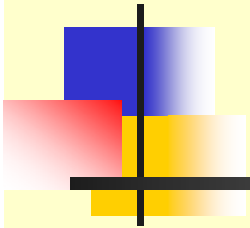


Integrated Site Security Project



**Denise Heagerty
CERN**

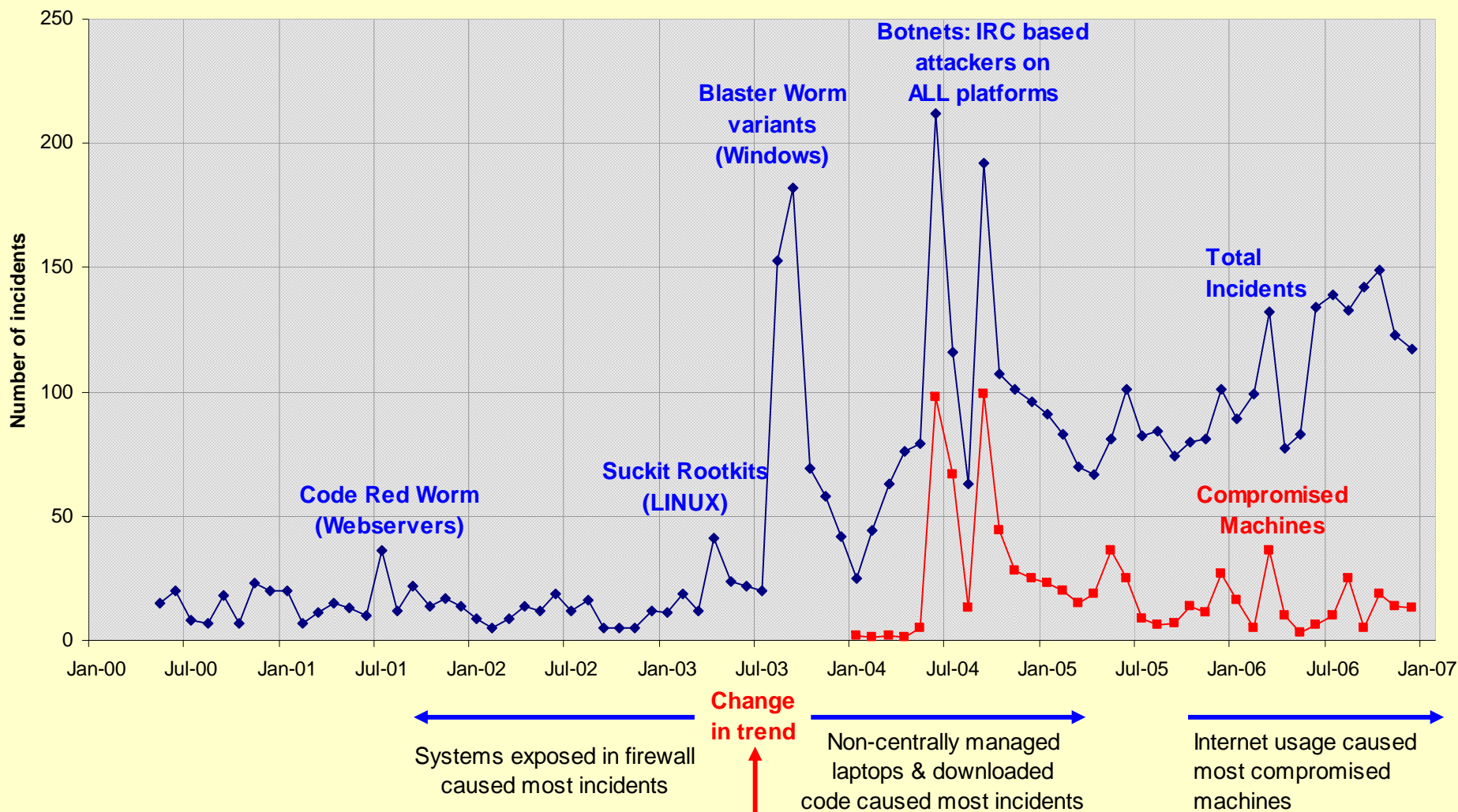
22 May 2007

Overview

- **Evolution of incidents at CERN**
- **Security goals for CERN**
- **Causes of security break-ins**
- **Integrated site security project**
- **ISSeG: Integrated Site Security for Grids**

Evolution of incidents since May 2000

Timeline for Security Incidents May 2000 - December 2006



Security Goals for CERN

- **Keep the site working effectively and able to assure the organisation's mandate**

- **Prevent/Limit the impact of incidents based on their risks. Specifically:**
 - Pro-actively alert/protect against common and likely attacks
 - Rapidly isolate systems placing the site at risk
 - For services, ensure that security incidents do not adversely affect the service definition levels (availability, privacy, ...)
 - Balance the cost of an incident against the cost of the ability to prevent it

- **Ensure the ability to record, measure and control risks (human, financial, image, ...)**

Causes of break-ins (1)

- **Known security holes**

- Unpatched systems and applications are a constant target
- Additional code often lacks automated updates (e.g. web plug-ins)

- **0 Day exploits: security holes without patches**

- Firewall, application and account access controls give some protection
- Users are key targets for exploits (social engineering)

- **Weak/missing/default passwords**

- Care is needed when installing additional (commercial) applications which may have known default passwords

- **Insufficient file protections**

- Popular for transiting illegal data or as a stepping stone for further break-ins
- Insufficiently protected web pages can be abused for unwanted advertising
- Web based mail archives need sufficient protections

Causes of break-ins (2)

- **Files on the Internet hiding trojan code**
 - Popular files are targets, e.g. music, video, games, software
 - Hiding trojans in 'free' security tools is a known devious trick
- **Capturing passwords**
 - Compromised systems at remote sites are used to capture passwords
 - Keyboard loggers are popular in new viruses
- **Tricking users is (too) often successful**
 - To visit rogue web sites , open attachments, execute code ...
 - Web based forums and Instant Messaging are growing targets
 - Often combined with 0day exploits
 - Phishing attacks to steal passwords, identity, bank and credit card details

Additional Concerns...

- **Oday exploits are increasing**
 - Little/no time for preventative action
- **Botnets are evolving**
 - Will become harder to detect
- **Social engineering is getting harder to detect**
 - Tricks are sophisticated and targeted
- **Databases are a key target**
 - Identity and information theft is profitable
- **Web applications are a key target**
 - <http://www.honeynet.org/papers/webapp/>
- **P2P technologies are hard to control**
 - Used for voice, video, software updates....
 - Difficult to distinguish P2P traffic from suspicious network activity

Integrated Site Security Project: Motivation

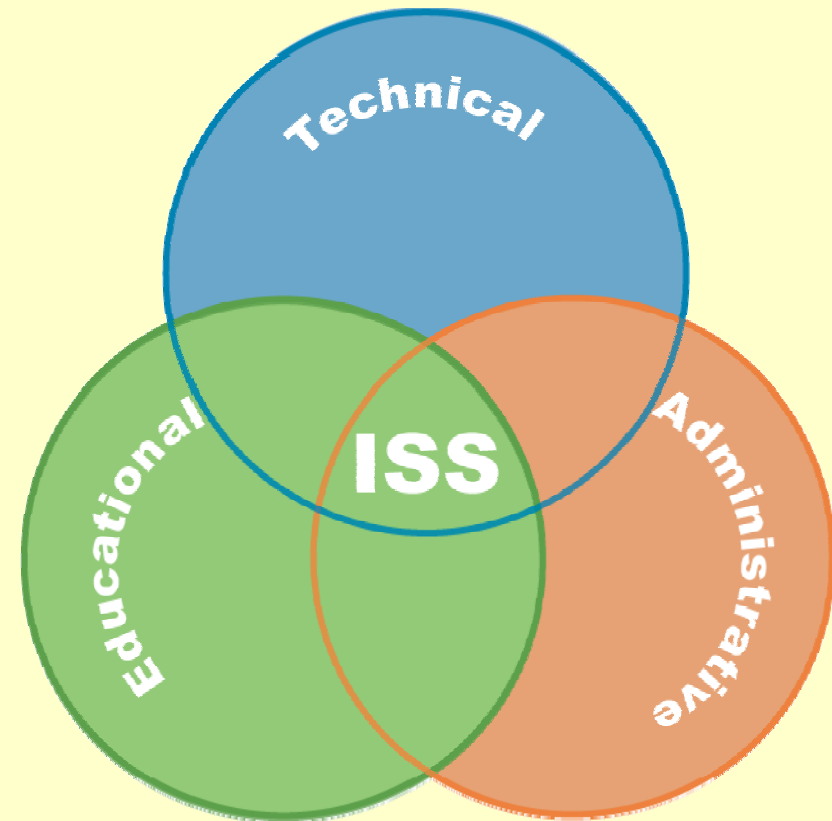
- **Incidents were increasing**
 - Recovery is expensive: loss of service, diverted resources, ...
 - **Major incidents had impacted normal working**
 - Network and other services had been unavailable
 - **Control systems needed additional protection**
 - Moving to 'commodity' solutions but security is lacking
 - **Grid computing extends security implications**
 - Sites are interconnected and incidents can easily spread
 - **Technical solutions provide only partial protection**
 - Policies and procedures need to be defined/updated/enforced
 - People need training and clear responsibilities
- This led to the Integrated Site Security concept**
- Combining technical, administrative and educational security solutions

Strategic Directions Identified

- **Centralise management of resources**
 - adapt security levels based on groups of devices or users
 - must be flexible enough to meet needs and avoid exceptions
- **Integrate identity and resource management**
 - link formal registrations with account controls
- **Enhance network connectivity management**
 - database-driven with links to devices and people
- **Integrate and evolve security mechanisms and tools**
 - adapt to new threats and technologies (e.g. 10Gbps links)
- **Integrate security training, best practices and administrative procedures**
 - ensure security training and clear responsibilities
 - balance academic freedom with its risks and costs

ISSeG: Integrated Site Security for Grids

- Project co-funded by the European Commission
<http://www.isseg.eu>
- Extends and disseminates ISS expertise:
 - Recommendations
 - Methodologies
 - Training Material
- Targets Grid sites



ISS: Integrated Site Security