Forense em memória com volatility, LiME e outras ferramentas

João Eriberto Mota Filho

Foz do Iguaçu, PR, 30 out. 2017

Sumário

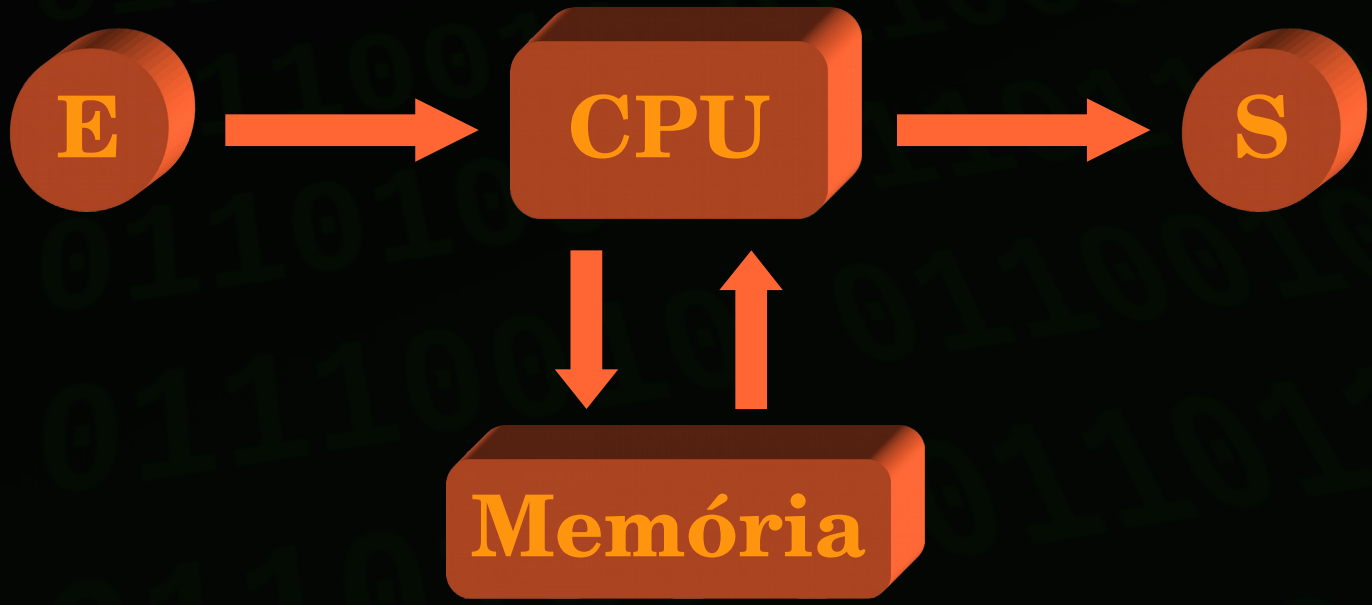
- Modelo von Neumman
- Estrutura básica de memória
- Arquivos de swap e de hibernação
- Persistência das informações
- Dump de memória
- Análise binária com volatility
- Análise visual
- Conclusão

Sumário

- **Modelo von Neumman**
- Estrutura básica de memória
- Arquivos de swap e de hibernação
- Persistência das informações
- Dump de memória
- Análise binária com volatility
- Análise visual
- Conclusão

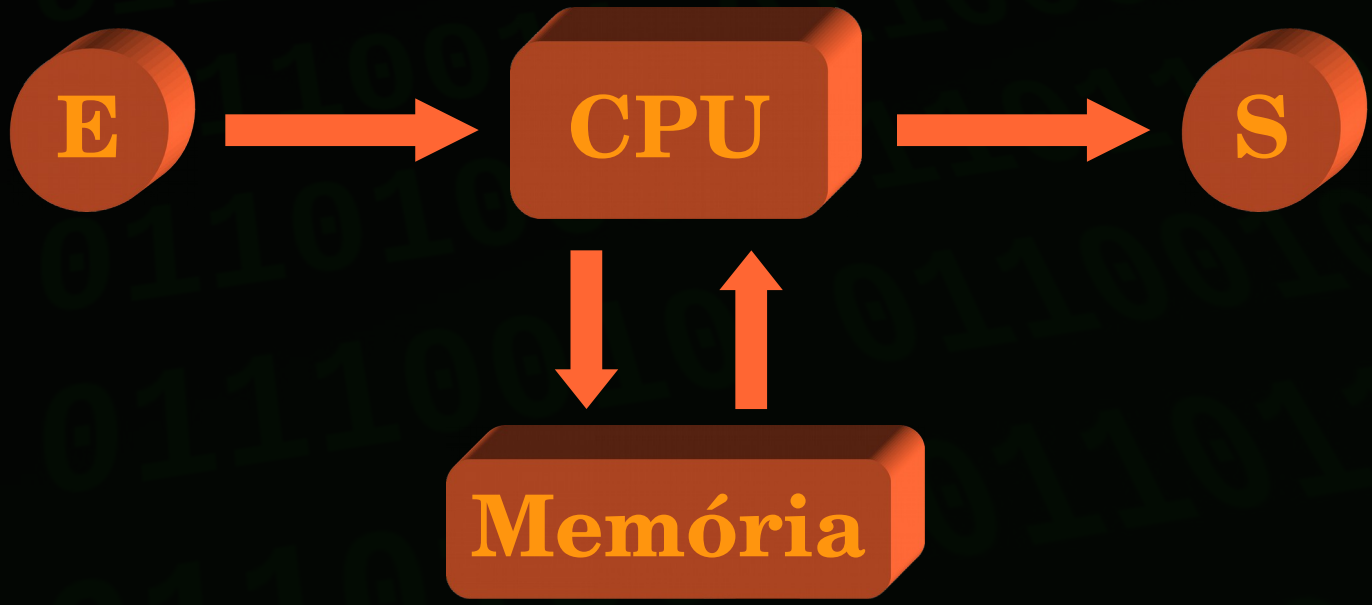
Modelo von Neumman

- Criado por John von Neumman em 1945.
- Modelo clássico de arquitetura de processamento.
- Tudo passa pela memória! (inclusive senhas)



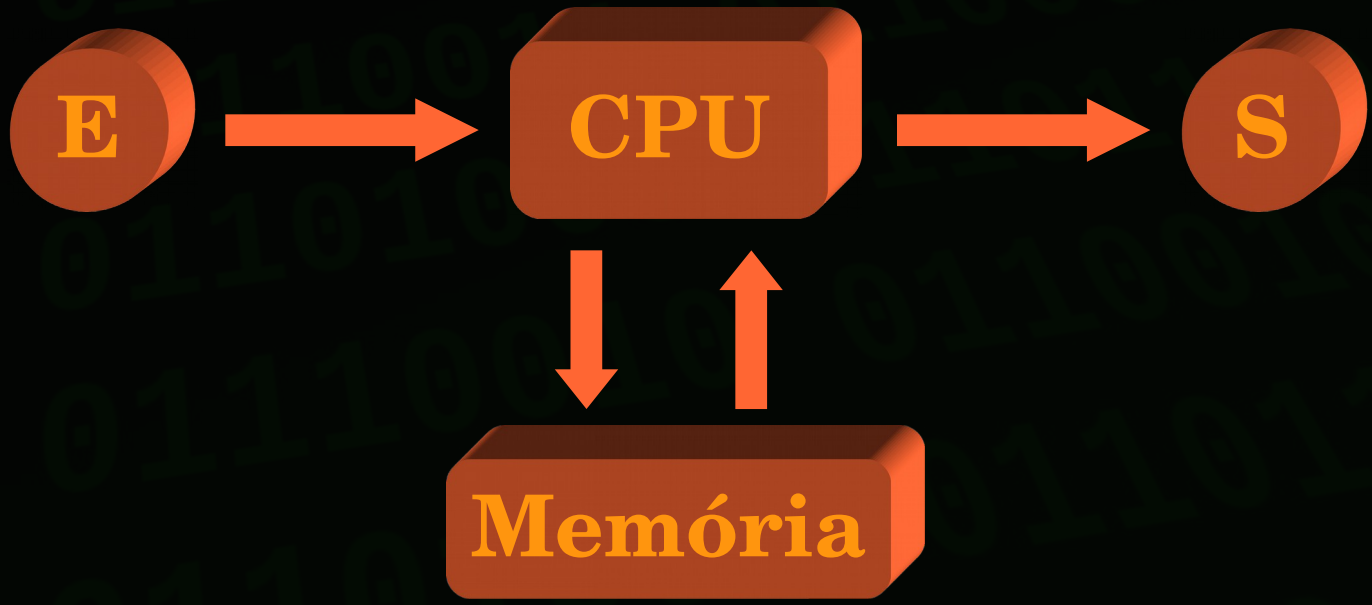
Modelo von Neumman

- Normalmente, assim como nos filesystems, a real deleção de dados na memória não ocorre.
- Aplicações sérias e que necessitam de segurança geram um compartimento e "wipam" esse compartimento.



Modelo von Neumman

- No Debian, o pacote secure-delete disponibiliza ferramentas para o wipe de memória, swap e disco.



Sumário

Estrutura básica de memória

- Similarmente aos filesystems, memórias trabalham com blocos, conhecidos como páginas.
- O tamanho de cada página será determinado pela arquitetura de processador.
- Como exemplo, a arquitetura Intel para PC de 32 e 64 bits utiliza páginas com 4 KB de tamanho.
- Geralmente, o conteúdo das páginas é controlado pelo processo que as utiliza.
- É difícil correlacionar páginas sem saber como o processo as gerenciou. Então, é possível recuperar conteúdos por páginas, independentemente.

Sumário

- Modelo von Neumman
- Estrutura básica de memória
- **Arquivos de swap e de hibernação**
- Persistência das informações
- Dump de memória
- Análise binária com volatility
- Análise visual
- Conclusão

Arquivos de swap e de hibernação

- O swap, juntamente com a RAM, compõe a memória virtual.
- Processamentos só ocorrem na RAM!
- O swap só é utilizado quando:
  - Não há mais RAM disponível.
  - Há hibernação habilitada (no Linux).
- Um swap utilizado poderá conter informações preciosas.
- O arquivo de hibernação é uma cópia da RAM.
- No MS Windows temos os arquivos pagefile.sys (swap menos frequente), hiberfil.sys (hibernação) e o novo swapfile.sys (swap frequente, implementado desde o Windows 8).

Sumário

- Modelo von Neumman
- Estrutura básica de memória
- Arquivos de swap e de hibernação
- **Persistência das informações**
- Dump de memória
- Análise binária com volatility
- Análise visual
- Conclusão

Persistência das informações

- O que acontece com o conteúdo da RAM quando desligamos o computador?
- Atualmente, na maioria das vezes, o conteúdo da RAM é mantido, mesmo com o computador desligado.
- Fatores:
  - Fontes controladas pela placa-mãe.
  - Baterias recarregáveis constantemente acopladas.
  - Nanoeletrônica.
  - RAMs mais novas podem manter dados estaticamente, como ocorre com os discos sólidos.

Sumário

Dump de memória

- Há alguns softwares que podem ser utilizados para realizar o dump de memória nos diversos sistemas operacionais.
- GNU/Linux e Android: LiME.
- MS Windows: DumpIt (junção do Win32dd com Win64dd).
- OS X: OSXPMem.
- Demonstração do LiME.

Sumário

Análise binária com volatility

- A perícia de dumps de memória pode ser feita por varredura visual ou por análise binária.
- A varredura visual envolve, apenas, ferramentas simples e observação humana.
- A análise binária exige ferramentas de interpretação específicas.
- O volatility faz análise binária de dumps de memória oriundos de GNU/Linux (incluindo Android), MS Windows e OS X.

Análise binária com volatility

- Com a análise binária é possível obter diversos dados sobre o sistema operacional como processos ativos, conexões de rede, usuários logados, além da extração de arquivos diretamente da memória.
- A análise binária só será possível se o dump de memória for feito a partir da máquina ligada e tendo sido operada pelo suspeito.
- Também é possível analisar arquivos de hibernação.
- Demonstração do volatility...

Sumário

- Modelo von Neumman
- Estrutura básica de memória
- Arquivos de swap e de hibernação
- Persistência das informações
- Dump de memória
- Análise binária com volatility
- **Análise visual**
- Conclusão

Análise visual

- A análise visual depende da criatividade e persistência.
- Muitas vezes é baseada em palavras-chave.
- Poderá ser feita a partir de qualquer dump, mesmo que este tenha sido obtido a partir de uma máquina inicialmente desligada.
- É possível periciar arquivos de swap e hibernação.
- Ferramentas como strings, egrep, hexedit e mcview facilitam o processo.
- Cuidado com strings: ele remove caracteres acentuados.
- Demonstração...

Sumário

Conclusão

- Na perícia digital, a memória virtual é um campo rico e fértil para as mais variadas buscas.
- As análises binária e visual poderão ser combinadas.
- A análise binária dependerá das condições de coleta da RAM.
- Poderão ser analisados arquivos de swap e hibernação.
- Cuidado ao utilizar máquinas públicas.
- Não venda smartphones e tablets usados!

Esta palestra está disponível em:

http://eriberto.pro.br

Siga-me no Twitter @eribertomota