ارائه فایل سیستم امن مبتنی بر TPM با پشتیبانی گروه

ارائه دهنده: امین سرده مقدم

مقدمه

- امنیت داده موضوع مهم جهان امروز
- امنیت داده در فایل سیستم
- طرح های مختلف برای فراهم کردن امنیت (استفاده از الگوریتم های رمزنگاری)
- مزیت استفاده از روش های رمزنگاری
- پیاده سازی به صورت نرم افزاری
- استفاده از سخت افزار در طرح پیشنهادی
- طراحی شده برای کاربران خانگی

3

کارهای مشابه

- CFS:
  - ارائه شده در سال ۱۹۹۳
  - مبتنی بر NFS
  - پیاده سازی در سطح کاربر
  - مشکل کارایی
  - سطح امنیتی پایین
  - تنها برای یک کاربر

4

کارهای مشابه

- TCFS:
  - پیاده سازی در سطح کرنل
  - کارایی بهتر
  - توانایی کار کردن با فایل سیستم های راه دور
  - دسترسی گروهی به منابع رمز شده
  - تکیه بر کلیدهای عبور ورود و ذخیره کلیدهای رمزنگاری روی دیسک
  - محدود به کرنل نسخه ۲.۲.۱۷ و پایین تر
  - مبتنی بر NFS

5

کارهای مشابه

- EFS:
  - ارائه شده توسط مایکروسافت
  - استفاده از روش های احراز اصالت و ACL ویندوز
  - ذخیره کلیدها روی دیسک در جعبه قفل رمز شده با کلمه عبور کاربران
  - رمزنگاری مجدد این جعبه قفل در صورت کلمه عبور کاربر
  - قابل دسترس نبودن اطلاعات در صورت تغییر کلمه عبور همه کاربران توسط مدیر سیستم

6

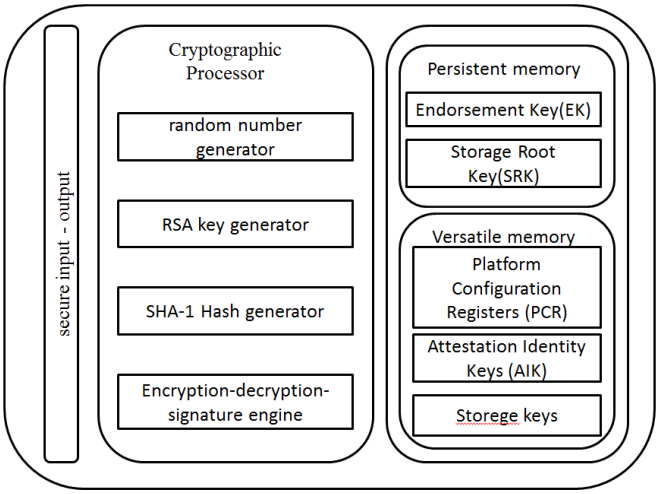
کارهای مشابه

- Transcrypt:
  - طراحی در سطح کرنل
  - رمزنگاری شفاف
  - مدیریت کلید قوی
  - سهولت در دسترسی به داده
  - کوچک کردن محدوده اعتماد
  - عدم پیشتیبانی از گروه
  - احتیاج به دسترس پذیری به منابع شبکه و عدم کارایی در صورت خرابی شبکه
  - ضعف در جامعیت

7

سیستم فایل امن ارتقا یافته

- معرفی TPM



8

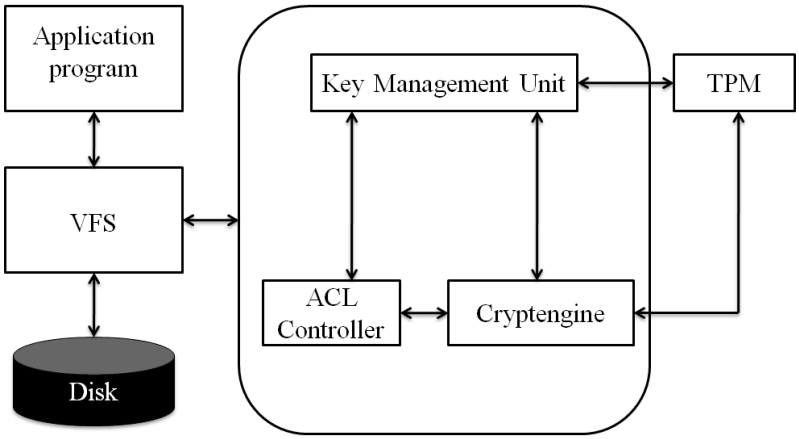
سیستم فایل امن ارتقا یافته

- اهداف
  - محرمانگی
  - جامعیت
  - کنترل دسترسی قوی
  - شفافیت
  - راحتی

9

سیستم فایل امن ارتقا یافته

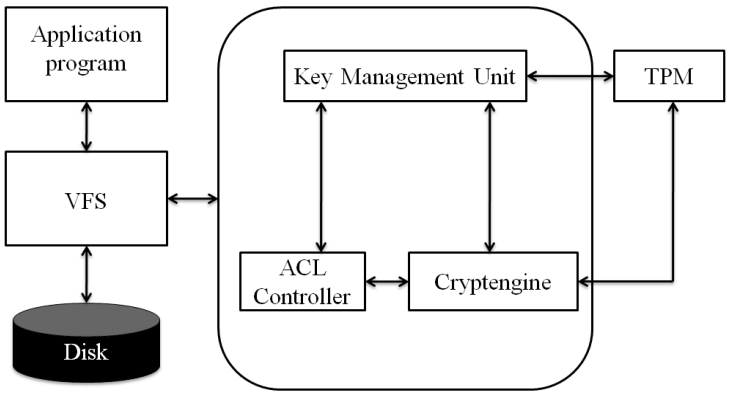
- طراحی فایل سیستم امن پیشنهادی



10

معماری سیستم فایل امن ارتقا یافته

- معماری طرح پیشنهادی



11

معماری سیستم فایل امن ارتقا یافته

- واحد مدیریت کلید
  - تهیه کلید رمزنگاری برای موتور رمزنگاری و توکن ها برای کنترل کننده لیست دسترسی
  - محاسبه HACL و DHACL و تحویل به کنترل کننده لیست کنترل دسترسی
  - تحویل کلید خصوصی کاربران از طریق یک مسیر امن

12

معماری سیستم فایل امن ارتقا یافته

- موتور رمزنگاری
  - رمزنگاری فایل با استفاده از الگوریتم Blowfish
  - صفر کردن فضایی که کلید در آن ذخیره شده است
  - آماده کردن فایل برای تحویل به VFS

13

معماری سیستم فایل امن ارتقا یافته

- کنترل کننده لیست دسترسی
  - تغییر درایه های لیست کنترل دسترسی به صورت:

User : username : rwx : token

  - اضافه کردن HACL و DHACL به لیست کنترل دسترسی
  - بررسی مجوزها برای دسترسی به فایل

14

عملیات فایل سیستم امن ارتقا یافته

- ایجاد فایل
  - ایجاد فایل توسط کاربر، ذخیره آن و انتخاب گزینه رمزنگاری
  - تغییر لیست کنترل دسترسی در صورت لزوم
  - تولید کلید رمزنگاری متقارن و توکن ها توسط واحد مدیریت کلید
  - تهیه لیست کنترل دسترسی توسط کنترل کننده لیست کنترل دسترسی
  - محاسبه HACL و DHACL توسط واحد مدیریت کلید
  - تحویل HACL و DHACL به واحد کنترل کننده لیست دسترسی
  - رمزنگاری فایل توسط موتور رمزنگاری و محاسبه درهم آن

15

عملیات فایل سیستم امن ارتقا یافته

- ایجاد فایل (ادامه ...)
  - تحویل فایل رمز شده همراه لیست کنترل دسترسی به VFS برای ذخیره روی دیسک

16

عملیات فایل سیستم امن ارتقا یافته

- دسترسی به فایل
  - تحویل فایل رمز شده به CE توسط VFS
  - جداسازی بخش های مختلف فایل شامل لیست کنترل دسترسی، درهم فایل و ...
  - محاسبه درهم جدید و مقایسه آن با درهم قبلی برای بررسی جامعیت فایل
  - تحویل لیست کنترل دسترسی به واحد کنترل کننده لیست کنترل دسترسی
  - بررسی جامعیت لیست کنترل دسترسی با استفاده از واحد مدیریت کلید

17

عملیات فایل سیستم امن ارتقا یافته

- دسترسی به فایل (ادامه ...)
  - بررسی مجوزها و تحویل توکن کاربر به واحد مدیریت
  - تحویل کلید متقارن رمزنگاری به موتور رمزنگاری
  - رمزگشایی فایل و تحویل آن به VFS

18

تحلیل و ارزیابی امنیتی

- مدل تهدید
  - حملات برون خط: دسترسی فیزیکی به دستگاه ذخیره سازی
  - حملات برخط: جستجوی حافظه برای یافتن کلید، دستیابی به کلید در هنگام انتقال به فضای کاربری و ....

19

تحلیل و ارزیابی امنیتی

- ویژگی های فایل سیستم امن ارتقا یافته
  - پیاده سازی در سطح کرنل
  - صفر شدن حافظه کلید توسط موتور رمزنگاری
  - رمز شدن کلید خصوصی با کلید عمومی کاربران(محرمانگی و احراز اصالت)
  - حفظ جامعیت لیست کنترل دسترسی
  - حفظ جامعیت فایل
  - پشتیابی از کارت هوشمند و حافظه فلش برای ذخیره کلید خصوصی
  - استفاده از الگوریتم Blowfish
  - در نظر گرفتن کاربر ارشد به عنوان کاربر معمولی

20

با سپاس فراوان از توجه شما