Function Call Tracing Attacks to Kerberos V

Julian L. Rrushi
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano

Outline

- Definition of FCT
- Kerberos V in Linux
- FCT through DynInst API
- FCT through Interposition Libraries
- Discussion
- Conclusions

Function Call Tracing

- Local interception and manipulation of unencrypted information
- A run-time malicious activity
- Potentially performed through viral code
- No modification of binaries is required

Kerberos V

- Key Distribution Centre
  - Authentication server
  - Ticket granting server
- Kerberos Administration Service
- In Linux
  - krb5-server
  - krb5-libs
  - krb5-workstation

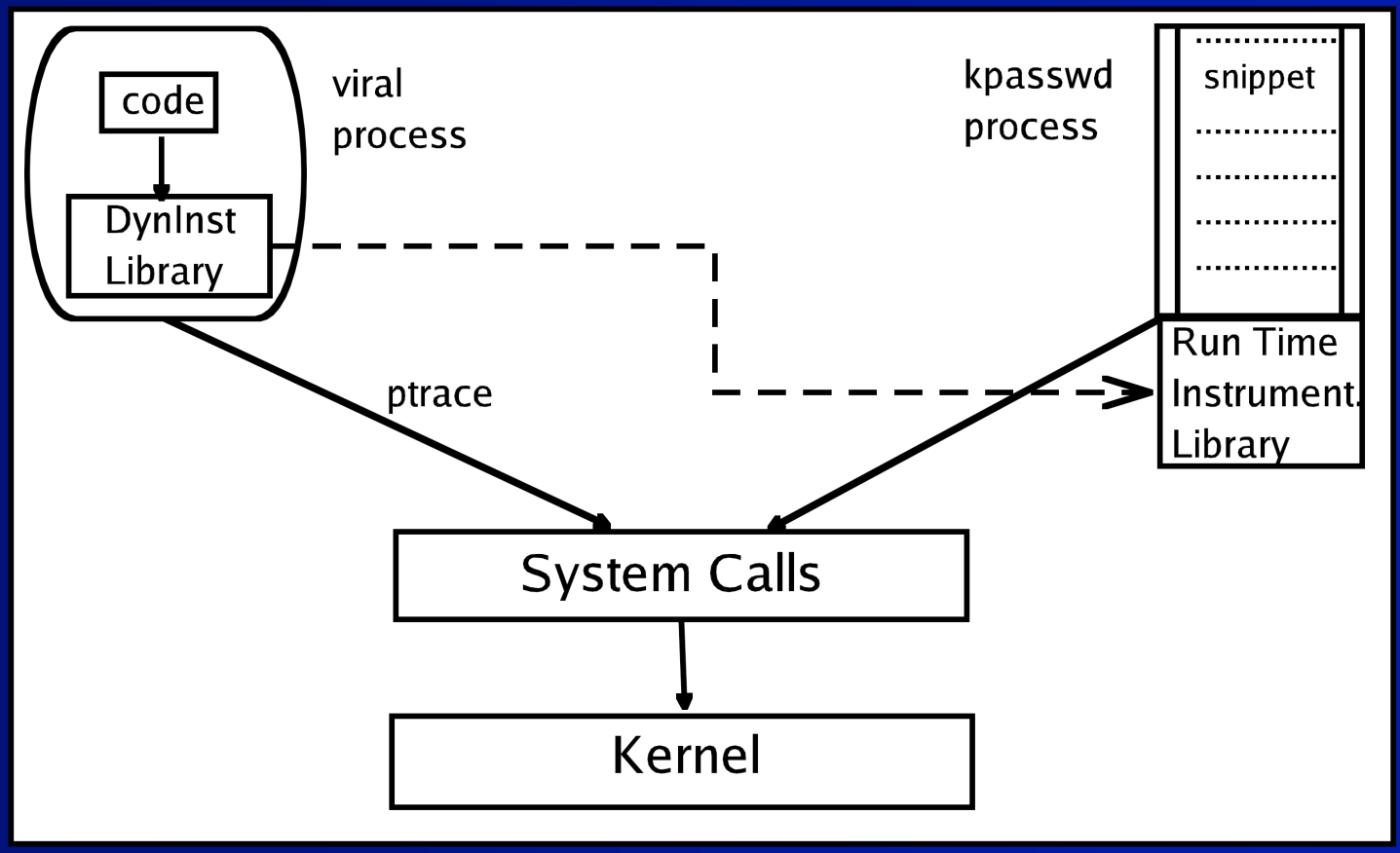
FCT Through DynInst API

- Insert new instructions into the address space of the target process
- Dynamically load new libraries
- Replace single instructions or entire functions

FCT Through DynInst API

- Attachment to the Kerberos process
- Location of the target function in the image of the Kerberos process
- Snippet insertion at the entry point of the target function

FCT Through DynInst API



FCT Through Interposition Libraries

- Interposition libraries
- Achieving interposition
  - Environment variables
  - Linkage table
  - Dyninst

FCT Through Interposition Libraries

- Interception of sensible information
- Process hijacking
- Function neutralization

Discussion

- Under some circumstances FCT can be performed directly
- Infection characteristics in a time-sharing system

Conclusions

- Function Call Tracing to Linux implementations of Kerberos V
- Problematic nature of tracing the function calls a program makes to the stack of shared libraries
- Demonstration of the power of DynInst as an attack tool
- Dangers deriving from switching shared libraries

Thank you!