TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

Usable Management Tools for the Smarter Grid's Data Avalanche

tcipg.org

Overview and Problem Statement

The present and future smart grid has a vast population of diverse devices that generate lots of data. The variety, large volume, and spontaneous generation of data result in what one of our industry partners has called a "data avalanche." Data avalanches of the future will likely be quite large if the number of devices on the smarter grid is larger than the number of devices on the Internet.

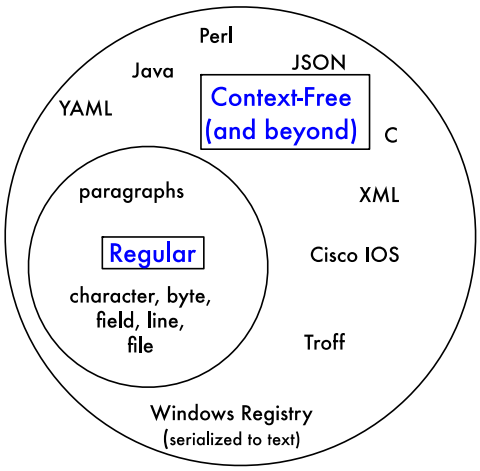
Our research focuses on the following question: How can humans deal with the smart grid "data avalanche" and thereby gain an increased situational awareness for the smarter grid?

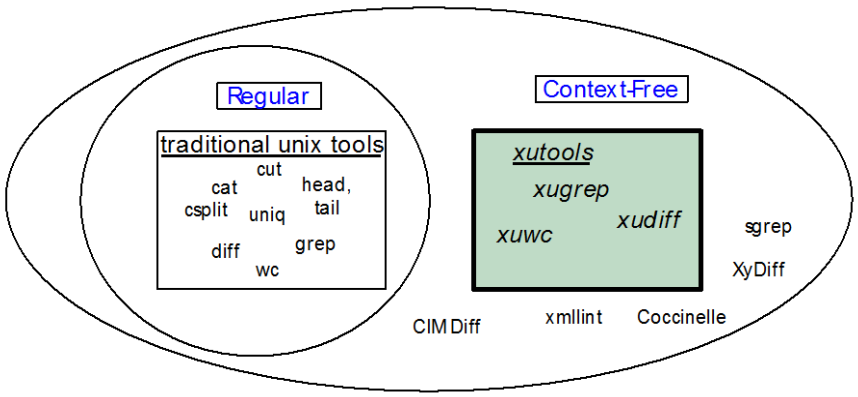
Research Objectives

- **Goal:** We want to enable a more reliable, consistent, affordable audit driven by the flood of data used to configure devices on power control networks.
- **Motivation:** Power control networks must comply with NERC CIP
  - Failure to comply costs up to $1.5 million per day of violation
  - **Audit is expensive**: 30 man days per day; hundreds of thousands to millions of dollars.
  - **Can we** automatically generate change logs and reports of change and thereby **reduce the cost of audit**?
- We research new approaches to **efficient management and auditing of devices on control networks.**
- **Smart Grid Application Area:** Cyber-security situational awareness, NERC CIP compliance audit.

Technical Description and Solution Approach

- Security policies are in **many different languages**.
- Most **policies** and associated security artifacts are **structured text**.
- Many language-specific structures are not recognized by traditional tools.
- Our eXtended Unix text-processing tools (XUTools) process high-level language constructs.
  - xugrep: extract
  - xuwc: count
  - xudiff: compare
- **Our approach** appeared in a **Slashdotted** and widely covered poster **at USENIX LISA 2011** and will appear as a full paper at USENIX LISA 2012.





Results and Benefits

- In IEEE PECI 2012, we identified specific NERC-CIP provisions that our tools address.

	CIP Provisions	Revision	Summary Description	Device Dataset
Software	CIP 003-4	R6	Change Control and Configuration Management	Windows Registry
Software	CIP 010-1	R1.1, R1.2, R1.5, R2.1	Baseline configuration development and comparison	Windows Registry
Network	CIP 005-4a	R5.2	Update network documentation within 90 days of the change	Cisco IOS

- Fall 2012, we demonstrated the ability to **inventory, measure similarity, and see the usage of high-level language constructs in a router configuration file**.
- Since the constructs have names that persist across multiple versions of a configuration file, **we can use these construct types as units of analysis to directly quantify network evolution**.
- **Technology Readiness Level:** Seeking real-world practitioners to evaluate our results.

Object Groups in the Dartmouth Core: 2005-2009		
year	number	size (min/avg/max)
2005	0	0/0/0
2006	0	0/0/0
2007	0	0/0/0
2008	6	2/4.0/6
2009	117	2/4.0/21

ACLs in the Dartmouth Core: 2005-2009		
year	number	size (min/avg/max)
2005	18	2/6.0/39
2006	34	2/8.0/80
2007	39	2/7.0/39
2008	62	2/6.0/39
2009	64	2/7.0/39

Object Groups in the Dartmouth Core: 2005-2009					
year	number	clusters	3-clusters	2-clusters	unclustered
2005	0	0	0	0	0
2006	0	0	0	0	0
2007	0	0	0	0	0
2008	6	0	0	0	0
2009	117	100	4	9	87

ACLs in the Dartmouth Core: 2005-2009					
year	number	clusters	3-clusters	2-clusters	unclustered
2005	18	17	0	1	16
2006	34	31	0	3	28
2007	39	36	0	3	33
2008	52	49	0	3	43
2009	64	58	2	2	54

Researchers

- Gabriel A. Weaver, Gabriel.A.Weaver@Dartmouth.edu
- Sean W. Smith, sws@cs.dartmouth.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security