1. Problem: Timing Channels

- Suppose an adversary has compromised a machine and is trying to *exfiltrate a secret* without raising suspicion.
- One way to do this is via a **covert timing channel**. A compromised host manipulates the timing of transmitted packets, e.g., inter-packet delay (IPDs), to encode the secret. Many different encodings have been proposed in the literature, e.g., TRCTC, MBCTC, ...
- **Receiver:** Decodes leaked information by analyzing observed IPD patterns.
- A system administrator wants to **detect** this.

2. State of the art

- State-of-the-art detectors assume that legitimate and covert IPDs can be distinguished by distribution *shape* statistics and/or *regularity* statistics.
- Statistics-based covert channel detection has inherent limitations:
  - The estimation of legitimate IPDs can be **inaccurate**.
  - Channels can use a **low rate** to avoid traffic distortion.
  - Building a **general detector** is hard because the adversary can easily come up with new encodings.

3. Our approach: TDR

   - **Key insight #1:** Rather than looking for specific, known channels, we can compare the message timing to what it should be if the machine is not compromised.
   - **Key insight #2:** How do we know what the timing should be? **Predicting** is hard, but all we really need to do is **reproduce** it.

   We propose **Time-deterministic replay (TDR):**

   A variant of deterministic replay that reproduces not only the functional behavior of a program, but also its precise timing.

4. Challenge: Time noise

   - Execution time depends on many factors: cache effects, interrupts, ...
   - Result: non-deterministic timing ("time noise")
   - **Our TDR prototype,** Sanity, **eliminate or mitigate** various sources of time noise.

5. Evaluation

   - **How well can Sanity reduce time noise?**
     - Experiment: Run SciMark2 with Oracle JVM and with Sanity.
     - Sanity’s time noise is **orders of magnitude lower** (0.08%-1.22%).
   
   - **How well can Sanity reproduce packet timing?**
     - Experiment: Run 100 one-minute NFS traces and compare replay IPD against play IPD.
     - Sanity’s IPDs during replay are within **1.85%** of the original IPDs (97% of IPDs are within 1%).
   
   - **How well can Sanity detect covert timing channels?**
     - Experiment: Four covert channels and four other statistics-based detectors. Each combination has at least 50 one-minute NFS runs with cross-validation.
     - Not surprisingly, statistical-based detectors have difficulties with the more advanced covert channels.
     - Sanity achieves **perfect detection** (AUC=1) for all four covert channels, including the ‘**needle in a haystack**’. 

---

*This work was partially supported by the National Science Foundation through grants CNS-1056140 and CNS-1056486.*