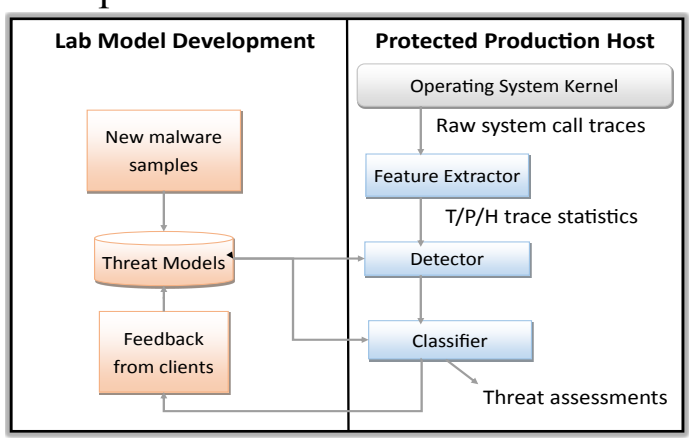
TTP: Medium Securing the Wireless Philadelphia Network

Steven Weber, Kapil R. Dandekar, Spiros Mancoridis, and Harish Sethu

Malware monitoring and classification in Keyspots Community Computing Centers

- **Features:**
  - ◇ System call traces of malware and benign processes
  - ◇ Host-based anomaly detection
  - ◇ Mimic the production environment on live hosts



- **Deployment and evaluation:**
  - ◇ **Real-world scenario**: anomaly detectors were deployed on various KEYSPOT locations of the Philadelphia Keyspots Community Computing centers
  - ◇ Test against **125,000** malware processes, **76,000** distinct malware samples
  - ◇ Dataset time frame: more than **100 days**

Anomaly detection in DNS data from a major Internet Service Provider (ISP)

- **Motivations:**
  - ◇ Detecting volume anomalies in a large DNS dataset (4.6×10^7 DNS queries over 23 minutes) using distributed PCA based anomaly detection algorithms
  - ◇ Evaluated the tradeoff between comm. cost and solution quality of the distributed algorithms
- **Distributed PCA algorithm:**
  - ◇ Data is compressed locally, there is no need to send the whole local measurements
- **Results:**
  - ◇ Distributed PCA methods have little quality degradation, yet achieve significant savings in comm. bandwidth

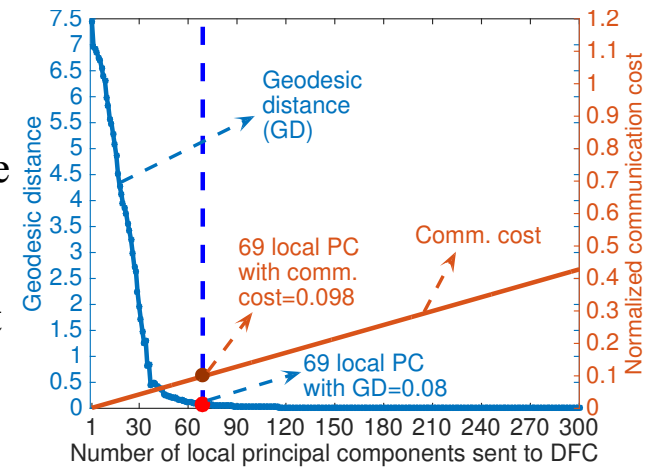


Fig 1. Horizontal partitioning with s=2

Adaptive Sampling and Statistical Inference for Anomaly Detection

Key contributions:

◇ A new efficient strategy for online performance monitoring of data centers using adaptive-rate compressive sampling

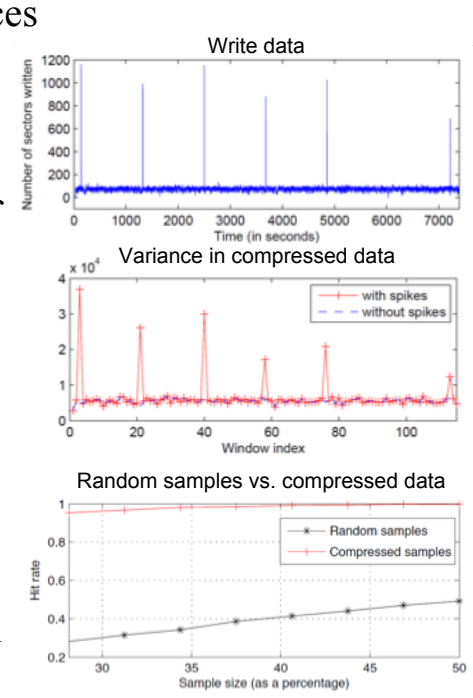
◇ A new method for anomaly detection in computer systems with compressed measurements

◇ A new, fast and distributed method of detecting anomalies in network traffic feature matrices

Results:

◇ Reconstructed data from adaptive-rate compressive sampling allows detection of abrupt changes and trends achieving 90% hit rate when the sample size is just 25%

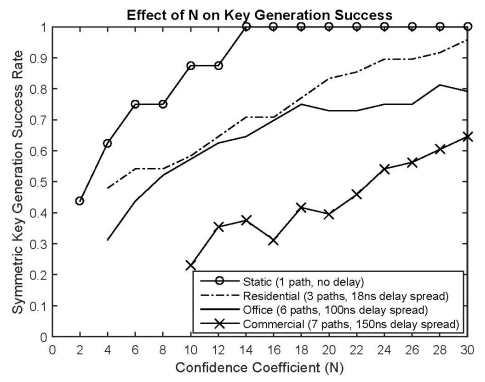
◇ Hit rate achieved using the variance of the compressed samples: greater than 95% when the sample size is greater than 28% , substantially better than with random samples



Establishing shared secret keys over wireless channels

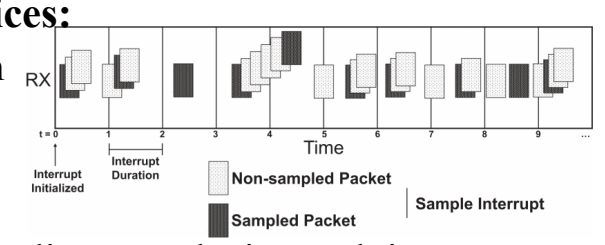
Generating symmetric keys without "hints":

- Previous PHY layer secret key generation algorithms relied on indices, salts etc. to be shared with TX node.
- Using a wireless channel emulator, we experimentally evaluated our new algorithm leveraging channel trends.
- The algorithm establishes symmetric keys without exchanging any initialization vectors, nonce, salts etc.



Road to COTS devices:

- An implementation on COTS devices
  - ◊ Intel 5300 chip
  - ◊ iwlwifi driver



- Interrupt-based sampling uses the internal timer to capture packets and minimizes hardware customization.
- A firmware update is necessary to introduce the new protocol to the chipset's driver.

References

1. Tingshan Huang, Nagarajan Kandasamy, and Harish Sethu, "An efficient strategy for online perfor- mance monitoring of datacenters via adaptive sampling," to appear in IEEE Transactions on Cloud Computing, 2016.
2. Tingshan Huang, Harish Sethu, and Nagarajan Kandasamy, "A new approach to dimensionality re- duction for anomaly detection in data traffic," to appear in IEEE Transactions on Network and Service Management: Special Issue on Big Data Analytics for Management, 2016.
3. Tingshan Huang, Nagarajan Kandasamy, and Harish Sethu, "Anomaly detection in computer systems using compressed measurements," in Proceedings of the IEEE International Symposium on Software Reliability Engineering (ISSRE), November 2015.
4. Raymond Canzanese, Spiros Mancoridis, and Moshe Kam, "Run-time Classification of Malicious Processes Using System Call Analysis," in IEEE International Conference on Malicious and Unwanted Software (MAL- CON), October, 2015.
5. Raymond Canzanese, Spiros Mancoridis, and Moshe Kam, "System Call-based Detection of Malicious Pro- cesses," in IEEE International Conference on Quality, Reliability, and Security (QRS), August, 2015.
6. Ni An and Steven Weber, "On the performance overhead tradeo↵ of distributed principal component analysis via data partitioning", Proceedings of the Conference on Information Sciences and Systems (CISS), Princeton NJ, March 2016.
7. Kapil Dandekar et al., "Symmetric Encryption Key Generation Using Wireless Physical Layer Information Without Sharing Any Information Pertinent To The Key", U.S. Patent Application Submitted, 2016.

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

Drexel UNIVERSITY