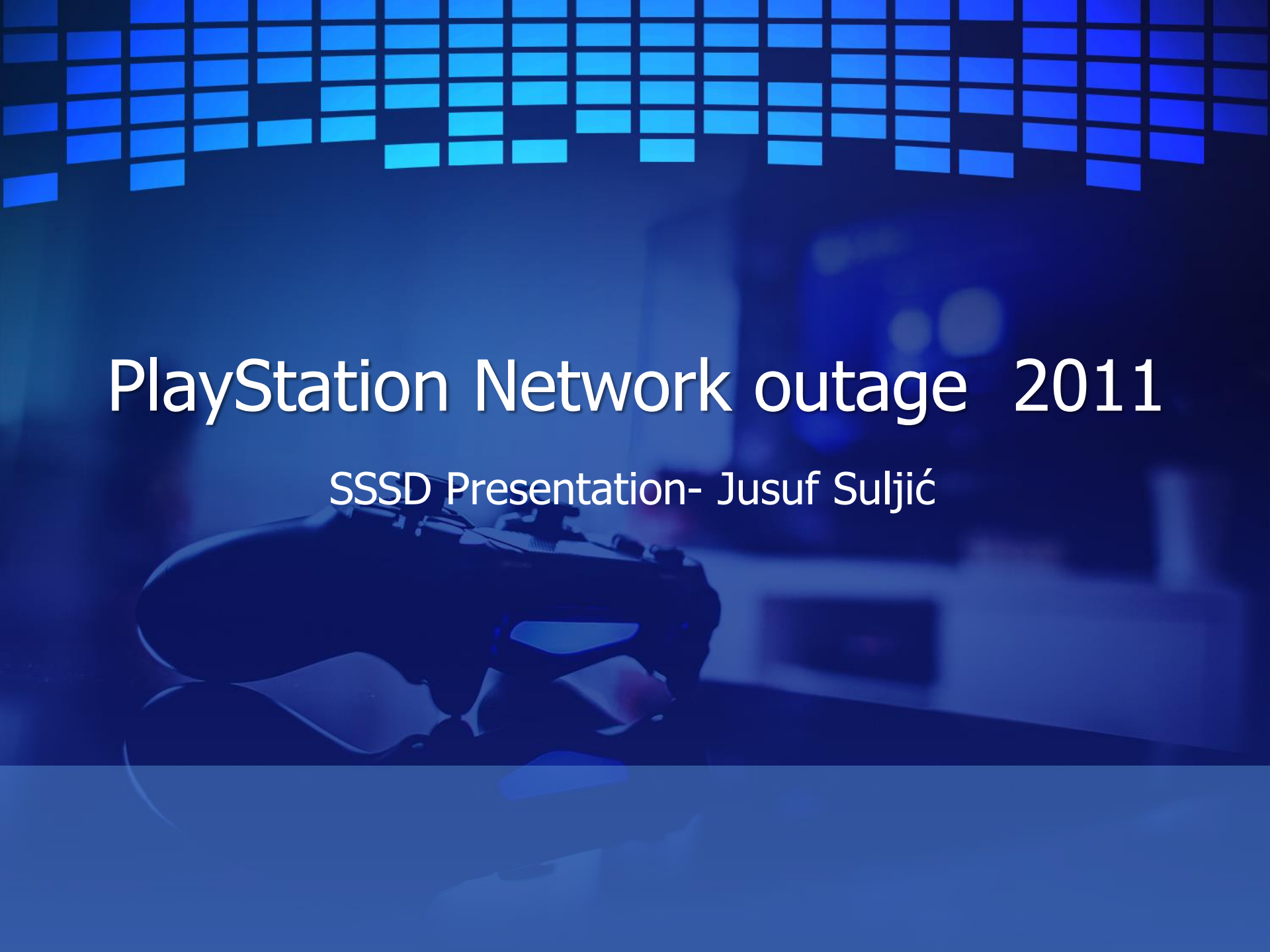
PlayStation Network outage 2011

SSSD Presentation- Jusuf Suljić



Background

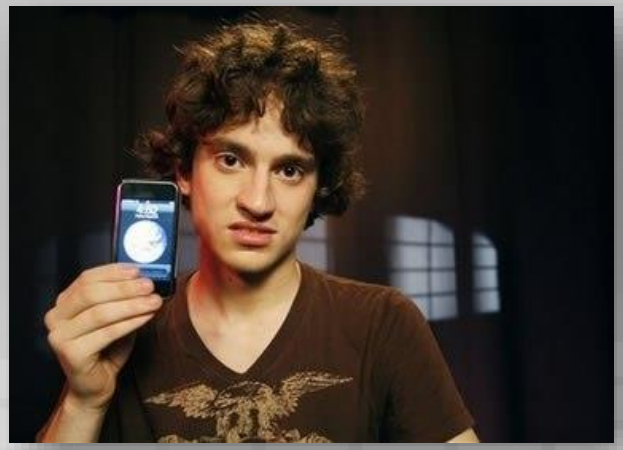
- On April 20, 2011, Sony acknowledged that it was "aware certain functions of the PlayStation Network" **were down**. Upon attempting to sign in via the PlayStation 3, users received a message indicating that the network was "undergoing maintenance".
- The company later announced an "**external intrusion**" had affected the PlayStation Network and Qriocity services.
- This **security breach** resulted in compromising personal information (emails, passwords, credit card numbers and etc.) of around **77 million PSN users worldwide** and it counts today as one of the biggest digital data security breaches in history.

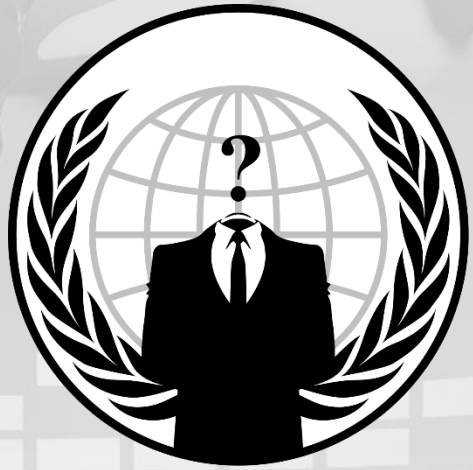
Qriocity

The exposure

The exposure

- This intrusion occurred between April 17 and April 19. On April 20, Sony suspended all PlayStation Network and Qriocity services worldwide.
- On May 3rd, Sony Computer Entertainment CEO Kazuo Hirao claimed that Sony systems were under attack for the past month and half ("**geohot's**" root keys, "**Anonymous**" DDoS attacks), suggesting that hackers were targeting Sony for a long time.
- The outage lasted for **23 days**.



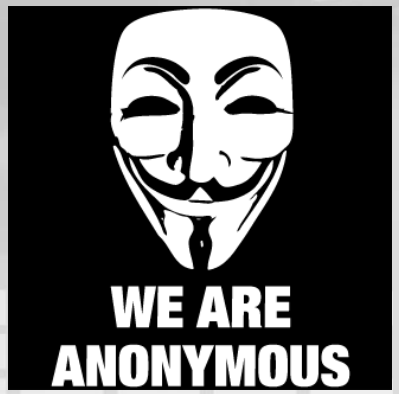


Who could have done it?

Possible Anonymous involvement

- Earlier in April, the decentralized hacker group called "**Anonymous**", publicly stated that they are planning to "protect the freedom of knowledge", meaning that all hacks are meant to punish Sony for taking actions against hackers like "**geohot**".

"Anonymous is on your side, standing up for your rights. We are not aiming to attack customers of Sony. This attack is **aimed solely at Sony**, and we will try our best not to affect the gamers, as this would defeat the purpose of our actions. If we did inconvenience users, please know that this was **not our goal**".



Known issue

- The **vulnerability** through which the data has been compromised, was actually **well-known** in the PS hacking community.
- On May 1st, Sony holds a conference on which they apologize for the inconveniences, announce "welcome back" gifts for users, and clarify that their systems **3-layered security was breached** because of a **known** vulnerability.
- They also explain that there is no evidence that the credit card info, which was encrypted, was stolen. And bank bureaus confirmed there were no suspicious transactions after the incident.
- Forensic evidence also suggested that all personal data was queried from the **account database**, meaning the database security was compromised (possibly via **SQL injection**, but nothing official was posted).

Unencrypted personal details

- Credit card data was encrypted, but Sony admitted that other user information was not encrypted at the time of the intrusion.
- On May 2nd, Sony clarified the "**unencrypted**" status of users' passwords, stating that:

"While the passwords that were stored were not "**encrypted**," they were transformed using a cryptographic hash function. There is a difference between these two types of security measures which is why we said the passwords had not been encrypted. But I want to be very clear that the passwords were not stored in our database in cleartext form."

Another breach

- On May 3rd, Sony stated in a press release that there may be a correlation between the **attack** that had occurred on April 16th towards the PlayStation Network and one that compromised **Sony Online Entertainment** on May 2nd .
- This portion of the attack resulted in the theft of information on **24.6 million** Sony Online Entertainment account holders.
- Sony was heavily criticized by organizations that were calling this breach "difficult to excuse" and "an act of simply gross incompetence".

Sony
Interactive
Entertainment

What are the consequences?

Consequences

- Sony was “slammed” by lawsuits:
  - **Canada - $1 billion** - "If you can't trust a huge multi-national corporation like Sony to protect your private information, who can you trust?” [5]
  - **UK - £250,000 -** penalty for putting large amounts of data at risk.
- In return, Sony had to offer an **Identity Theft Insurance Policy** of **$1 million** to already registered users.
- The fact that PSN was offline for 23 days, brings up the idea of how much revenue did Sony lose along with the game development companies that they partnered with.
- Money aside, Sony had lost the **trust** of its dedicated users, making them second guess any attempts at accessing the platform.

Solutions to prevent these problems

- **Prevent** intentional or unintentional **disclosure of sensitive data** at rest, in use or in motion to authorized parties.
- Maintain adequate **security** and provide **usability**.
- **Protect** customer data and brand reputation.
- **Protect** personally identifiable information and intellectual property.

Technical measures

01 **Endpoint security**

Restrict access to local admin functions.

02 **Host encryption**

Ensure disks and data are encrypted on all servers, workstations, laptops and mobile devices.

03 **Software upgrade**

Regularly update the software firmware.

04 **Network monitoring**

Log inappropriate sensitive data transfers.

05 **Access/usage monitoring**

Monitor access and usage of high-risk data to identify potentially inappropriate usage.

05 **Export/Save control**

Restrict user ability to copy sensitive data into unapproved containers (e.g. e mails, browsers).

Conclusion

Conclusion

- We can safely say that Sony broke one of the core principles in online business, which is **transparency**.
- They knew about the vulnerability, but did not react on time and their security measures were simply not good enough.
- After the incident, Sony opened up some more positions like "**Chief Information Security Officer**" in order to add more layers of security.
- They also added **automatic software monitoring**, enhanced level of **data encryption**, enhanced **detection software** and additional **firewall**.

Could Sony have prevented it ?

Yes!


THANK YOU!

References

1. https://manuals.playstation.net/document/en/psp/current/music/index_qm.html
2. https://en.wikipedia.org/wiki/George_Hotz
3. https://en.wikipedia.org/wiki/Anonymous_(hacker_group)
4. https://en.wikipedia.org/wiki/Cryptographic_hash_function
5. https://en.wikipedia.org/wiki/2011_PlayStation_Network_outage#cite_note-85