Storage Jamming

John McDermott & David Goldschlag
Naval Research Laboratory

Anna Suen

August 5, 2002

Preview

- Definition of Storage Jamming
- Jamming Characteristics
- Vulnerability to Jamming
- Reducing Vulnerability
- Anti-Jamming
  - Detection Mechanisms
  - Commingled-Object Detection
  - Quarantine Approaches

Storage Jamming

- malicious modification of stored data to disrupt or degrade an organization's operations
  - aka. attacking, hacking, intruding, etc…
- jammer's goal:
  - to reduce the quality of stored data without being detected

8/5/02 3

Assumptions

- exclude user mistakes and software flaws
- easy to stop jamming once it is detected

Definitions

- *bogus values* – values introduced into storage by the jammer
- *authentic values* – values we meant to store

8/5/02 4

Jamming Characteristics

- Persistence of Bogus Values
  - changes can be persistent or restored after an arbitrary length of time
  - *repeat-back jamming* – save deleted objects/values and reintroduce them later
- Security Attributes of the Jamming Program
  - jammer may be an authorized or unauthorized program

8/5/02 5

Jamming Characteristics (cont.)

- Target System Structure
  - harder to detect jamming in poorly structured system
  - modularity and encapculation in well-structured system
    - isolate the effects of bogus data to a single part of the system
    - easier to determine that the source of the system error was bogus data

8/5/02 6

Jamming Characteristics (cont.)

- Means of Choosing Bogus Values
  - arbitrary
  - random
  - interpolated
  - replayed
  - permuted
  - etc…
- Means of Choosing Target Data Items
  - randomly
  - via some selection criteria
  - by piggybacking on an application program

8/5/02 7

Jamming Characteristics (cont.)

- Class of Target Data
  - application data, linkage data, metadata, system data
  - level of abstraction of target data items
    - i.e., units of target data could be data in a relational database or disk blocks in the nodes of a B+ tree
  - size or granularity of target data items
    - sets of data
    - components of a data item

8/5/02 8

Jamming Characteristics (cont.)

- Rate of Change in Target Data
  - if there are many updates to the data, then jamming may be easier
- Rate of Jamming
  - jam as fast as possible without being detected
  - run continuously, making changes infrequently

8/5/02 9

Jamming Characteristics (cont.)

- Extent of Jamming
  - barrage jamming – jamming widely but slowly
  - spot jamming – jamming by only modifying a critical subset of the stored data
- Adaptability of the Jammer
  - ability to adapt to detection mechanisms

8/5/02 10

Jamming Characteristics (cont.)

- Means of Introducing the Jammer
  - via network
  - installed during software development
  - installed separately after an information system is deployed
  - via firmware

8/5/02 11

Vulnerability to Jamming

- Interceptibility
  - a measure of the ease with which an enemy can determine the existence, function, and location of a system
- Accessibility
  - a measure of the ease with which an enemy can reach a system with an effective electronic warfare attack
- Susceptibility
  - a measure of system properties that determines the effect of attacks on the system's performance

8/5/02 12

Susceptibility

- This paper's primary concern
- Important criteria: detection of jamming
  - if jamming is detected, then we can assume that the jammer will cease to be effective
  - a system that easily detects jamming is not susceptible to the jammer

8/5/02 13

Reducing Vulnerability

- Follow certain general system engineering practices
  - reduces vulnerability
  - do not really address the problem
- Adopt specific anti-jamming techniques
  - more effective way to reduce vulnerability

8/5/02 14

General Software & System Engineering Practices

- System should be well-designed
- System data should be designed
- System behavior should be specified
- Major state transitions should be transactional

8/5/02 15

General Software & System Engineering Practices (cont.)

- Use commercial data management products for data storage
- Use fault tolerance techniques to increase the difficulty of jamming data
- Use computer security techniques to increase the difficulty of jamming data

8/5/02 16

Anti-Jamming

- Detection Mechanisms
- Commingled-Object Detection
- Quarantine Approaches

8/5/02 17

Detection Mechanisms

- Background systems to detect jamming in a timely fashion
- Strategy:
  - arrange the data storage in such a way that jamming changes are easily detected
- Mechanisms:
  - specialized data integrity constraints
  - multi-process multi-domain transactions
  - detections objects

8/5/02 18

Mechanisms

- Specialized data integrity constraints
  - simplify detection due to checking efficiency
  - difficult for jammer to create bogus values that satisfy them
- Multi-process multi-domain transactions
  - structure updates, deletes, etc. such that no single process could determine bogus values
- Detection objects
  - data structures that appear to be part of an application, but are not used

8/5/02 19

Detection Objects

- always remains in a predictable state
  - if not, then probably modified by a jammer
- correspond to *protected data items*
  - data items intended to store legitimate data

8/5/02 20

Detection Object Properties

- Indistinguishability
  - to the jammer, detection objects are indistinguishable from their corresponding protected data items
- Sensitivity
  - only the jamming detection process is allowed to modify detection objects

8/5/02 21

Detection Objects (cont)

- If a detection process inserts enough detection objects into the storage structures of an information system, an active jammer will eventually jam one of the detection objects and be detected.
- Only protect the sets of data to which they correspond

8/5/02 22

Commingled-Object Detection

- only the detection process determines if the data item is a detection object
- detection process installs detection objects
  - some attribute is recorded to identify it as a detection object
- detection objects interspersed with protected data items

8/5/02 23

Commingled-Object Detection

- Strategy:
  - detection process resets all detection objects to the proper state
  - run the programs to be scanned
    - should set the detection objects to another proper state
  - if detection objects not in expected state, then there may be jamming
- less effective against slow jammers

8/5/02 24

Quarantine Approaches

- Three types:
  - Quarantine System
  - Quarantine Subsystem
  - Quarantine Application

8/5/02 25

Quarantine System

- most powerful detection mechanism
- a copy of the system to be protected
  - has all the programs that run on the protected system
- will detect slow jammers, random bit-level barrage jammers, spot jammers, programs that jam by changing data outside their own application, and programs that jam by deliberately writing incorrect values

8/5/02 26

Quarantine System

- Strategy:
  - not need to distinguish detection objects from protected data items
  - after an update, the detection process will be able to detect any bogus change to any part of each table

8/5/02 27

Quarantine Subsystem

- like quarantine system, except it runs on same hardware as the operational system it protects
- advantage: allows each site to have different software installed
- disadvantage: operational system must be able to support it

8/5/02 28

Quarantine Application

- like a partial quarantine subsystem
- runs a script against the programs, data definitions, metadata, etc of a single application instead of using all the programs and data definitions of the operational system

8/5/02 29

Detection Objects in the System Life Cycle

- detection objects
  - designed and implemented late in a system's life cycle
- background detection process
  - designed and integrated as early as possible in a system's life cycle

8/5/02 30

Review

- Definition of Storage Jamming
- Jamming Characteristics
- Vulnerability to Jamming
- Reducing Vulnerability
- Anti-Jamming Techniques
  - Detection Mechanisms
  - Commingled-Object Detection
  - Quarantine Approaches

8/5/02 31

Question

- Can anti-jamming techniques be used to protect against fraud?

8/5/02 32