

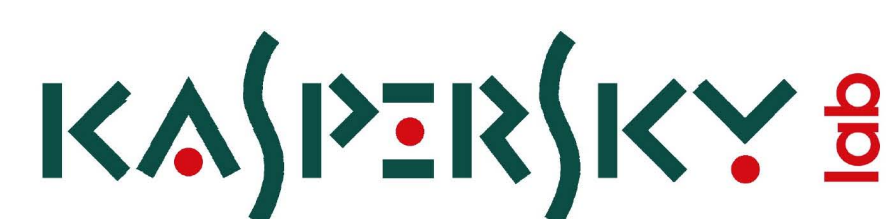
Protecting Data with Forensics Just-in-Time(FoJiT)

Christopher N. Gutierrez, Eugene H. Spafford, Saurabh Bagchi, and Thomas Yurek

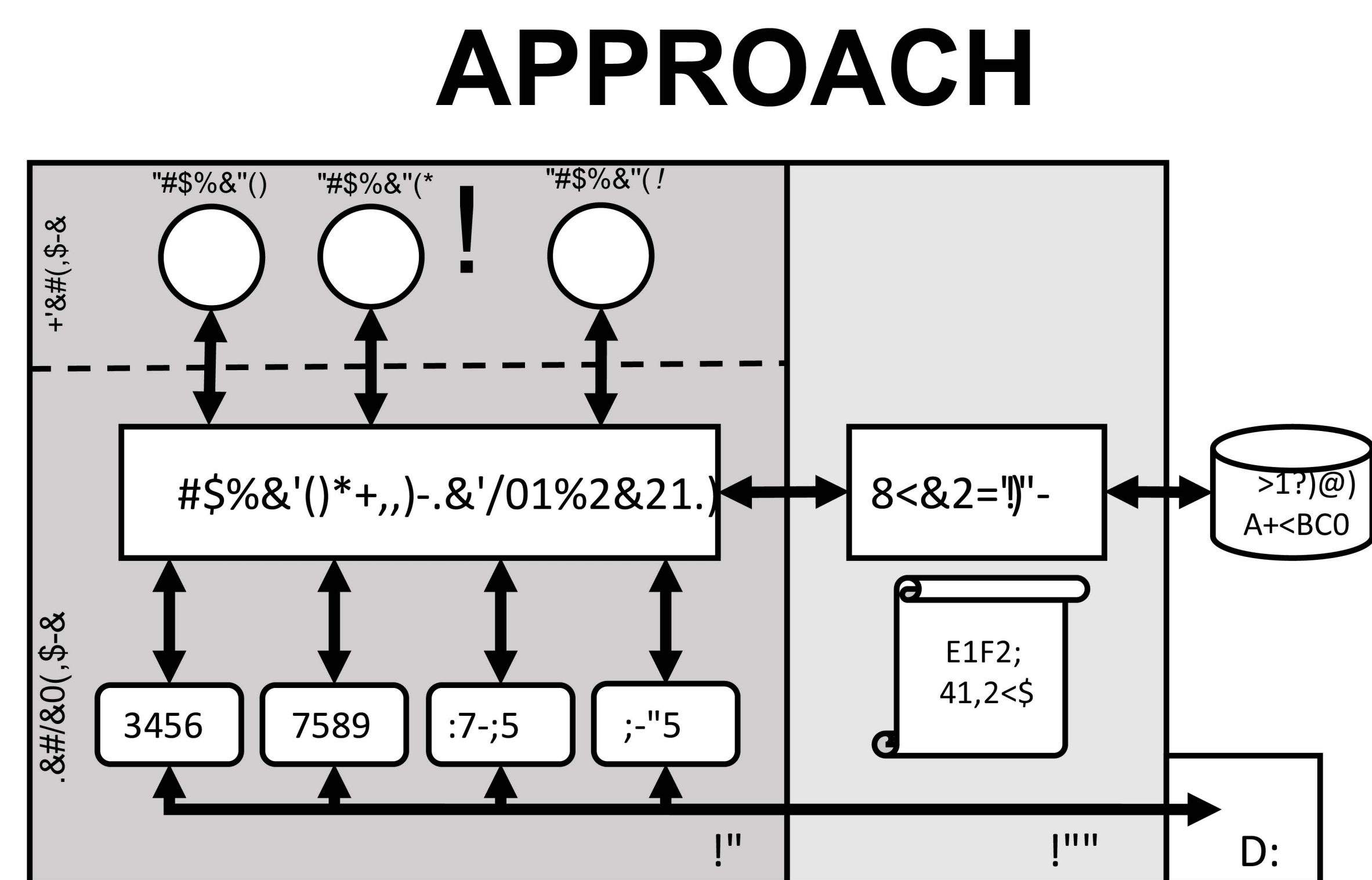
PROBLEM



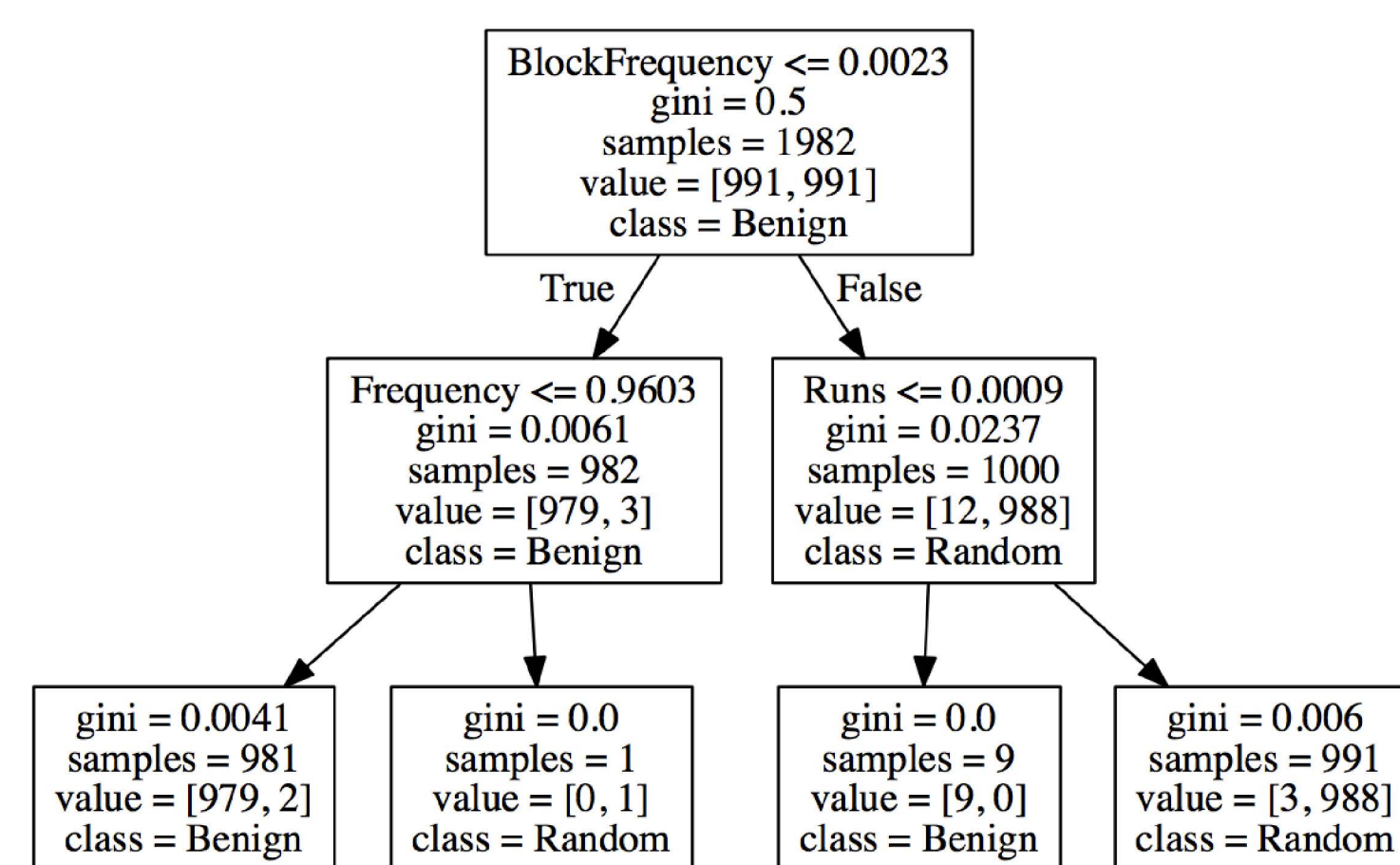
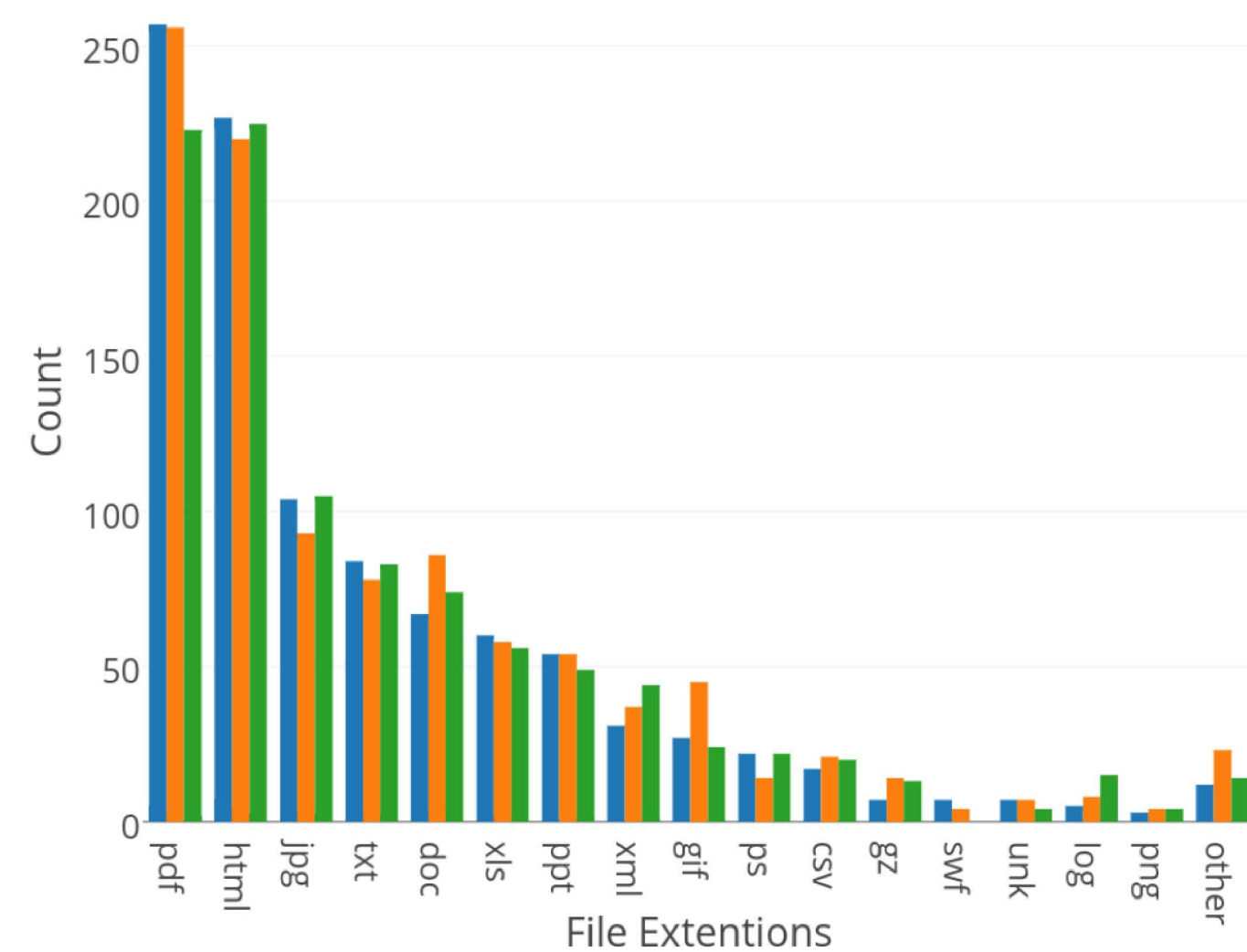
DESTRUCTIVE STONEDRILL
WIPER MALWARE ON THE LOOSE
 by Michael Mimoso March 6, 2017



TRICKY LOCKY RANSOMWARE
ROBS AMERICAN HOSPITALS
 by Kate Kochetkova March 25, 2016



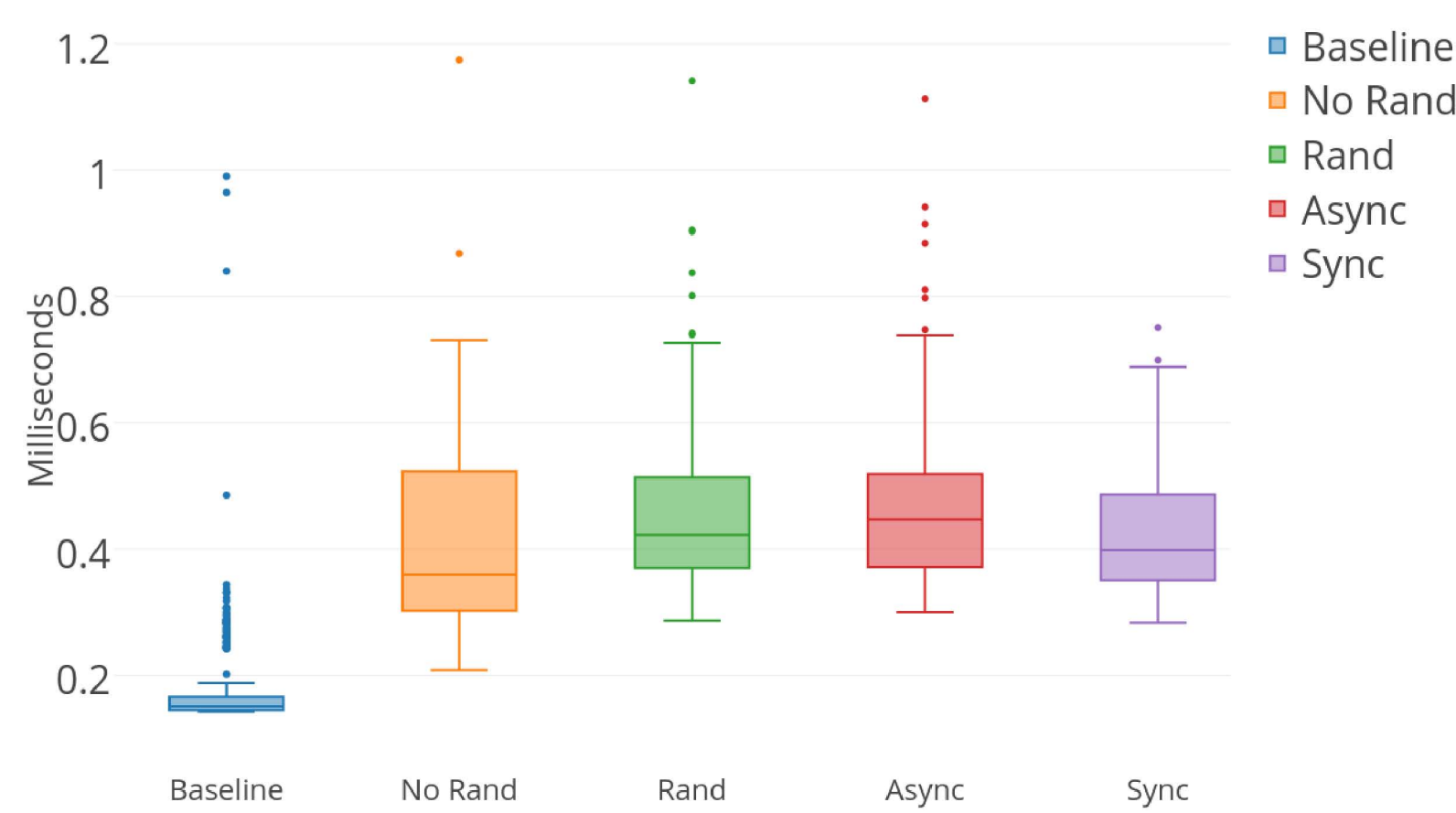
Preliminary Results



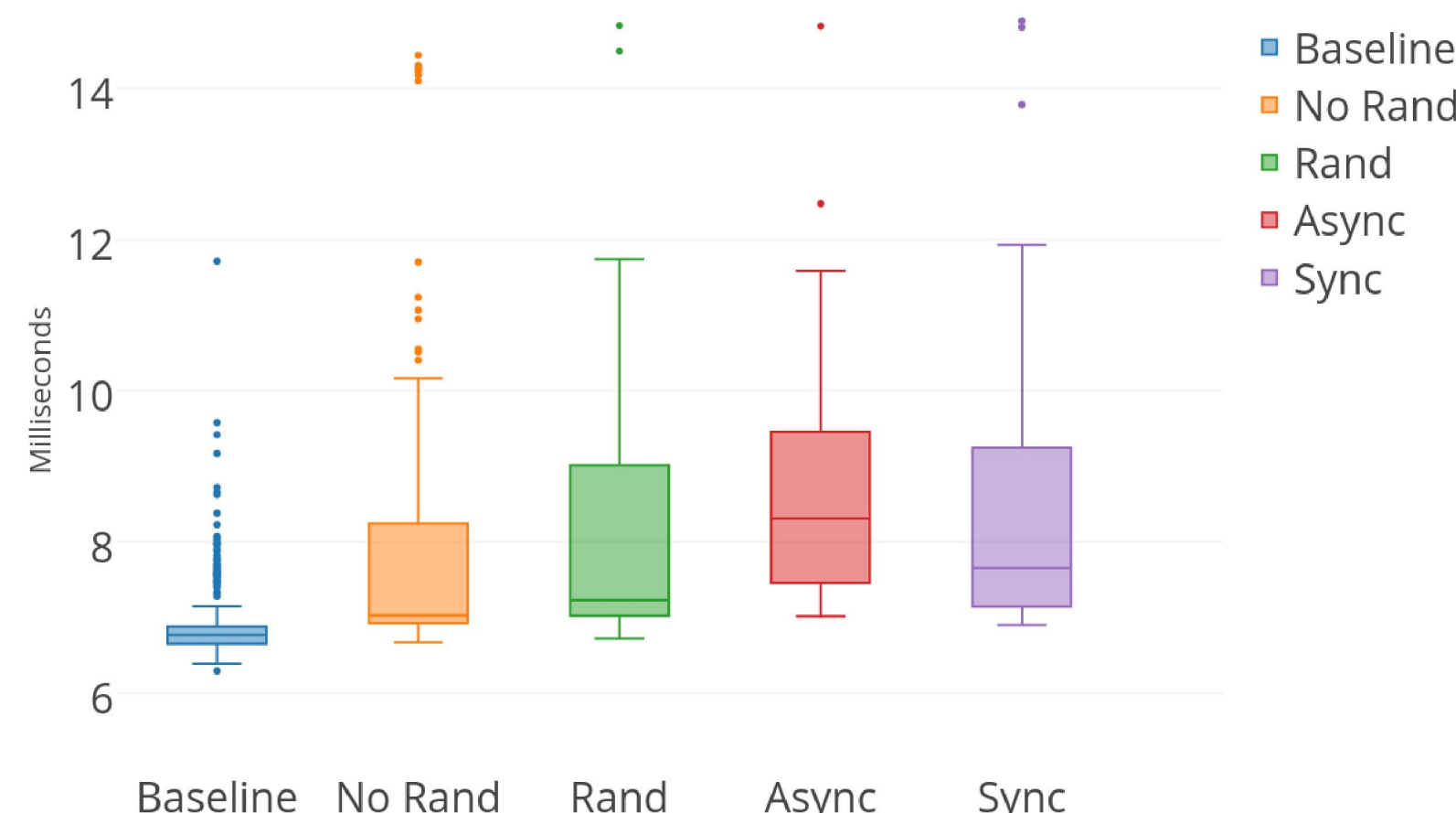
Ground Truth	Benign	TN 99.90%	FP 0.10%	[989]
	Destructive	FN 0.50%	TP 99.50%	[989]
		Benign	Destructive	Prediction

Ground Truth	Benign	TN 99.90%	FP 0.10%	[989]
	Destructive	FN 0.30%	TP 99.70%	[989]
		Benign	Destructive	Prediction

FoJiT 512KB Write Latency for Reactive Policy, n = 100



FoJiT 16MB Write Latency for Reactive Policy, n=100



Algorithm	Description	Tools
AFSSI-5020	Three passes: random data, then complement shifted by 8-bits, then complement shifted by 16-bits [14]	Eraser[15]
AR 380-19	Three passes: a random byte, then another random byte, then complement of the second random byte [14]	Eraser[15]
British HMG ISS (Baseline)	Single pass of zeros [14]	Eraser[15]
British HMG ISS (Enhanced)	Three passes: zeros, then ones, then random data [14]	Eraser[15]
Canadian RCMP TSSIT OPS-II	Seven passes: Three alternating passes of zeros and ones, then a pass of a random byte [14]	Eraser[15]
DoD 5220.22-M(ECE)	Seven passes: A combination of random bytes, complement of random bytes, and zeros [14]	Eraser[15]
DoD 5220.22-M (e)	Three passes: zeros, then ones, then random [14]	Eraser[15], sdelete[16]
German VSITR	Same as Canadian RCMP TSSIT OPS-II [14]	Eraser[15]
Overwrite with zeros	Single pass of all zeros	BleachBit[17]
Pseudorandom data	Overwrite with random bits [14]	Eraser[15]
Russian GOST P50739-95	Three passes: Single pass of zeros, then random data [14]	Eraser[15]
Schmeier's Algorithm[18]	Seven passes: first pass zeros, second pass ones, remaining passes consist of random data [14]	Eraser[15]

This work was supported, in part, by a grant from National Science Foundation Grant EAGER-1548114.

Special thanks to Adam Hammer for his assistance in deploying the testing environment.