Threats to privacy arising in the management of data stored in Computer Systems

Gustavo Betarte

Instituto de Computación, Facultad de Ingeniería
Universidad de la República, Uruguay
www.fing.edu.uy/~gustun

Overview

- The use of any modern computer system (pc, tablet, smartphone, ...) leaves unintended traces of expired data and remnants of users' past activities

Overview

- The use of any modern computer system (pc, tablet, smartphone, ...) leaves unintended traces of expired data and remnants of users' past activities
- We put forward the issue of the unintended persistence of data stored in digital repositories

Overview

- The use of any modern computer system (pc, tablet, smartphone, ...) leaves unintended traces of expired data and remnants of users' past activities
- We put forward the issue of the unintended persistence of data stored in digital repositories
- This data can be recovered by forensic analysis, and it may pose a threat to privacy

Data preservation and analysis

- Preserving a historical record of activities and data is critical for a wide range of applications
  - To recover after system failure
  - To analyze past events after a breach
  - To audit compliance with security policies

Data preservation and analysis

- Preserving a historical record of activities and data is critical for a wide range of applications
  - To recover after system failure
  - To analyze past events after a breach
  - To audit compliance with security policies
- Intentional preservation of history can thus serve a good purpose (inexpensive storage makes it possible)

Data preservation and analysis

- Preserving a historical record of activities and data is critical for a wide range of applications
  - To recover after system failure
  - To analyze past events after a breach
  - To audit compliance with security policies
- Intentional preservation of history can thus serve a good purpose (inexpensive storage makes it possible)
- Conversely, in many scenarios, retaining a history of past data or operations can pose a serious threat to privacy and confidentiality
  - In large institutions and enterprises, systems that retain data for too long risk unwanted disclosure, for example by security breach

Data remnants

- Modern computer systems unintentionally preserve history

Data remnants

- Modern computer systems unintentionally preserve history
- It can be surprisingly difficult to remove traces of the past from computer systems

Data remnants

- Modern computer systems unintentionally preserve history
- It can be surprisingly difficult to remove traces of the past from computer systems
- Without precise control over data destruction, unwelcome remnants of past data can become a serious problem

Data remnants

- Modern computer systems unintentionally preserve history
- It can be surprisingly difficult to remove traces of the past from computer systems
- Without precise control over data destruction, unwelcome remnants of past data can become a serious problem
  - A wealth of sensitive data, including financial and medical records, have been recovered from decommissioned hard drives

Data remnants

- Modern computer systems unintentionally preserve history
- It can be surprisingly difficult to remove traces of the past from computer systems
- Without precise control over data destruction, unwelcome remnants of past data can become a serious problem
  - A wealth of sensitive data, including financial and medical records, have been recovered from decommissioned hard drives
  - Digital documents published on the Web have been found to include sensitive content believed to be deleted

Data remnants

- Modern computer systems unintentionally preserve history
- It can be surprisingly difficult to remove traces of the past from computer systems
- Without precise control over data destruction, unwelcome remnants of past data can become a serious problem
  - A wealth of sensitive data, including financial and medical records, have been recovered from decommissioned hard drives
  - Digital documents published on the Web have been found to include sensitive content believed to be deleted
  - Email was used in court cases against Enron employees and released to the public, some of which was contained in deleted items in folders

Unintended data retention
Example scenarios

- Businesses can unintentionally violate privacy regulations by leaving data in table or file storage

Unintended data retention
Example scenarios

- Businesses can unintentionally violate privacy regulations by leaving data in table or file storage
- Analysts that investigate data repositories recovered from lost or stolen computers can reveal sensitive information that was thought to be deleted

Unintended data retention
Example scenarios

- Businesses can unintentionally violate privacy regulations by leaving data in table or file storage
- Analysts that investigate data repositories recovered from lost or stolen computers can reveal sensitive information that was thought to be deleted
- Authorized investigators may recover data from equipment subpoenaed or seized from a crime scene, or simply in situations where company policy has been violated

Unintended data retention
Embedded Database storage

- Message headers and time stamps for messages believed to be deleted can be found on disk in embedded databases (*Mail.app* in *OS X*)

Unintended data retention
Embedded Database storage

- Message headers and time stamps for messages believed to be deleted can be found on disk in embedded databases (*Mail.app* in *OS X*)
- *Firefox* allows applications to store data that persists across sessions in an *SQLite* database. This storage is a sophisticated replacement for cookies, and can be a prime resource for forensic investigators to recover inadvertently retained deleted data

Data Revelation
Through forensic analysis

- Remnants of past data and activities are revealed through forensic analysis

Data Revelation
Through forensic analysis

- Remnants of past data and activities are revealed through forensic analysis
- When forensic analysis is performed by authorized investigators it can be a valuable tool, helping to hold individuals or systems accountable for malicious or mistaken actions, but

Data Revelation
Through forensic analysis

- Remnants of past data and activities are revealed through forensic analysis
- When forensic analysis is performed by authorized investigators it can be a valuable tool, helping to hold individuals or systems accountable for malicious or mistaken actions, but
- When tools and methods of forensic analysis are used by an unauthorized party, it threatens privacy

Data Revelation
Threat model

- Threats to privacy and confidentiality usually result from unintended retention of data in lower storage layers, where data is accessible through interfaces that are not controlled by the application or the database

Data Revelation
Threat model

- Threats to privacy and confidentiality usually result from unintended retention of data in lower storage layers, where data is accessible through interfaces that are not controlled by the application or the database
- Existing security threats make it impossible to ensure that users will be limited to the intended interface provided by the application or the database where is stored the data. It is necessary to consider that an intruder will have unrestricted access to storage on disk

Data Revelation
Threat model

- Threats to privacy and confidentiality usually result from unintended retention of data in lower storage layers, where data is accessible through interfaces that are not controlled by the application or the database
- Existing security threats make it impossible to ensure that users will be limited to the intended interface provided by the application or the database where is stored the data. It is necessary to consider that an intruder will have unrestricted access to storage on disk
- This models the capabilities of a system administrator, a forensic investigator, a hacker who has gained privileges on the system, or an intruder who has breached physical security

Investigation: remnant data on memory cards
Description

- Memory cards are widely used in numerous electronic devices
- Provide interfaces allowing for a large array of private and confidential data to be stored into the card
- Investigation conducted by a team of Australian researchers (Szewczyk, Sansurooah; 2011)
  - **Goal**: to determine the sensitivity, type and amount of data that remained on second hand card memory post sale
  - In 2011, 119 second hand memory cards were randomly purchased from eBay Australia
  - **Findings**: highly sensitive data is stored on memory cards and it is not destroyed prior to sale

Investigation: remnant data on memory cards
Results

- State of the cards
  - 75% had their data deleted and or formatted
  - 12% were not recoverable
  - 13% were purchased with all data intact and no sign of data deletion attempt
- Some of the information types recovered
  - driver's license together with full name, address and date of birth and photo of the driver with a luxury card
  - real state settlement documents including names, addresses and purchasing information together with copies of bank deposit cheques
  - hundreds of photographics images of an office party where the name of the company was showed and exposed photos of employees towards the end of the night

Some concluding remarks

- Digital devices provide a false view of stored data
- Tools for removing data might not be effective
- Transparency principles to improve privacy seems to be needed

References

T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum

Data Lifetime is a System Problem.
In Proceedings of ACM SIGOPS European Workshop, 2004.

M. Geiger, L. Cranor

Scrubbing Stubborn Data: An evaluation of counter-forensic privacy tools.
IEEE Security and Privacy Magazine, 4(5): 16-25, 2006.

P. Stahlberg, G. Miklau, B. N. Levine

Threats to Privacy in the Forensic Analysis of Database Systems.
In Proceedings of SIGMOD 07, Beijin, China, 2007.

W. Enck, D. Octeau, P. McDaniel,S. Chaudhuri

A Study of Android Application Security.
In Proceedings of the 20th USENIX Conference on Security, Berkeley, CA, USA, 2011.

P. Szewczyk, K. Sansurooah

A 2011 investigation into remnant data on second hand memory cards sold in Australia.
In Proceedings of the 9th Australian Digital Forensics Conference, Perth Western, Australia, 5th -7th, December 2011