CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS’

DETECTING THREATENING INSIDERS WITH LIGHTWEIGHT MEDIA FORENSICS

Naval Postgraduate School &
The University of Texas at San Antonio

Dr. Simson Garfinkel (NPS) & Dr. Nicole Beebe (UTSA)

September 17, 2013

Homeland Security
Science and Technology

Team Profile

- Naval Postgraduate School
  - PI: Simson L. Garfinkel

- The University of Texas at San Antonio
  - PI: N. Beebe, Asst. Prof., Info Systems/Cyber Security
  - Co-PI: Daijin Ko, Prof., Mgmt Science & Statistics
  - >30,000 students with 142 degree programs
  - >$80M in funded research annually

Customer Need

- Indication & warning
  - Exfiltration threat
  - Illegal employee activity
- Detect anomalous storage
  - File/data collection
  - Authorized access
  - Anomalous relative to
    - User's history
    - Organization
    - Others in role

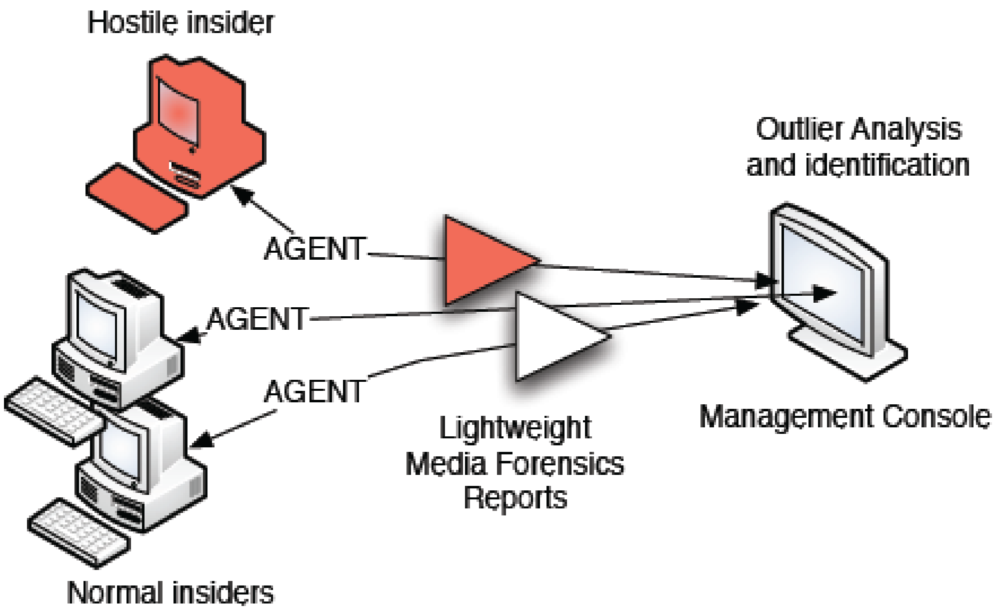
Copying 851 items (3.56 GB)

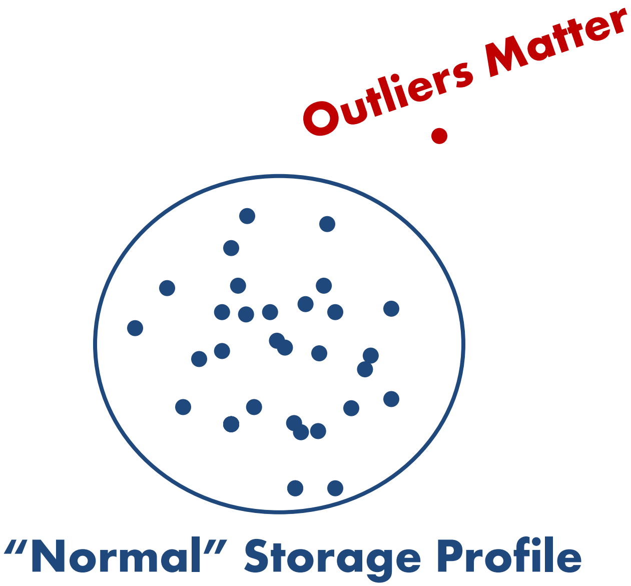
from **Research** (E:\U

Discovered 851 iten

Approach

- Frequently, covertly profile storage on hard disks
  - Lightweight, secure, local surveillance agents
- Identify statistical outliers for further analysis
  - Centralized management console for analysts


Hostile insider
Outlier Analysis and identification
AGENT
AGENT
AGENT
Lightweight Media Forensics Reports
Management Console
Normal insiders



Approach cont.

- Sample disk to collect desired data
  - `bulk_extractor`
  - Open-source, demonstrated capability, v1.4 released
- Client-server, enterprise response framework
  - `Google Rapid Response (GRR)`
  - Deploys client agents, communicates w/ management console, facilitates further investigation
- Anomaly detection agent
  - Univariate and multivariate outlier detection
  - Provide info about *why* client is an outlier

Benefits

Sample Detection Signature (CERT 2011)
if *the mail is from a departing insider*
and *the message was sent in last 30 days*
and *the recipient is not in organization's domain*
and *the total bytes summed by day is more than…*
then *send an alert to security operator*

- Benefits over past solutions
  - Not signature based
  - Not reliant on access patterns
  - Not reliant on policy definition, discovery, auditing
- Design constraints
  - Scalable, non-interfering with operations
    - Desktop: background process, samples disk data
    - Network: small amount, aggregated data transfer
    - Management console: scalable algorithms used
  - Network isolation (no Internet access required)
  - System agnostic (operating system, file system)
  - Includes deleted data in collection/analysis

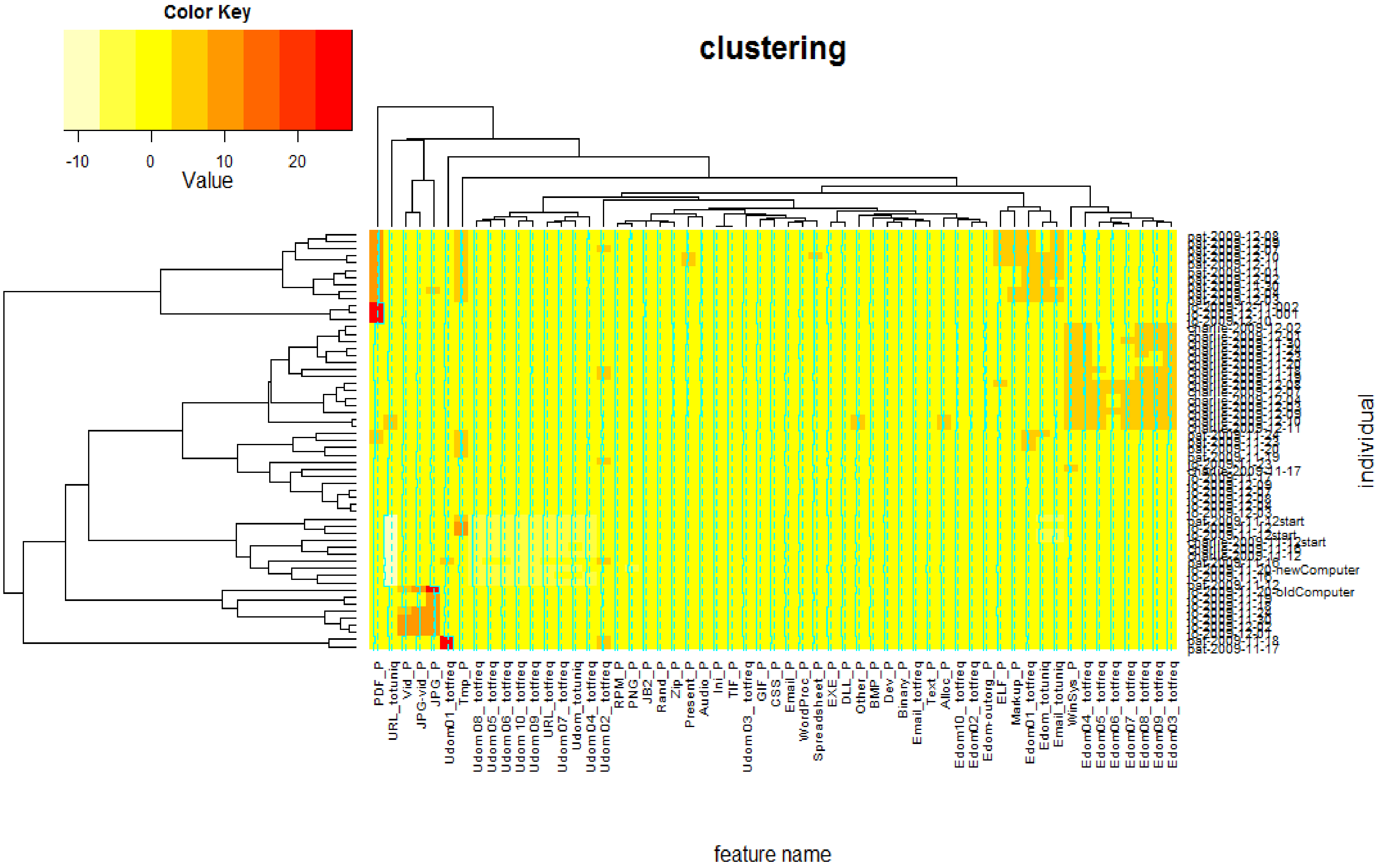
Competing Alternatives (sample)

- SIEM Appliances (Security Information & Event Management)
  - Various commercial tools
  - Disadvantages
    - Relies on fusion of system data & event logs
    - Not data/content focused
    - No analysis of deleted data
- Signature-based extrusion detection systems
  - Example: ELICIT (from MITRE)
  - Disadvantages
    - Presumes attacks follow a known signature
    - Policy discovery and measurement challenges

Current Status

- Technical Progress Toward Project Goals
  - `bulk_extractor` updated v1.4 just released
    - Added features & GRR integration preparation
  - `Sceadan` data type classifier updated v1.2 released
  - Extraction, transformation, loading of synthetic dataset
    - M57 Patents (digitalcorpora.org) case
  - Progress on anomaly detection algorithm
    - Theoretical development
    - Empirical data descriptive analyses (test assumptions)

Sample Univariate Anomaly Analysis



Next Steps

Three-Year Effort

	NPS Lead	UTSA Lead
Year 1	`bulk_extractor` upgrades	Outlier detection algorithm Synthetic data experimentation Real Data Corpus experimentation
Year 2	Integrate GRR (or other framework) Develop/test management console	Develop/test data outlier detection Develop/test visualization component
Year 3	Large-scale testing on partner net	Final dev. of outlier detection algorithm Final dev. of visualization agent

Contact Information

slgarfin@nps.edu

+1.202.649.0029

Nicole.Beebe@utsa.edu

+1.210.269.5647