CERN's Computer Security Challenges

Denise Heagerty
CERN Computer Security Officer

Openlab Security Workshop, 27 Apr 2004

Outline

- **Incident summary, 2001-2003**
- **Viruses, Worms and Backdoors**
  - Risks and actions taken so far
- **Software risks and restrictions**
  - P2P, IRC, IM, …
  - Balancing risk with academic freedom
- **Risks from visiting users**
- **Protecting control systems**
- **Protecting GRID resources**
- **Summary of CERN's computer security challenges**

Incident Summary, 2001-2003

2001	2002	2003	Incident Type
59	31	31	**System compromised (intruder has control)** ▪ security holes in software (e.g. ssh, kernel, IE, web, CVS)
42	25	32	**Compromised CERN accounts** ▪ *sniffed* or *guessed* passwords
11	21	429	**Serious Viruses and worms** ▪ Blaster/Welchia (414), Sobig (12) , Slammer(3)
13	21	143	**Unauthorised use of file servers and P2P software** ▪ insufficient access controls, P2P file-sharing, Skype
15	16	2	**Serious SPAM incidents** ▪ e.g. CERN systems used to originate SPAM
11	9	6	**Miscellaneous security alerts**
151	123	643	**Total Incidents**

Viruses, Worms and Backdoors (1)

are a serious security threat:

- **Infections increasingly occur before anti-virus patterns are available**
- **Infections regularly include backdoors which give system control to intruders**
- **Backdoors are difficult to detect**
  - e.g. initiated by a client program in response to pre-defined *normal* packets
- **Infections increasingly include keyloggers**
  - Used to collect passwords, credit card details, etc
- **Most infected PCs belong to visitors**
  - Managed by individuals and not part of CERN domain

Viruses, Worms and Backdoors (2)

Actions taken so far:

- **Pro-active anti-virus response**
  - E.g. Beta pattern files, specific filters on mail gateways, new viruses are reported, detection tools identify infected systems to disconnect
- **Computers must be registered and kept secure**
  - Computers detected as insecure can be blocked from the network and the registered contact informed
  - Collaboration is generally good, but expertise is insufficient
- **Strong management recommendation to run centrally managed systems (Windows and Linux)**
  - More than 5000 Windows and 3500 Linux PCs have automated patches
  - More than 1000 PCs are individually managed (visitors, non-standard)
  - Dual boot systems need to keep both systems patched

Risks from client software

- **Client software bypasses traditional security checks**
  - E.g. firewalls, application gateways, trusted web sites
- **P2P file sharing software is a target for spreading viruses**
  - Reports say more than 50% of KaZaA files contain viruses
- **IRC (Internet Relay Chat) is used by intruders**
  - E.g. to communicate together, to upload stolen data, to advertise tricked data
- **IM (Instant Messaging) is targeted by intruders**
  - E.g. Compromised systems via security holes, connections to non-trusted servers (ICQ), links to tricked web sites
- **Client systems may be converted to *Bots***
  - Allows intruders to control many systems e.g. to launch DDoS attacks

Software Restrictions

- **Software installation and use is restricted**
  - http://cern.ch/security/software-restrictions
- **Personal use of P2P software is NOT permitted**
  - http://cern.ch/security/file-sharing
  - http://cern.ch/security/skype
- **IRC bots and servers are NOT permitted**
  - Clients are permitted and used for a professional purpose
- **Personal installations of IM are not permitted**
  - CERN’s standard Windows/XP configuration includes Messenger
- **Systems and applications must be kept secure**
  - http://cern.ch/ComputingRules
  - Relies on user awareness and competence
  - Competes with publicity from the “friends network”

Balancing risk with academic freedom

Risks:

- **Personal use of CERN's computing and network facilities *is* permitted**
  - Defined at http://cern.ch/ComputingRules
  - e.g. personal email and web surfing
- **Social engineering tricks succeed**
  - E.g. virus infected attachments executed, insecure web sites visited
- **Academic curiosity increases risk**
  - E.g. Insecure software and spyware unintentionally installed

Counter-Measures:

- **Awareness raising campaigns**
- **Restrictive Rules**

Risks from Visiting Users

- **CERN’s users are located around the world**
  - Many are based at universities and research labs
- **Visiting users increasingly bring their laptops**
  - Need network access to CERN services and general Internet
  - Relies on users keeping their laptops secure
  - Network based tools detect some problems, e.g. scanning
- **Users need to access CERN systems remotely**
  - Key services directly on the Internet (mail, web, files)
  - Terminal Services offer additional functionality (client-server)
  - VPN for special cases (users agree to additional security rules)
- **Insecure laptops (connected directly or by VPN) are the biggest source of viruses**
  - Enforced network registration helps to fix them quickly, but does not prevent the problem

Protecting Control Systems

- **Accelerator and technical control systems are connected on a physically separate network**
  - No direct Internet access to/from off-site
  - Access restrictions on-site are difficult to manage
- **Off-site access for specialists**
  - Experts can be at home or at remote sites around the world
  - Some systems are managed by outsourced contracts
  - Connect via gateways, e.g. Windows Terminal Services
  - Token based authentication proposed for critical systems
- **Stability v Updates**
  - Automated patching and software updates based on needs and risk
- **Critical systems**
  - Reduce risk with gateways, firewalls, one-time passwords, …

Protecting GRID resources

- **GRID computing distributes applications across many sites with significant computing power**
- **Risks for GRID resources have been analysed**
  - http://cern.ch/proj-lcg-security/risk_analysis.html
- **Security holes are considered high risk**
  - Requires a rapid process for applying security updates
  - Respond rapidly to suspected break-ins
  - Good collaboration between CSIRTs
  - Reduce risk by combining relevant security tools
    - e.g. firewalls, access control, intrusion detection
- **Limit the risk for DoS attacks**
  - Restrict network access to GRID systems
  - Respond rapidly to attacks, e.g. disconnect from the network

Summary of security challenges

- **Limit the impact of viruses and worms**
  - Avoid significant computer and network downtime
- **Protect client and server software**
  - Solutions beyond vulnerability scanning and automated patching
  - Limit the ability of users to introduce security exposures
    - P2P, IRC, IM are prone to social engineering tricks
- **Prevent network access for insecure systems**
  - How to detect security exposures before allowing network access?
- **Protect control systems**
  - Solutions must be easily manageable and allow remote Internet access for authorised experts
- **Scale security solutions to GRIDs**
  - Tools need to be easy, fast and automated