CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

LINEBACkER: Bio-inspired analysis for network traffic

Pacific Northwest National Laboratory

Doug Nordwall

9/18/2013

Homeland Security

Science and Technology

Team Profile: Pacific Northwest National Laboratory

- PNNL is a US Department of Energy Office of Science laboratory
  - Approximately 50% of business volume is for applications in national security
  - Strong emphasis on transitioning research techniques and ideas into operational use
  - 10+ year history of multi-site data cyber collection and analysis for Department of Energy labs and other critical infrastructure

Customer Need: Share Data to Protect Network Without Exposing Details

- Multi-institution sharing yields better awareness
- But raw data exposes institutional details
  - Obfuscation before sharing makes data useless
- Volume, rate, complexity, and evolution of traffic make costly or exact matching impractical

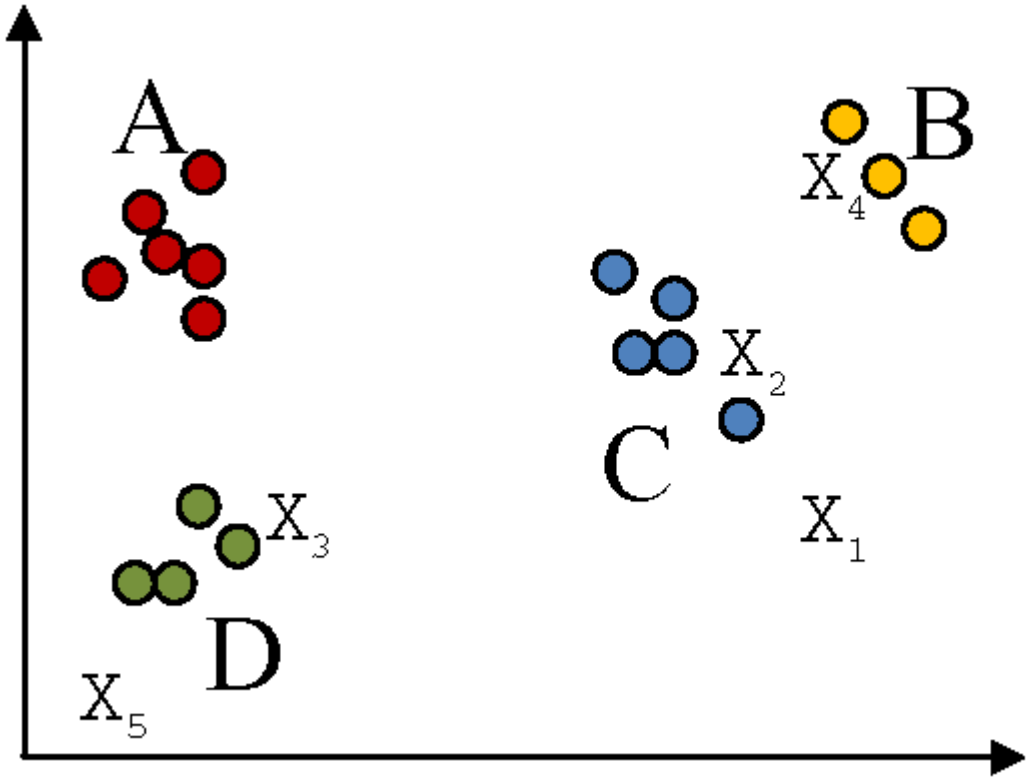
Customers need a way to express and share traffic1) **that protects details of** infrastructure; 2) provides a feature-preserving representation that facilitates **discovery of meaningful patterns**; and 3) that is flexible enough to **recognize mutations** on previous malicious behavior.

LINEBACkER Approach

- LINEBACkER concept
  - use a transformed representation of packet *sequences*
  - associate sequences with each other to suggest *families*
  - build *models* of the family from highly conserved attributes of family members
  - use models as the basis for new *signatures/sensors*

- Can be constructed using normally available data
- Patterns emerge from quantitative analysis, suggest new signatures to look for
- Can account for drift in the underlying phenomena using biological principles

Approach: Finding Behavior Primitives



1. Cluster historical data.
2. Label each cluster with a single character
3. Map new events in a behavior stream to their nearest cluster

The sequence of real events:
X1, X2, X3, X4, X5

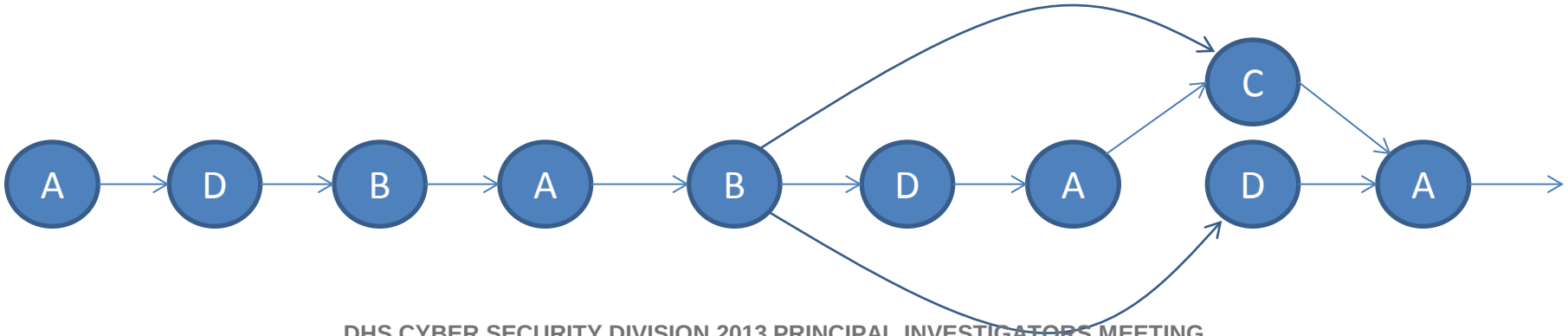
is converted to the string:
CCDBD

This is a lossy mapping that discards raw-data level detail but preserves the ability to find trends and similarities.

Approach: Generating Signatures

```
Sequence 1: ADBABDACACBADCCBACBDBCDDDBCDBCBCBCB...
Sequence 2: ADBABDACACBADCCBACBDBCDDDBCDBCBCBCB...
Sequence 3: ADBAB--CACBADCCBACBDBCDDDBCDBCBCBCB...
Sequence 4: ADBAB--CACBADCCBACBDBCDDDBCDBCBCBCB...
Sequence 5: ADBAB--DACBADCCBACBDBCDDDBCDADADADA...
Sequence 6: ADBAB--DACBADCCBACBDBCDDDBCDADADADA...

Consensus : ADBAB   ACBADCCBACBDBCDDDBCD
```



Approach: A Plan for Sharing Without Exposure

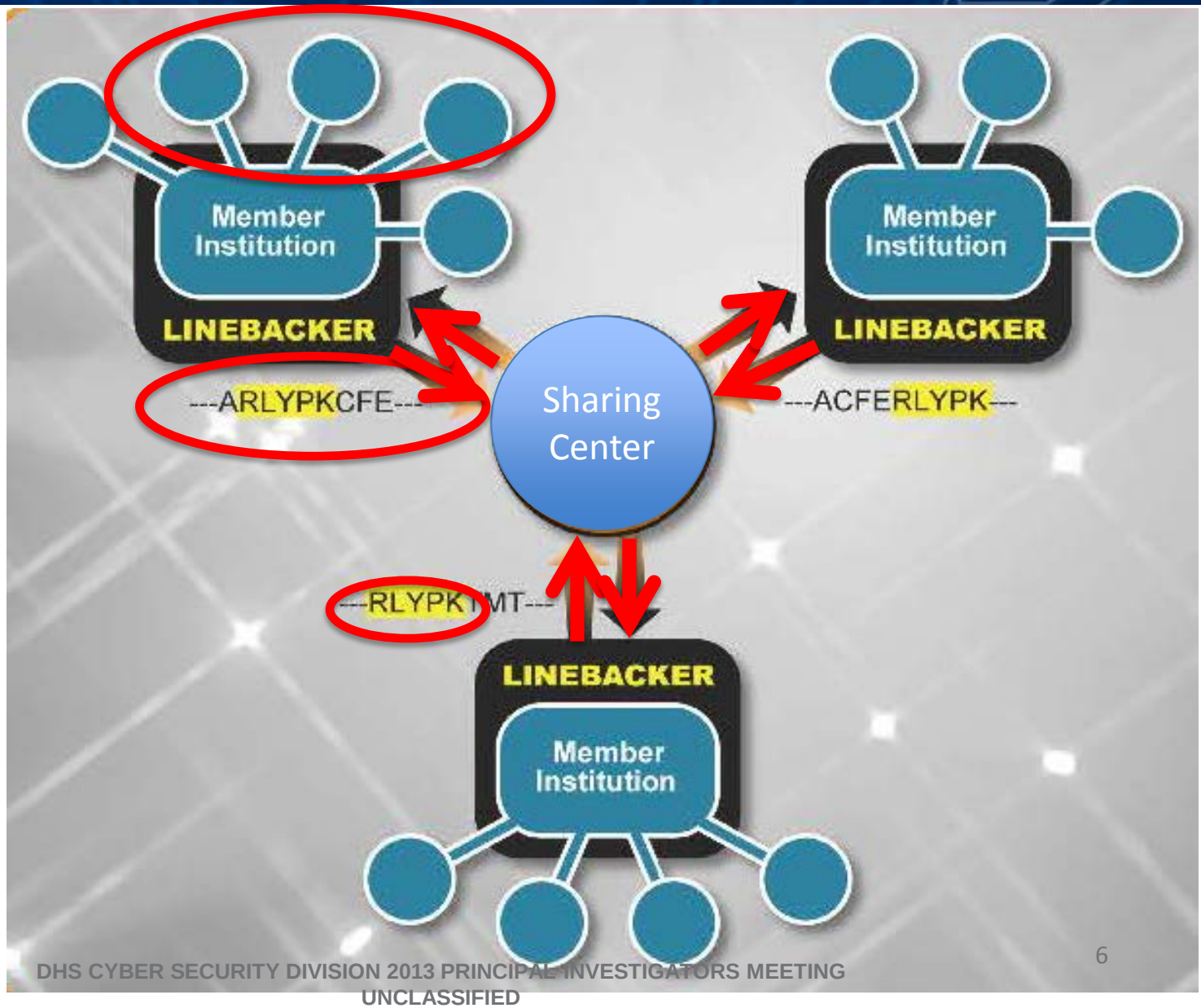
1. Data is collected through sensors at member locations

2. Behavior strings are generated from network traffic

3. Strings are shared via an independent center

4. Analysis is performed on strings and trends are discovered

5. Alerts in string format are generated and pushed back



Benefits

- **Increased Situational Awareness:** Intermediate representation for traffic that allows institutions to share without exposing infrastructure details
- **Line-speed Analysis:** Large data reduction using intermediate form
- **Rapid Discovery of Complex Behavior Sequences**: Ability to discover trends with flexible bio-inspired methods

Current Status

- Several candidate methods evaluated for lossy mapping (Milestone 1, complete)
  - Full packet
  - URL only
  - Bidirectional netflow (selected)
- Baseline behavior (Milestone 2, in process– expected completion of first analysis Sep 2013)
- Development of software for rapid translation in progress (Milestone 3, in process– expected completion of first release to operational partners Oct 2013)

Next Steps

- Quantify performance of LINEBACkER
  - Testing and validation
  - DETER experiments
- Tech Transition Plan
  - ISAC model: working with REN-ISAC to deploy at member institutions
    - LINEBACkER is software and an analysis service
  - Commercial model:
    - LINEBACkER is software and we tune it specifically for different application environments
- Continue Technology Transition Activities
  - LINEBACkER featured as example of MLSTONES under current TTP effort (presenter E. Peterson)
    - Value creation workshop
    - Demo days for government, finance, VC
- Deploy LINEBACkER to REN-ISAC member institutions
  - Conversations with FS-ISAC to deploy using REN-ISAC model

Contact Information

- Doug Nordwall
  - Doug.Nordwall@pnnl.gov
- Chris Oehmen (PI)
  - Christopher.Oehmen@pnnl.gov