

# Practical Defenses Against Storage Jamming

*J. McDermott and J. Froscher*

Anna Suen  
October 1, 2002

## Preview

- Review & Terminology
- Classes of Attacks
  - External Jammer
  - Internal Jammer
- Defenses
  - Cryptography
  - Detection Objects
  - Replay Defense
  - Replication Defense

2

## Review

- Storage Jamming
  - malicious but sneaky modification of stored data
  - to reduce the quality of stored data
- Goal for the initiator
  - does not receive direct benefit
  - indirect – reduce quality without being detected
    - i.e.: deteriorating the position of the competitor

3

## Review

- assume Trojan horse does the storage jamming
  - can access data that the attacker cannot
- all the jammer has to do is write wrong, but plausible data
  - via the application program that generates authentic data
- assume that a detected jammer can be removed

4

## Terminology

- *authentic values*
  - values that were intended to be stored
- *bogus values*
  - values stored by a jammer
- *jam*
  - action of storing a bogus value
- *the storage object has been jammed*
  - when the storage object contains a bogus value

5

## Classes of Attacks

- **Internal Jammer**
  - only targets objects that have been accessed at the request of a user
  - harder to construct, but more problematic
    - use its host program's logic and security privileges to avoid detection objects or encryption
- **External Jammer**
  - targets any objects that are accessible in its current context

6

## Defenses

- Ineffective defenses
- Cryptography
- Detection Objects
- The Replay Defense
- Replication Defense

7

## Ineffective Defenses

- Audit Mechanisms
  - fine granularity attacks are undetected
- Intrusion Detection
  - avoided by fine granularity attacks
- Data Integrity Checks (checksums)
  - attack can occur before integrity check
- Replication
  - jamming software can replicate bogus values

8

## Cryptography

- Digital Signatures
  - bogus values can be inserted prior to signing
  - like checksums
- Threshold Schemes
  - suppose that data values are already known before the separate shadows are constructed
  - jammer has access to the data-generating application logic
    - can supply bogus values as input to the threshold scheme
  - can't be incorporated into large information systems
    - integration and performance reasons

9

## Cryptography

- Encryption
  - prevents jammer from reading or modifying data
  - NRL created a Trojan horse
    - jams an encrypted database without attacking its cryptographic system



### NOTE:

Careful encryption defense will stop many external jammers

- investigate low-overhead cryptographic schemes or protocols that will defeat external jammers

10

## Detection Objects

- copies of authentic data that appear to be part of the application, but aren't used
- to jammer – appear to be authentic data
- only detection process makes authentic changes
  - change from one precomputed state to another
  - if not in precomputed state, then it was probably jammed

11

## Detection Objects

- Two properties:
  - Indistinguishability
    - jammer can't tell the difference between detection objects and storage objects
  - Sensitivity
    - only the detection process is allowed to modify detection objects

12

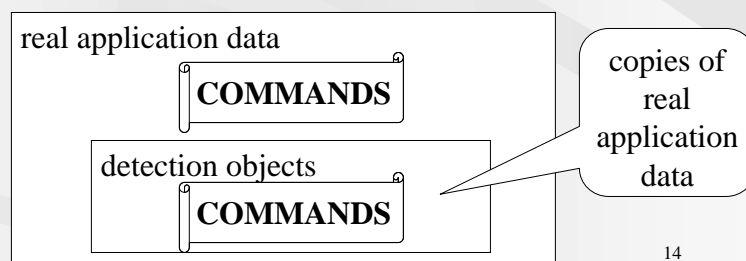
## Detection Objects

- internal jamming – problem for detection object defenses
  - if application containing an internal jammer never accesses detection objects
    - internal jammer never accesses detection object
  - if allow applications to access detection objects
    - integrity of application will be compromised
- Solution:
  - create separate subsystem that contains nothing but detection objects
  - replay defense

13

## The Replay Defense

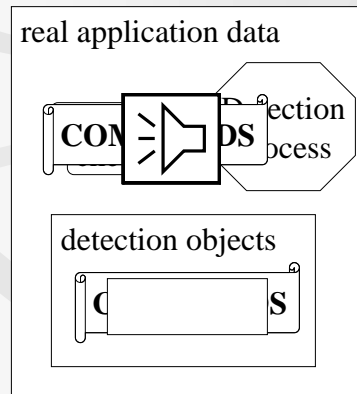
- commands are saved in a script as they are executed against real application data
- recorded commands are played back against a separate set of detection objects



14

## The Replay Defense

- Detection process:



1. After running the script, a checksum is computed on the detection objects.

2. Detection Process: checks the current state of the real application data against the checksum.

3. If the checksum matches, okay to run the new commands. Otherwise, alarm.

15

## The Replay Defense

- not necessary to verify either the replay script or the host program
  - jammers present during the creation of the script will have difficulty remaining synchronized with the contaminated script
- does not need to be applied to all data in the system
  - a subset is enough
- does not need to be running all the time
  - storage jamming is a continuous attack

16

## Replication Defense

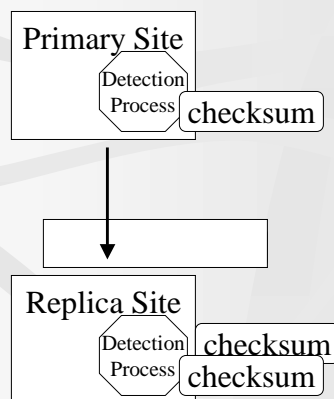
- architecture-specific
- in contrast to the replay defense:
  - no detection objects
  - updated through logical updates<sup>1</sup> submitted to applications with distinct provenances<sup>2</sup>

<sup>1</sup> *logical updates*: the change is transmitted as the text of the command that computes the new value (vs. physical updates – transmitted as a value)

<sup>2</sup> *provenance*: n. the place of origin, as of a work of art (Webster's Desk Dictionary, 1990 ed.) 17

## Replication Defense

- Detection process:



1. Primary site: After making changes to data, detection process computes checksum and sends it to each replica site.

2. Replica site: After logical update, detection process computes checksum and compares.

3. If there's a difference in the checksums, then there's a problem. 18

## Replication Defense


- challenges:
  - maintain a distinct provenance for the protected applications at each replica site
    - in theory, possible
    - in practice, some software may have commonality
  - prevent coordination between jammers at different sites if distinct provenance fails
    - hard for attacker to preserve one-copy serializability over all jams (hard for multiple jammers to coordinate over their bogus updates)

19

## Replication Defense

- advantage: can continue operations while under attack
  - at least one replica is authentic
  - can use authentic copy to recover from the attack

20



## Research Ideas

- investigate low-overhead cryptographic defenses
- investigate architectures that allow easy removal of malicious code

21

## Review

- Review & Terminology
- Defenses against storage jamming
  - Cryptography - ineffective
  - Detection Objects – only external jammer
  - Replay Defense – external & internal
  - Replication Defense – external & internal

22

# Questions?



23