

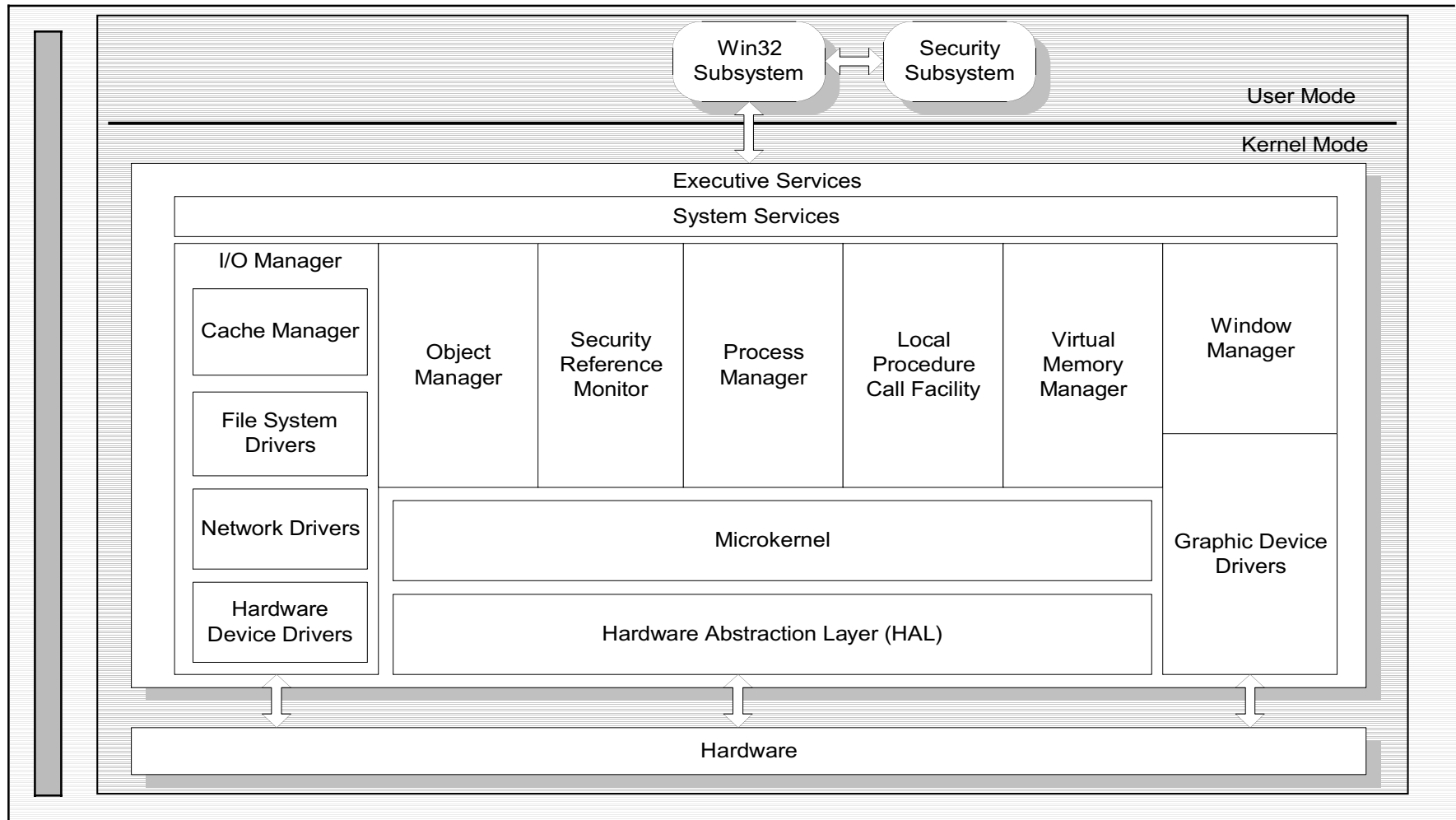
Windows NT Security Flaws by "NT Crackers"



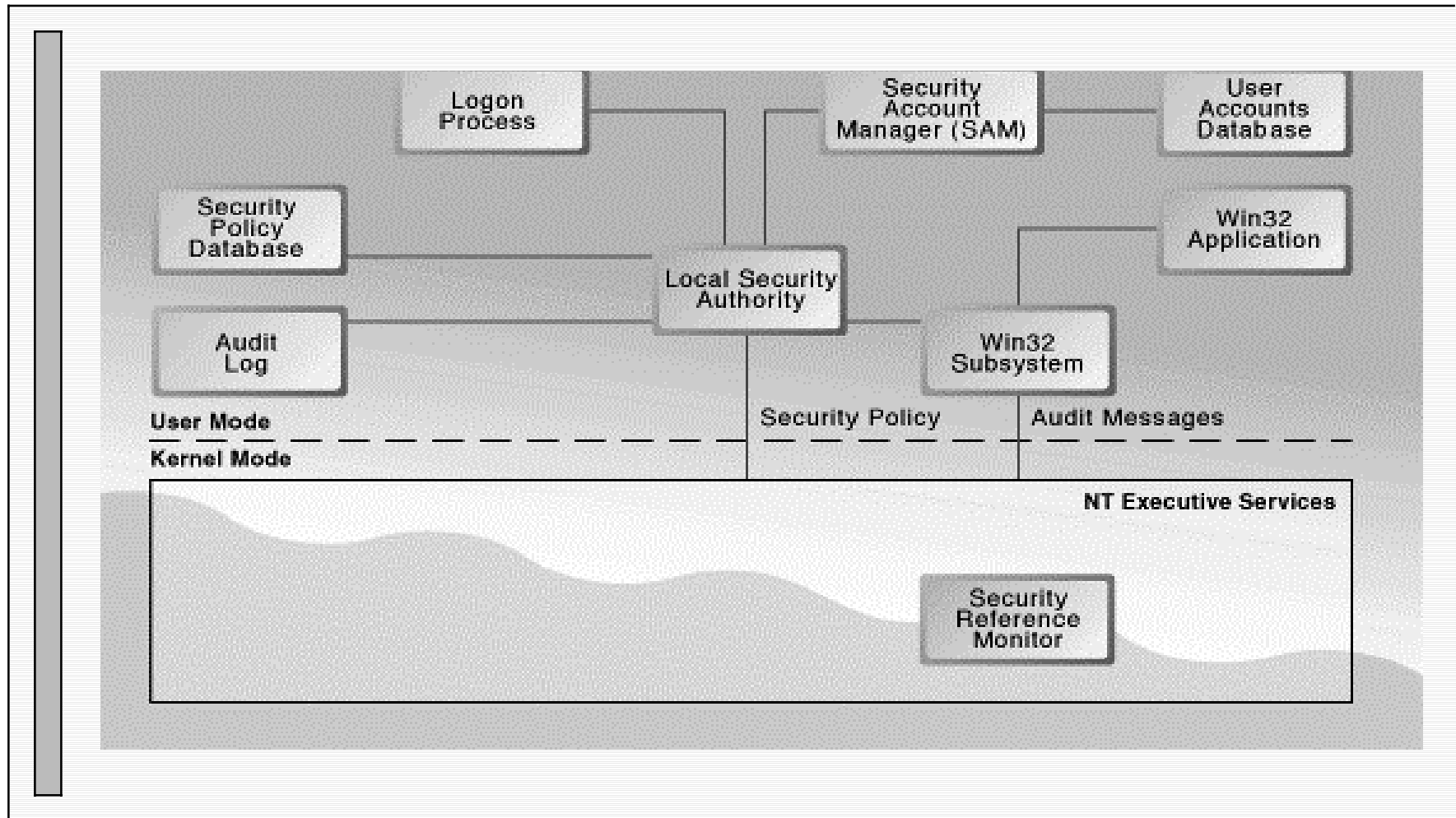
Overview

- **NT Architecture**
- **Basic NT Security Features**
- **NT Security Flaws**
- **Securing Windows NT**
- **Conclusion**

Architecture of Windows NT 4.0



Windows NT Security Components



Basic NT Security Features

- ⦿ Local Security Authority (LSA)

Basic NT Security Features

- ⊙ Local Security Authority (LSA)
- ⊙ Security Reference Monitor (SRM)

Basic NT Security Features

- ⊙ Local Security Authority (LSA)
- ⊙ Security Reference Monitor (SRM)
- ⊙ Security Account Manager (SAM)

Basic NT Security Features

- ⊙ Local Security Authority (LSA)
- ⊙ Security Reference Monitor (SRM)
- ⊙ Security Account Manager (SAM)
- ⊙ Access Control Lists (ACL)

Basic NT Security Features

- ⊙ Local Security Authority (LSA)
- ⊙ Security Reference Monitor (SRM)
- ⊙ Security Account Manager (SAM)
- ⊙ Access Control Lists (ACL)
- ⊙ Domains & Trusts

Secure Channels and Trusted Accounts

◎ Secure Channels

Designed to permit secure system-to-system communication (i.e. DC SAM replication)

◎ Trust Accounts

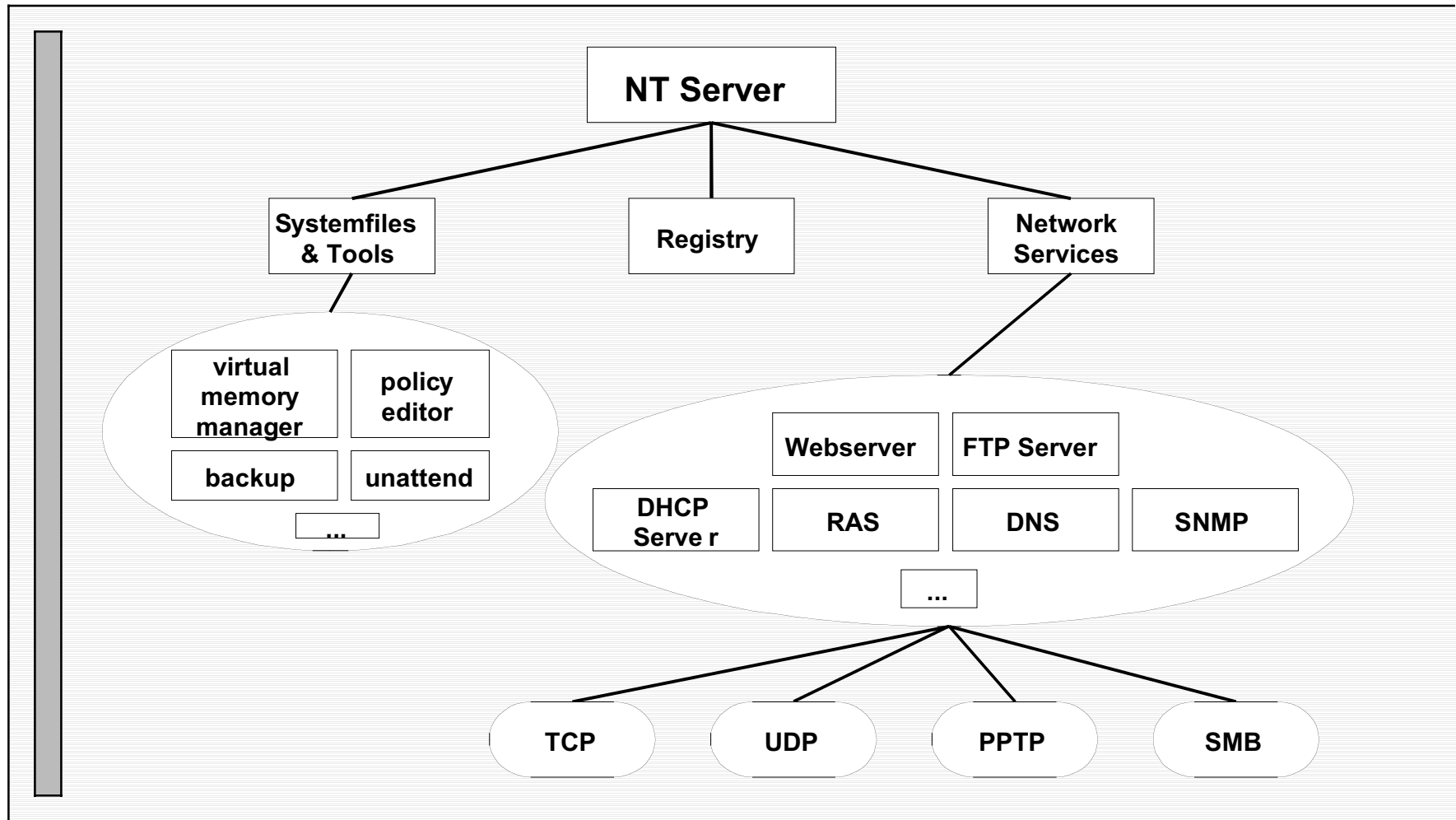
Hidden accounts used by NT to build secure channels

- < Server Trust Accounts. DC SAM replication
- < Workstation Trust Accounts. Pass-through authentication for local domain
- < InterDomain Trust Accounts. Pass-through authentication for remote domains

Basic NT Security Features

- ⊙ Local Security Authority (LSA)
- ⊙ Security Reference Monitor (SRM)
- ⊙ Security Account Manager (SAM)
- ⊙ Access Control Lists (ACL)
- ⊙ Domain & Trusts
- ⊙ Auditing
- ⊙ Logon Process
- ⊙ User Rights

Main locations for Windows NT Flaws



NT Security Flaws

- ⦿ NT Hotfixes
- ⦿ NT Service Packs



NT Security Flaws

- ⊙ Unauthorised Disclosure
- ⊙ Unauthorised Access
- ⊙ Denial of Service Attack



NT Security Flaws

Unauthorised Disclosure

Name: Clipboard

Description: If you lock a computer, it is still possible to paste the contents of the clipboard onto the username

Location: Kernel

Summary: There are a number of attacks leading to loss of confidentiality that are due to insufficient password protection.

Another major problem in this category is the use of other file/operating systems to gain access to NTFS filesystem.

NT Security Flaws

Unauthorised Access

Name: GetAdmin

Description: There are certain programmes available that a normal user can use to get administrator privilege.

NT Security Flaws

Denial of Service Attack

Name: Ping of Death

Description: By sending large ICMP packets from NT it is possible to corrupt the local TCP/IP stack.

Name: 'Land' attack

Description: By sending a spoofed packet with host and port address the same as the intended recipient and if the SYN flag is also set then it is possible to lock the machine.

NT Security Flaws

Miscellaneous Threats

- ⊙ NTFS Multiple Data Streams

E.g.

Notepad Text.txt

Notepad Text.txt:secret

- ⊙ Point-to-Point Tunnelling Protocol (PPTP)

The Registry

- ⊙ A Security Nightmare
- ⊙ The repository for all important data
- ⊙ A haven for Trojan horse attacks
- ⊙ Too complicated
- ⊙ Remote access
- ⊙ Lock it and audit, audit, audit...

Securing Windows NT

© C2 Compliance (e.g. C2config)

Securing Windows NT

- ⊙ C2 Compliance (e.g. C2config)
- ⊙ User Accounts

Securing Windows NT

- ⊙ C2 Compliance (e.g. C2config)
- ⊙ User Accounts
- ⊙ Registry

Securing Windows NT

- ⊙ C2 Compliance (e.g. C2config)
- ⊙ User Accounts
- ⊙ Registry
- ⊙ Network Services

Enhancements planned for NT 5.0

- ⊙ Kerberos replaces NTLM
- ⊙ Active Directory
- ⊙ Smart Cards
- ⊙ Identity mapping – X500 to NT SIDs
- ⊙ Security Configuration Editor (NT4 SP4)
- ⊙ Default ACLs on system directories & files
- ⊙ Encrypting File System
- ⊙ IPSEC

Conclusions

- ⊙ Windows NT can be secure

Conclusions

- ⊙ Windows NT can be secure
- ⊙ By default, it isn't secure

Conclusions

- ⊙ Windows NT can be secure
- ⊙ By default, it isn't secure
- ⊙ Over time, users have a tendency to make it less secure

Conclusions

- ⊙ Windows NT can be secure
- ⊙ By default, it isn't secure
- ⊙ Over time, users have a tendency to make it less secure
- ⊙ Watch the security alerts; understand enough to estimate their importance

Any Questions?

