Intrusion Tolerant IDS

James Riordan
Marc Dacier
Dominique Alessandri
Andreas Wespi
IBM Forschungslaboratorium
Rüschlikon, Switzerland

19 June 2001
MAFTIA

A European project whose aim is to develop:
- Malicious- and
- Accidental-
- Fault
- Tolerance for
- Internet
- Applications

In short: apply and develop dependability methods with respect to a malicious fault model.
Maftia Details

Maftia is a three year project with partners:

- University of Newcastle (UK)
- Universidade de Lisboa (P)
- DERA, Malvern (UK)
- Saarland University (D)
- LAAS-CNRS, Toulouse (F)
- IBM, Zurich (CH)
What is Intrusion Detection?

**Intrusion Detection** concerns the set of practices and mechanisms used towards detecting security errors and failures and diagnosing intrusions and attacks.

That is to say that ID is error detection and fault diagnosis with respect to a malicious fault model.
IDS and MAFTIA

Three addressed views of IDS and MAFTIA:

• How does the Intrusion Detection System help provide dependability for the entire system? ✓

• How does one build a dependable Intrusion Detection System?

• Do the other dependable components help for the Intrusion Detection System? ✗
Fault Injection

Fault Injection against
- Accidental misconfiguration
- Coarse scale attacks

IDS
Analysis
Attack Engine
Sensor
Target
Indications
Redundant Monitoring
Differential Observation

Compare snapshots of networks and machines

- NSA
- nmap
- Tripwire
Integration with Security Scanners

Integrate IDS with security scanner towards

- Reduction of false positives
- Greater context for true positives
- Fault injection ✓
- Differential observation ✓
Channels

Sender → Receiver

Sender → Filter → Receiver

Sender → Receiver
Channels

May be subject to event:

- Deletion
- Insertion
- Alteration

We need integrity, authenticity, QoS, and liveness.
Channels

So we can add to an event stream \( \{E_i\} \):

- Hash chaining
  \[ C_i = \mathcal{H}(C_{i-1}, E_i) \]
- Authentication codes
  \[ C_i = \mathcal{H}(S, C_{i-1}, E_i) \]
- Heart beat
  \[ \text{do \{sleep 60; log "beep";\}} \]
Conclusion

Dependability methods provide valuable insights into effective Intrusion Detection