Usable Management Tools for the Smarter Grid's Data Avalanche

G. A. Weaver and S. W. Smith

TCIPG

Goals and Motivation

Goal: A **more reliable, consistent, affordable audit driven by** the flood of **data used to configure devices** on power control networks

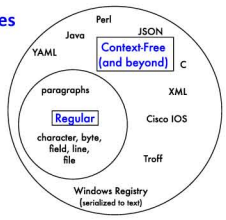
Motivation: Power control networks must comply with NERC CIP

- Failure to comply costs up to $1.5 million per day of violation
- **Audit is expensive:** a conservative estimate suggests that audits consume at least 30 man days per day and cost large IOUs – from hundreds of thousands to millions of dollars
- The smart grid might have **more devices than the current internet**

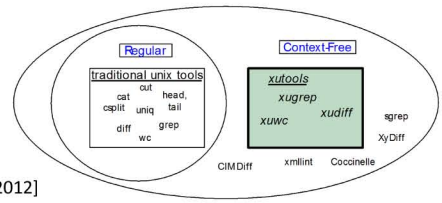
We research new approaches to **efficiently manage and audit devices on control networks and thereby reduce the cost of audit**

Fundamental Problem and 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 regular expressions
- Our eXtended UNIX test-processing tools (**XUTools**) process such structures.



xugrep: extract
xuwc: count
xudiff: compare



[USENIX LISA 2011, 2012]

Research Plan

- Work with utilities and auditors to evaluate our XUTools for NERC CIP audit
- Use practitioner feedback to improve our tools

	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

[IEEE PECI 2012]

Research Results

- We **can inventory, measure similarity, and see the usage of high-level language constructs** in router-configuration files.
- Since these 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**.

Evolution of Object Groups and ACLs

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

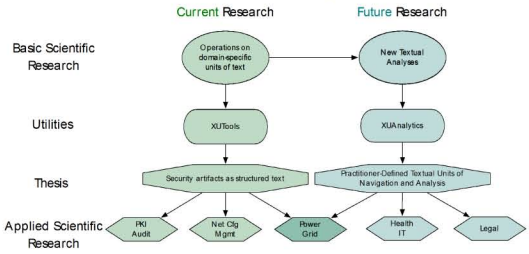
Evolution of Object Group and ACL Similarity

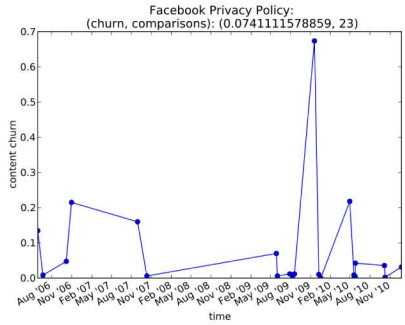
Object Groups in the Dartmouth Core: 2005-2009					
year	number	clusters	3-clusters	2-clusters	unclustered
2005	0	0	0	0	0
2006	0	0	0	0	0
2007	0	0	0	0	0
2008	6	0	0	0	0
2009	117	100	4	9	87

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

[Fall 2012]

Broader Impact





Interaction with Other Projects

- We have been working with Rakesh Bobba, Jun Ho Huh, and Edmond Rogers at the University of Illinois at Urbana-Champaign
- A portion of this research has also been funded by a gift from Google.

Future Efforts: We'll Help You Audit!

- **Work with utilities and auditors to evaluate our XUTools for NERC CIP audit.**

We Need:

- **Feedback** on how we plan to evaluate our XUTools
- **Utilities and auditors** willing to test and use our tools

Download our Tools

http://www.xutools.net/