

## Additional Newer Statistics

---

April 2007

Communications of the ACM, Vol.50, No. 4  
in News Track, pp.13 and  
in Digital Village, p.18

## News Track - Techworld.com

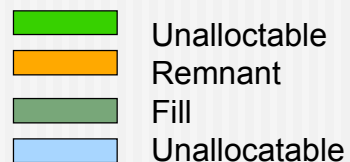
---

- Statistics exhibiting any damaging acts
- IT-employees
  - 86% of those who committed cypercrimes held technical positions and
  - 90% had system administrator rights
  - 41% of the IT saboteurs were employed at the time they did it
    - VPNs
    - Old passwords
- Help for detecting internal threats early as possible
  - [www.cert.org/archive/pdf/merit.pdf](http://www.cert.org/archive/pdf/merit.pdf)

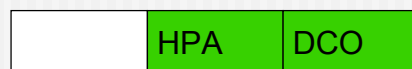
## Hiding Data, Forensics, and Anti-Forensics

- Data hiding tactics for Windows and Unix file systems
- Classification in 11 weak-points
- [www.berghe.net/publications/data\\_hiding/data\\_hiding.php](http://www.berghe.net/publications/data_hiding/data_hiding.php)

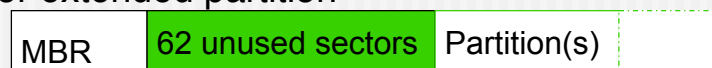
## Weak-points



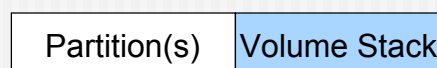
1. Host Protected Area and Drive Configuration Overlay



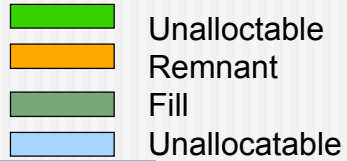
2. Unused space in Master Boot Record (MBR) or extended partition



3. Volume Stack

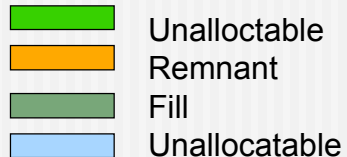


## Weak-points (2)





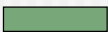
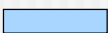
4. Partition Stack Remainder Based on Block Size
5. Boot Sector in non-bootable partition
6. Unallocated space in a partition
7. Good blocks marked "bad" fake bad blocks

## Weak-points (3)



8. Disk stack
  - File data
  - RAM
  - Disk Stack
  - File Stack
  - File Stack
  - File Stack
  - File Stack
  - File Stack
9. Unused space in Superblock (ExtX)
10. Unused space in block group (ExtX)
  - Unused position of an ExtX directory
  - Group Description Table
  - rest block group

## Weak-points (4)

	Unalloctable
	Remnant
	Fill
	Unallocatable

### 11. Directory entries

Directory Entries	
-------------------	--