

# RansomAir Filled with Clouds

Dusko Pavlovic, University of Hawaii

C3E, 23 October 2017, Atlanta GA

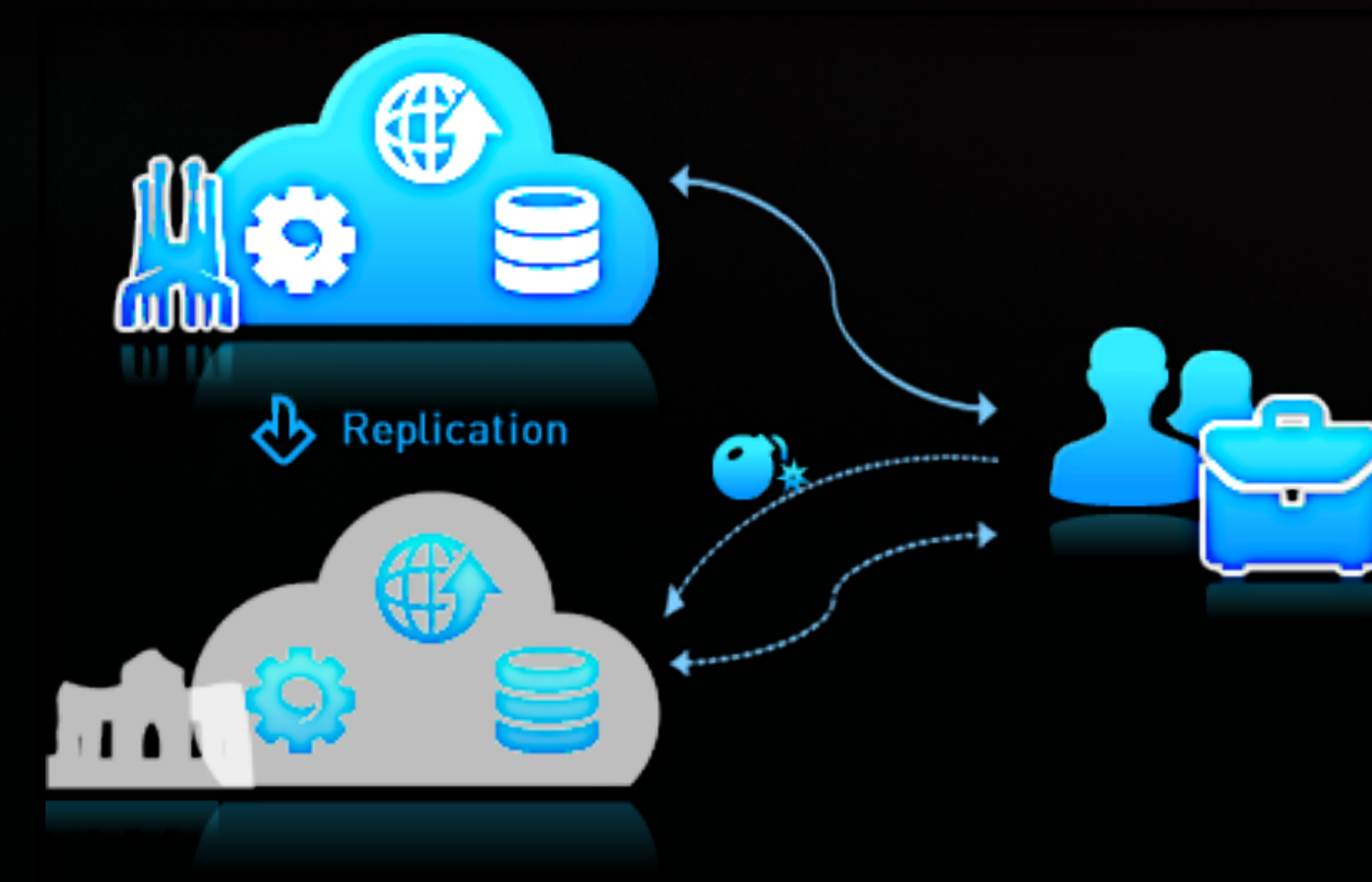
- Problem: ransom attacks



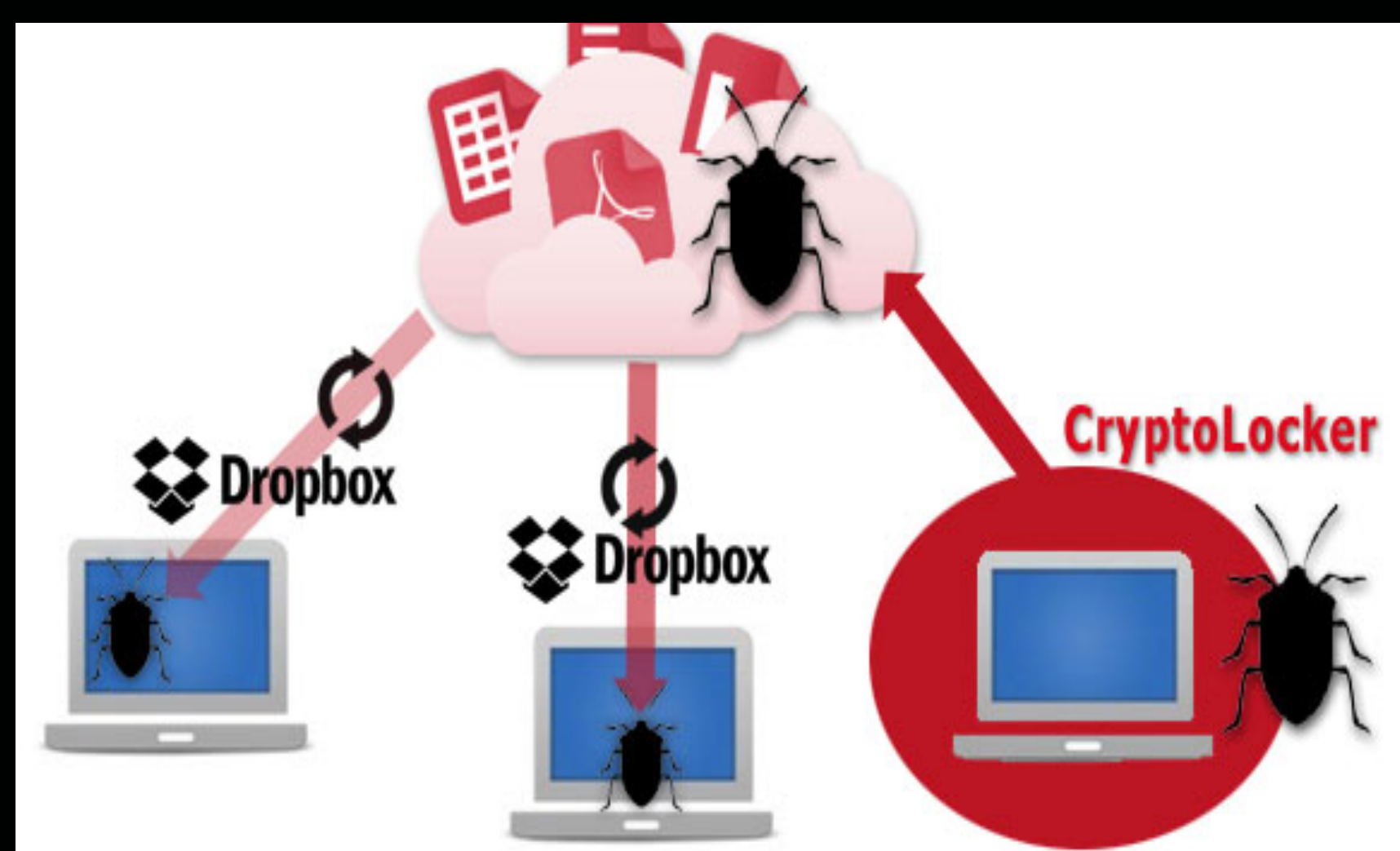
- Insight: data are different



- Solution: cloud storage



- PROBLEM: cloud security

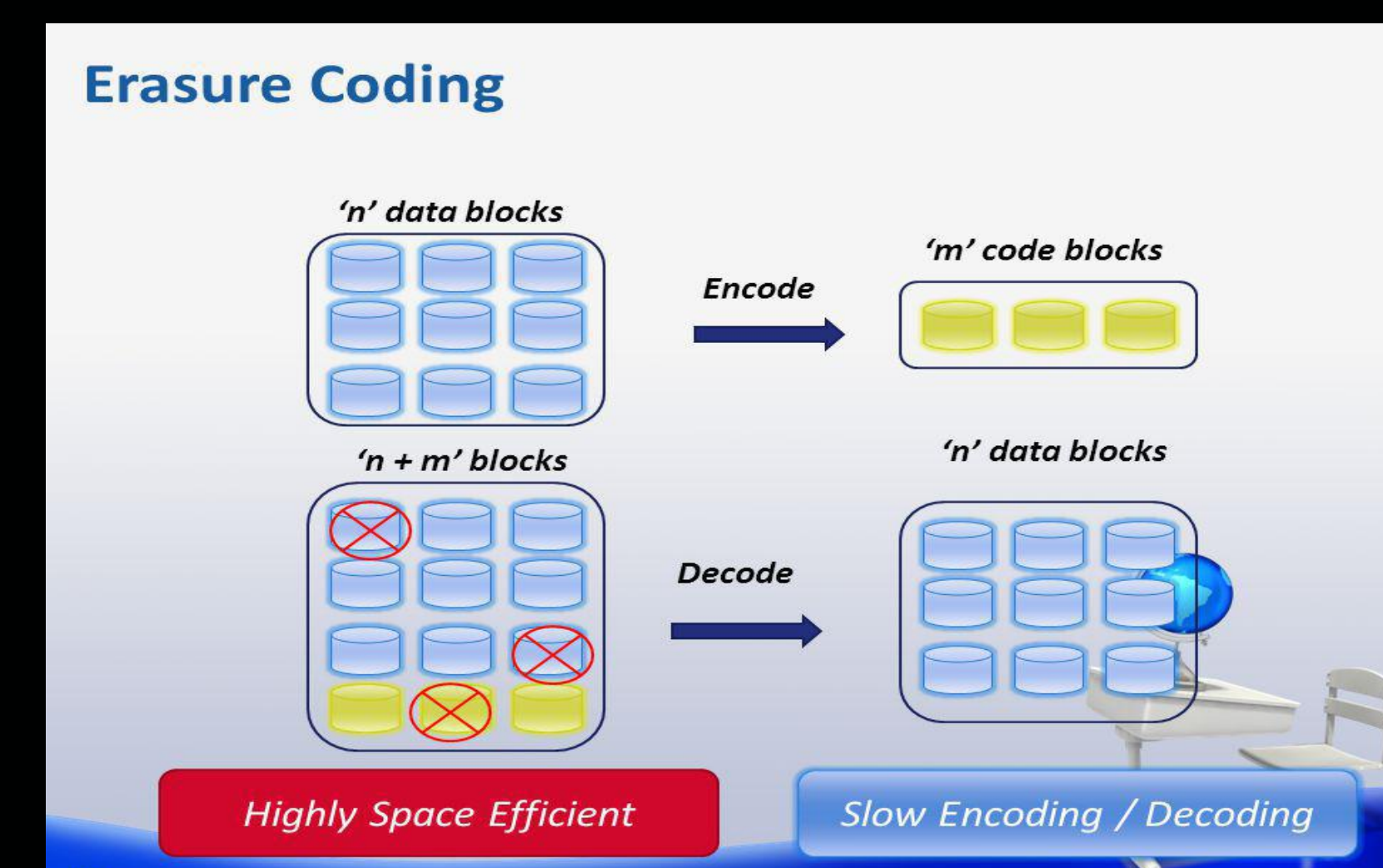


Even lightweight encryption incurs **slowdown**

- INSIGHT: slow recovery ok

- crypto requires ongoing fast decryption
- data attacks are not ongoing
- data recovery is rarely needed

- SOLUTION: code, not crypto



Coding incurs **speedup**

- SOLUTION: deletion channel security

Encoding (using sudoku)

4	6	5	3	1	7	2	9	8
9	8	7	6	4	2	3	5	1
1	3	2	8	5	9	7	6	4
8	5	9	4	7	3	1	2	6
6	7	3	2	8	1	5	4	9
2	1	4	9	6	5	8	7	3
7	9	1	5	3	4	6	8	2
5	4	6	1	2	8	9	3	7
3	2	8	7	9	6	4	1	5



4317287411268916322145154651732874

Decoding

4		3	1	7	2			
	8	7		4				1
1		2					6	
8		9				1	6	
	3	2						
2	1	4		5				
		1	5		4	6		
5			1					7
3	2	8	7		4			



4	6	5	3	1	7	2	9	8
9	8	7	6	4	2	3	5	1
1	3	2	8	5	9	7	6	4
8	5	9	4	7	3	1	2	6
6	7	3	2	8	1	5	4	9
2	1	4	9	6	5	8	7	3
7	9	1	5	3	4	6	8	2
5	4	6	1	2	8	9	3	7
3	2	8	7	9	6	4	1	5

Eavesdropping

4317287411268916322145154651732874  $\rightsquigarrow$   $\Pr(\text{guess 45 digits}) = 9^{-45}$



Computational Cybersecurity in Compromised Environments  
2017 Fall Workshop | October 23-25, 2017 | Atlanta, Georgia