ISSeG

Integrated Site Security for Grids

EU-FP6 Project 026745

Checklist for System Administrators

David Jackson, STFC

CHEP 07, Victoria BC, 4 September 2007

Integrated
Site
Security for
Grids

www.isseg.eu

Information Society and Media

Checklist

1. Harden the OS and Applications
2. Keep the OS and Applications up-to-date
3. Use a local firewall
4. Take advantage of the logs
5. Ensure that all passwords are secure
6. Take extra precautions for privileged accesses
7. Use security products when relevant
8. Take into account physical security
9. Keep your security knowledge up-to-date.

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

1. Harden the OS & applications

- **minimise the number of packages installed**
- **minimise the number of accounts enabled**
- **minimise the number of network services offered**
- **minimise the number of privileged processes running** (this includes running with least privileges whenever possible)
- **tighten the configuration of the major services** (this includes limiting access to the minimum)

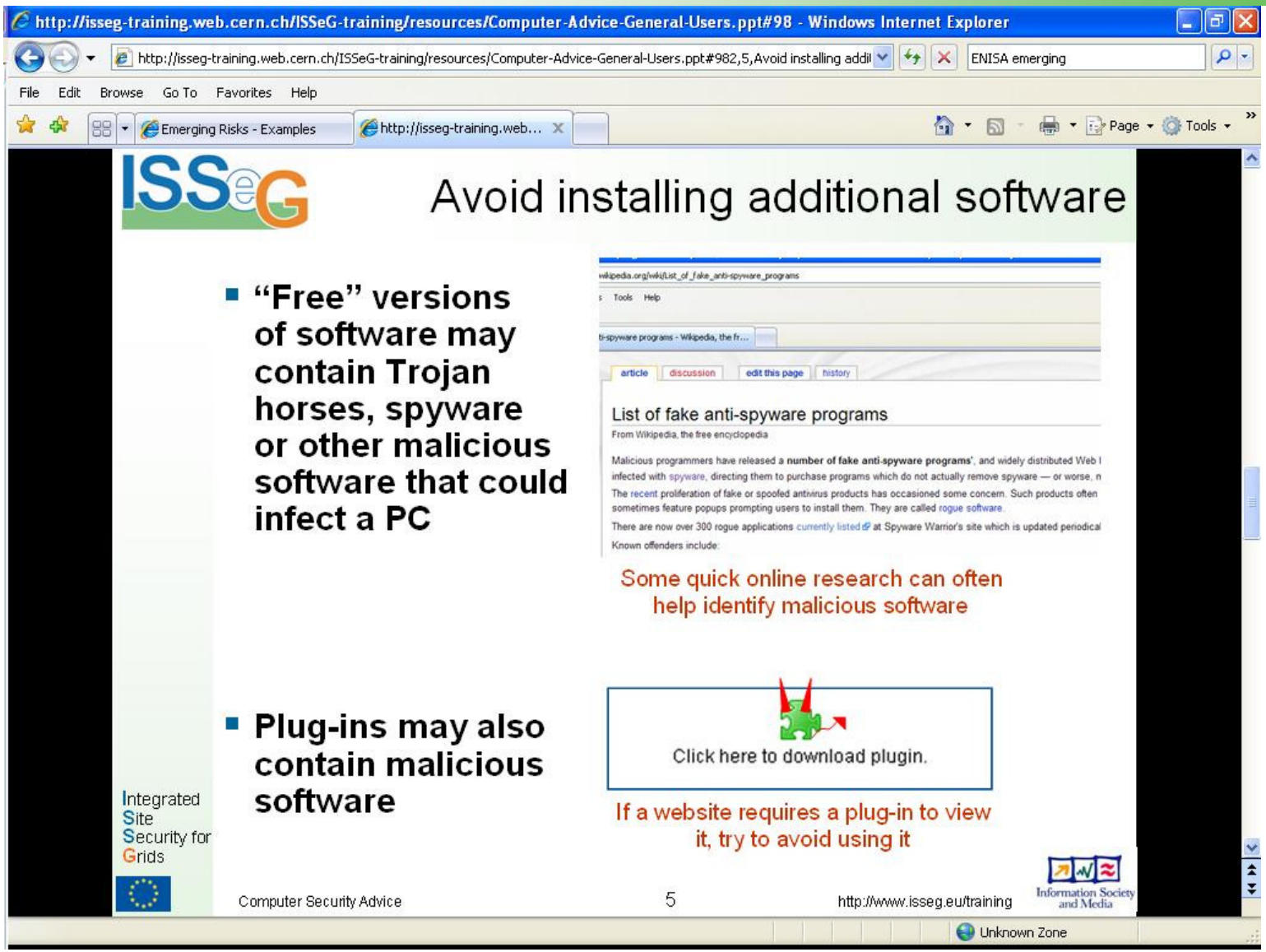
If your users have "admin rights"…

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

user training – e.g. www.isseg.eu



Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

2. Keep the OS & Apps up-to-date

- **install all the security patches as soon as possible**
- **ideally, use a system that automates patching**

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

3. Use a local firewall

- **install a local firewall configured to only allow what is expected** (i.e. default policy is deny)
- **ideally, also filter outgoing network traffic**

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

4. Take advantage of the logs

- **select appropriate logging levels for all sensitive components**
- **frequently review the logs to detect suspicious activity**
- **ideally, store the logs remotely to avoid tampering**

5. Ensure that all passwords are secure

- **make sure the passwords used are good enough** (ideally, enforce this with the appropriate tools)
- **make sure the passwords are not exposed** (this includes using encrypted protocols such as https)
- **make sure the passwords are changed regularly**

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

6. Take extra precautions for privileged a/c

- **restrict privileged accesses to the bare minimum**
- **use delegation to minimise the number of operations requiring**
- **full privileges** (for instance use sudo on Unix)
- **log all actions executed with system privileges**

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

7. Use security products when relevant

- **anti-virus**
  (ideally, with automatic signature update)
- **Intrusion Detection Systems**
  (both host-based and network-based)
- **integrity checkers to detect system modifications**

Integrated Site Security for Grids
www.isseg.eu

Information Society and Media

8. Physical access & 9 Security Knowledge

- 8. Take into account physical security (when relevant)
- 9. Keep your security knowledge up-to-date

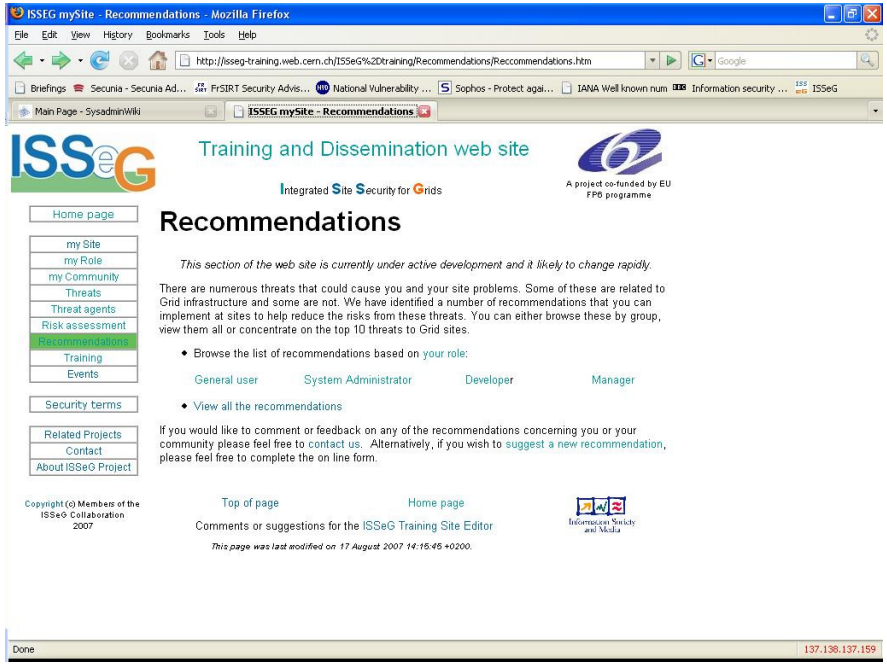
Integrated Site Security for Grids

www.isseg.eu

Information Society and Media

Implementing the checklist

- The ISSeG project are developing a number of recommendations that will include links to practical advice on how to implement some or all of the above suggestions.



http://www.isseg.eu/

Integrated Site Security for Grids

www.isseg.eu

Information Society and Media