- **Network(ed) Filesystems.**

> **"There are three kinds of death in this world. There's heart death, there's brain death, and there's being off the network."**
>
> **-- Guy Almes**

Copyright Information

Chapter 64
Filesystems

- **Agenda**
  - **Basic Threats for Network Filesystems**
  - **Selected Protocols**
  - **Feeding and Care**

Basic Threats for Network Filesystems

- **Use as designed.**

Threats to Networked File Storage

- **File data (obviously)**
  - **Few network file systems offer encryption**
  - **Focus on LAN & performance**
- **Login credentials**
- **Access controls**
- **Service discovery**
  - **Remote Procedure Calls (RPC)**
- **Denial of Service**

Distributed Computing

- **Distributed Computing Environments (DCE)**
    - **require more than file services**
    - **process cooperation (locking)**
    - **clustering, local copies, replication**
- **Network traffic reveals roles of servers**
- **Replication shuffles data**
    - **Guard all replicated data!**

Selected Protocols

- **Common Protocols for File Sharing.**

Appletalk

- **Model OSI layer implementation**
  - **Covers layer 1 to 7**
  - **Uses addresses translated into names**
- **Local network protocol**
  - **Local services complete with routing**
  - **Zeroconf functions**

Network File System (NFS)

- **Also known as "No File Security"**
  - **No authentication**
  - **NFS V2/V3 rely on UID/GID**
  - **NFS server handles security**
- **NFS V4 addresses shortcomings**
  - **RPC with Kerberos V5**
  - **SPKM/LIPKEY – Public Keys**

Server Message Block (SMB)

- **Created by IBM in 1983**
- **Peer-to-peer protocol**
  - **Client sends requests, server answers**
- **Microsoft® modified original specs**
  - **NTLM V1/V2 authentication**
  - **Unicode, long filenames**
- **Different dialects in use (Windows, Samba)**
- **Vista uses SMB 2.0**
  - **Reduced complexity**

Common Internet File System (CIFS)

- **SMB 1.x with extensions**
  - **symlinks, hardlinks, larger file size**
  - **gets rid of NetBIOS ballast, pure TCP/IP**
  - **offers RPC and access to domain services**
  - **used for NAS services**
- **Available since MS Windows 2000**

- **How To Keep File Stores Out Of Trouble.**

General Security Principles

- **Limit network filesystems to local network**
- **Transport network FS traffic securely**
  - **Use VPN technology**
  - **Use encapsulation as necessary**
- **Monitor filesystem performance**
  - **Look for anomalies**
  - **Detect unauthorised access**

Stress Tests

- **Test network file systems**
  - **with various loads**
  - **with corrupted data (fuzzing)**
  - **with concurrent access (read/write)**
- **Test while backup system is running**
- **Establish a baseline for normal operation**
- **Monitor for anomalies**

Separation

- **Most network file systems are local**
- **Separate file services**
  - **Put public data into DMZs**
  - **Especially true for SAN/NAS**
  - **Take care of replication**
- **Allow only trusted clients to connect**
  - **Enable port security**
  - **Use 802.1X if possible**

- **Summary**
  - **Filesystems belong to the LAN.**
  - **Limit access to file services.**
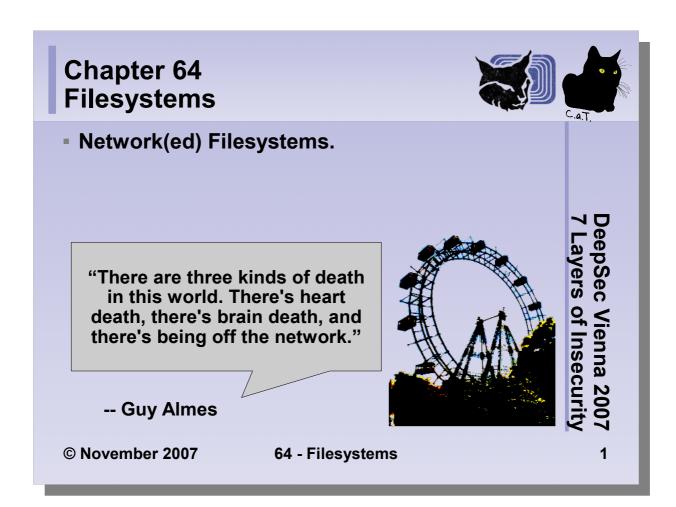 - **Use secure transport when routing via WAN**

Thank You

- **Questions?**

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 64
Filesystems

▪ **Network(ed) Filesystems.**

> "There are three kinds of death in this world. There's heart death, there's brain death, and there's being off the network."

-- Guy Almes

DeepSec Vienna 2007
7 Layers of Insecurity

© **November 2007**   **64 - Filesystems**   **1**

Copyright Information

- **Some rights reserved / Einige Rechte vorbehalten**
- **Michael Kafka, René Pfeiffer, Sebastian Meier
  C.a.T. Consulting and Trainings, Vienna, Austria**
- **You may freely use, distribute and modify this work under following agreement:**
- **Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:**

**Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)**

**Only for non commercial use
Nur für nichtkommerzielle Nutzung**

**Derivative work under same licence
Derivative Arbeit unter selber Lizenz**

http://www.creativecommons.com

**DeepSec Vienna 2007
7 Layers of Insecurity**

© November 2007   **64 - Filesystems**   **2**

Chapter 64
Filesystems

- **Agenda**
  - **Basic Threats for Network Filesystems**
  - **Selected Protocols**
  - **Feeding and Care**

**DeepSec Vienna 2007
7 Layers of Insecurity**

© November 2007   **64 - Filesystems**   **3**

Basic Threats for Network Filesystems

- **Use as designed.**

© November 2007   **64 - Filesystems**   **4**

DeepSec Vienna 2007
7 Layers of Insecurity

Threats to Networked File Storage

- **File data (obviously)**
  - **Few network file systems offer encryption**
  - **Focus on LAN & performance**
- **Login credentials**
- **Access controls**
- **Service discovery**
  - **Remote Procedure Calls (RPC)**
- **Denial of Service**

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007   **64 - Filesystems**   **5**

Distributed Computing

- **Distributed Computing Environments (DCE)**
  - **require more than file services**
  - **process cooperation (locking)**
  - **clustering, local copies, replication**
- **Network traffic reveals roles of servers**
- **Replication shuffles data**
  - **Guard all replicated data!**

© November 2007   **64 - Filesystems**   **6**

DeepSec Vienna 2007
7 Layers of Insecurity

Selected Protocols

- **Common Protocols for File Sharing.**

© November 2007   **64 - Filesystems**   **7**

DeepSec Vienna 2007
7 Layers of Insecurity

Appletalk

- **Model OSI layer implementation**
  - **Covers layer 1 to 7**
    - **Uses addresses translated into names**
- **Local network protocol**
  - **Local services complete with routing**
  - **Zeroconf functions**

© November 2007　　　**64 - Filesystems**

**DeepSec Vienna 2007
7 Layers of Insecurity**

8

Network File System (NFS)

- **Also known as "No File Security"**
  - **No authentication**
  - **NFS V2/V3 rely on UID/GID**
  - **NFS server handles security**
- **NFS V4 addresses shortcomings**
  - **RPC with Kerberos V5**
  - **SPKM/LIPKEY – Public Keys**

**DeepSec Vienna 2007
7 Layers of Insecurity**

© November 2007   **64 - Filesystems**   **9**

The Network File System (NFS) exists since 1989 (for version 2). NFS V3 was "ready" in 1995. NFS was originally developed by SUN Microsystems. SUN handed the development to the Internet Engineering Task Force (IETF). NFS V4 was specified in 2000, influenced by the Andrew File System (AFS) and Common Internet File System (CIFS).

Server Message Block (SMB)

- **Created by IBM in 1983**
- **Peer-to-peer protocol**
  - **Client sends requests, server answers**
- **Microsoft® modified original specs**
  - **NTLM V1/V2 authentication**
  - **Unicode, long filenames**
- **Different dialects in use (Windows, Samba)**
- **Vista uses SMB 2.0**
  - **Reduced complexity**

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007   **64 - Filesystems**   **10**

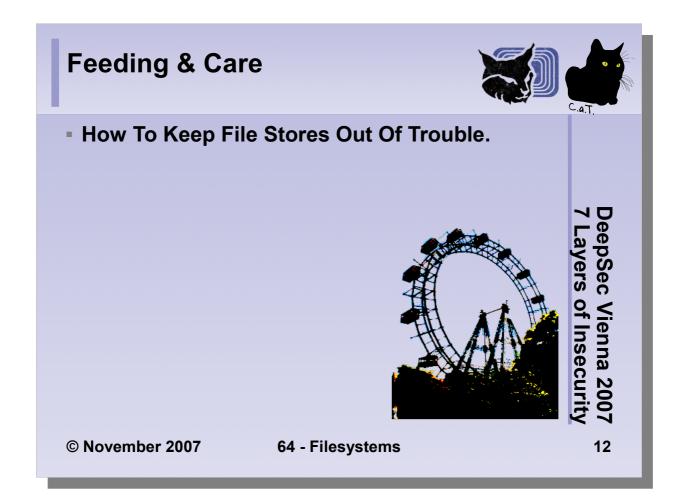# Common Internet File System (CIFS)

- **SMB 1.x with extensions**
  - **symlinks, hardlinks, larger file size**
  - **gets rid of NetBIOS ballast, pure TCP/IP**
  - **offers RPC and access to domain services**
  - **used for NAS services**
- **Available since MS Windows 2000**

**DeepSec Vienna 2007
7 Layers of Insecurity**

© November 2007   **64 - Filesystems**   **11**

Feeding & Care

- **How To Keep File Stores Out Of Trouble.**

**DeepSec Vienna 2007
7 Layers of Insecurity**

© November 2007   **64 - Filesystems**   **12**

General Security Principles

- **Limit network filesystems to local network**
- **Transport network FS traffic securely**
  - **Use VPN technology**
  - **Use encapsulation as necessary**
- **Monitor filesystem performance**
  - **Look for anomalies**
  - **Detect unauthorised access**

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007   **64 - Filesystems**   **13**

Stress Tests

- **Test network file systems**
  - **with various loads**
  - **with corrupted data (fuzzing)**
  - **with concurrent access (read/write)**
- **Test while backup system is running**
- **Establish a baseline for normal operation**
- **Monitor for anomalies**

**DeepSec Vienna 2007
7 Layers of Insecurity**

© November 2007   **64 - Filesystems**   **14**

Separation

- **Most network file systems are local**
- **Separate file services**
  - **Put public data into DMZs**
  - **Especially true for SAN/NAS**
  - **Take care of replication**
- **Allow only trusted clients to connect**
  - **Enable port security**
  - **Use 802.1X if possible**

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007　　　　**64 - Filesystems**　　　　**15**

Chapter 64
Filesystems

- **Summary**
  - **Filesystems belong to the LAN.**
  - **Limit access to file services.**
  - **Use secure transport when routing via WAN**

© November 2007   **64 - Filesystems**   **16**

DeepSec Vienna 2007
7 Layers of Insecurity

Thank You

- **Questions?**

© **November 2007** 64 - **Filesystems** 17

DeepSec Vienna 2007
7 Layers of Insecurity