Storage Jamming

Anna Suen

September 5, 2002

Preview

- Describe/define Storage Jamming
- Storage Jammer
- Terminology
- Promising Target System
- Attacker
- Model of Storage Jamming

Storage Jamming

- malicious but surreptitious modification of stored data
- to reduce the quality of stored data
- the attack deviates the state of the stored data from the authentic state

Storage Jamming

- unlike confidentiality: information flow not a central issue
- *fraud*: unauthorized flow of assets where the perpetrator is concerned with maintaining the integrity of the data as they flow the wrong way
  - storage jamming: unauthorized flow of lesser importance
    - data being destroyed at source
- *DoS*: little concern with avoiding detection
  - storage jamming: only makes sense if undetected
- lies between the boundaries of fraud, unauthorized leakage, and DoS

Storage Jammer

- assume that a Trojan horse does the storage jamming
  - can access data that attacker can't
- manual storage jamming possible
  - generally less effective

Storage Jammer's Goal

- initiator does not receive direct benefit
- indirect – reduce quality without being detected
- i.e.:
  - deteriorate the competitor's position
  - financial gain

Terminology

- *authentic values*
  - values that were intended to be stored
- *bogus values*
  - values stored by a jammer
- *jam*
  - action of storing a bogus value

Terminology (cont.)

- *lifetime*
  - number of jams the storage jammer can perform against a specific system before being discovered
  - function of the rate and extent of its jamming, specific user population, and seriousness of its impact on the real world

Promising Target

- systems with complex stored data
  - authenticity can't be determined by inspection
  - i.e. – legacy systems, distribution and inventory systems, simulations, data warehouses, command and control systems
- promising hosts: data-creating application programs that don't have high assurance

The Attacker

- expects the bogus state will affect the victim's performance of some real-world task
- does not want victim to experience a catastrophic failure
- expects victim won't detect bogus data and will continue to use damaged data for a long time

The Attacker

- occasionally write wrong, but plausible data
  - via the application program that generates authentic data
- more conventional security techniques generally not useful
  - i.e.: access control, cryptography, intrusion detection

Model of Storage Jamming

- adopt the Unity model of computation
  - “Towards a Model of Storage Jamming” (McDermott and Goldschlag)
  - ???

Papers

- **Storage Jamming**, 1996
  - John McDermott, David Goldschlag
  - *Database Security IX: Status and Prospects*
- **Towards a Model of Storage Jamming**, June 1996
  - John McDermott, David Goldschlag
  - *Proceedings of the Ninth Computer Security Foundations Workshop*
- **Doc, Wyatt, and Virgil: Prototyping Storage Jamming Defenses**, 1997
  - J. McDermott, R. Gelinas, S. Ornstein
- **Practical Defenses Against Storage Jamming**, 1997
  - J. McDermott, J. Froscher

To learn more about...

- Unity Model
  - Chandy and Misra. *Parallel Program Design: A Foundation*.
- Information Warfare
  - Ammann, Jajodia, McCollum, and Blaustine. Surviving information warfare attacks on databases. *Proceedings of the IEEE Symposium on Research in Security and Privacy.*