Paper Review Title**: InkTag: Secure Applications on an Untrusted Operating System,** O. Hofmann, S. Kim, et., al

Reviewer: swayanshu shanti Pragnya

1. Summarize the (at most) 3 key main ideas.

The paper is all about the design and implication of a virtualization based architecture which can provide strong safety with the presence of malicious operating system

1. Design over view of "para-verification"
2. System interactions which can provide trustworthy and safe operating system.
3. Ink tag which can create consistency for securing data and metadata

2. State the main contribution of the paper

The primary contributions are-

1. Methods of Recoverability from system crashes
2. Para-verification to check the authenticity of operating system
3. **In-tag which can help to run useful applications in operating system**
4. They tried to secure the operating system by using in-tag

3. Critique the main contribution

3.a. Rate the significance of the paper on a scale of 5 (breakthrough), 4 (significant contribution), 3 (modest contribution), 2 (incremental contribution), 1 (no contribution or negative contribution). Explain your rating in a sentence or two.

It is a significant contribution so I would rate as 5 because the in-tag includes the following features-

1. **Security of operating system**
2. **Verifying operating system**
3. Control flow integrity
4. Process and access control methodology
5. **Basic memory isolation**

1. ***b. Rate how convincing is the methodology: do the claims and conclusions follow from the experiments? Are the assumptions realistic? Are the experiments well designed? Are there different experiments that would be more convincing? Are there other alternatives the authors should have considered? (And, of course, is the paper free of methodological errors.)***

Most of the methodologies are convincing which includes the following majors,

1. **In-tag security guarantees**:

- ✓ synchronization between OS managed data and hypervisor-data
- ✓ Applications can fork(), exec() so process control

- ✓ Access control and naming with File i/O
- ✓ OS cannot change registers or program counter so control flow integrity

2. **Basic memory isolation:**

   - ✓ Match page table updates and requests from applications
   - ✓ Interposes on page table updates

3. c. What is the most important limitation of the approach?

Though it's a brilliant paper but still have few limitations like,

1. Interpreting low level page tables
2. The pointer results must be validated by applications
3. Mapping of memory
4. Communication with hypervisor
5. Problem in handling the interaction gap between application and hypervisor

4. Rate the writing in the paper on a scale of 5 (great) to 1 (muddled), and justify your ranking. Did you have to re-read sections? Were algorithms clearly explained? Did the paper have a logical flow?

Writing-5

Its really a good paper as the major issue of security of operating system can be solved by this in-tag architecture.

The paper had a structural flow and proper explanation of methodology like starting from the paper objective, recovery methodology, limitations, future work for improvising the performance and correctness are well explained.

As the authors clearly explained the design, implementation and method behind each protocol, it's easy to understand the logic & architecture.

Proper implementation of methodology and validation is the key attraction of the paper.

5. Answer one of the following three questions (whichever is most relevant for this paper):

1. What lessons should system researchers and builders take away from this work?2. What is the lasting impact of this work? 3. What (if any) questions does this work leave open?

By answering the question 1 these are the following points which researchers can work further,

1. Verification accuracy for system calls

2. High performance authenticity on operating system

3. Additional features to block malicious applications from operating system

4. Managing the memory efficiency