CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

Evidentiary Integrity for Incident Response (EIIR)

Cyber Incident Response: WAIT! "I should have written that down"

Exelis Inc., Information Systems

Jeffrey Isherwood

16 September 2013

Homeland Security

Science and Technology

Exelis Profile

C4ISR Electronics & Systems

Electronic Systems

Combining These Technologies

>Electronic Warfare

>Force Protection

>Networked Communications

>Radar

>Composite Structures

>Reconnaissance & Surveillance

>Undersea Acoustics

Providing Customers With:

Networks for tactical communications and data exchange, and countermeasures to sense and deny threats to aircraft, ships, ground vehicles and personnel

Geospatial Systems

Combining These Technologies

>Airborne Situational Awareness

>Information Exploitation

>Space-Based Satellite Imaging

>Weather & Climate Monitoring

>GPS

>Night Vision

Providing Customers With:

Next-generation imaging that integrates space, airborne, ground and soldier sensors into broader, coordinated systems.

Information & Technical Services (I&TS)

Information Systems

Combining These Technologies

>Information-Enabled Mission Solutions

>High-End Engineering Services

>Air Traffic Management Systems

>Commercial Aviation Solutions

>Satellite Ground Systems

>Spectrum Management

>Space, Ground and Range Ops, Sustainment, Upgrade and Modernization

Providing Customers With:

Data fusion, network integration and critical decision support services.

Mission Systems

Combining These Technologies

>Global Base Operations and Infrastructure support

>Battlefield Network Communications & Information Support

>Worldwide Logistics & Deployment Support

>Ground Vehicle & Equipment Maintenance

Providing Customers With:

A broad range of critical service, support and logistics solutions that enable efficient operations in the most demanding environments.

Customer Need

- ***Industry feedback:***
  - Poor availability of robust command line tools that can be effectively presented in court
  - Lack of forensic incident response documentation often prohibits prosecution
  - Improper documented IT action hampers law enforcement investigations

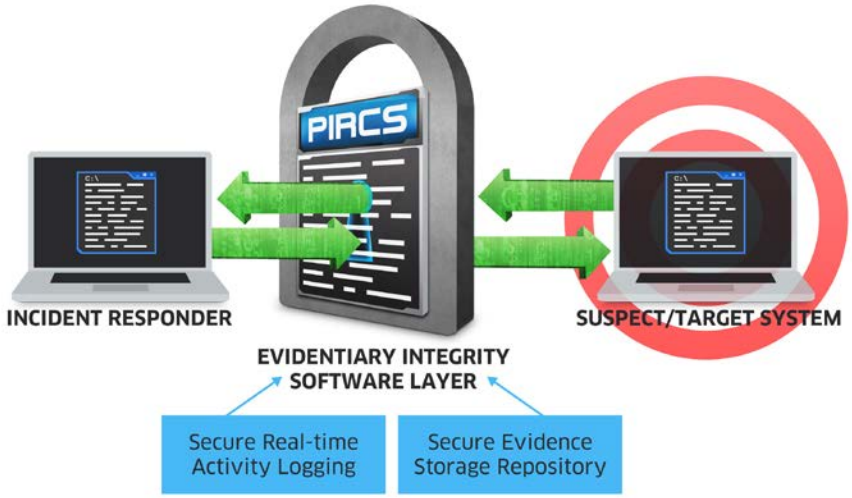
- ***July 2013 SANS Institute***: "Survey of Digital Forensics & Incident Response"
  - ***57%*** *indicated they were looking for legal evidence that could hold up in court*
  - *The survey emphasized the need for :*
    - Treating all cases as if they may end up in arbitration or even legal proceedings
    - Applying rigor in the collection and management of evidence
    - Increasing the trustworthiness so that the evidence can be defended
    - Sound processes that can withstand challenge under outside scrutiny

Source: (Henry, Williams, Wright, 2013)

Approach

- Proactive Incident Response Command Shell (PIRCS) is a seamless and customizable Windows® operating system command shell wrapper that enables cyber incident responders to encapsulate and secure evidence collected during a command line incident response.

- PIRCS consists of the following three core components:
  - Secure real-time activity logging
  - Evidentiary collection and encapsulation
  - Secure evidence storage repository



Approach *(continued)*

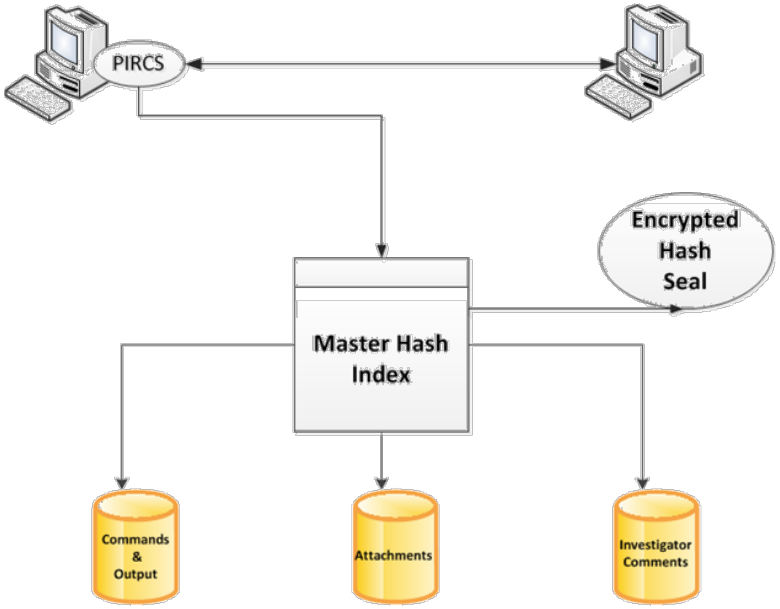
- Secure Real-Time Activity Logging
  - Full duplex logging of any end-user interaction with the command line interface
  - Full ‘service’ level logging that generates time-stamped entries for all software management actions
  - All logs are populated in real-time and is supported by:
    - Bit-stream hashing
    - Full duplex recording
    - Validated data integrity storage

Approach *(continued)*

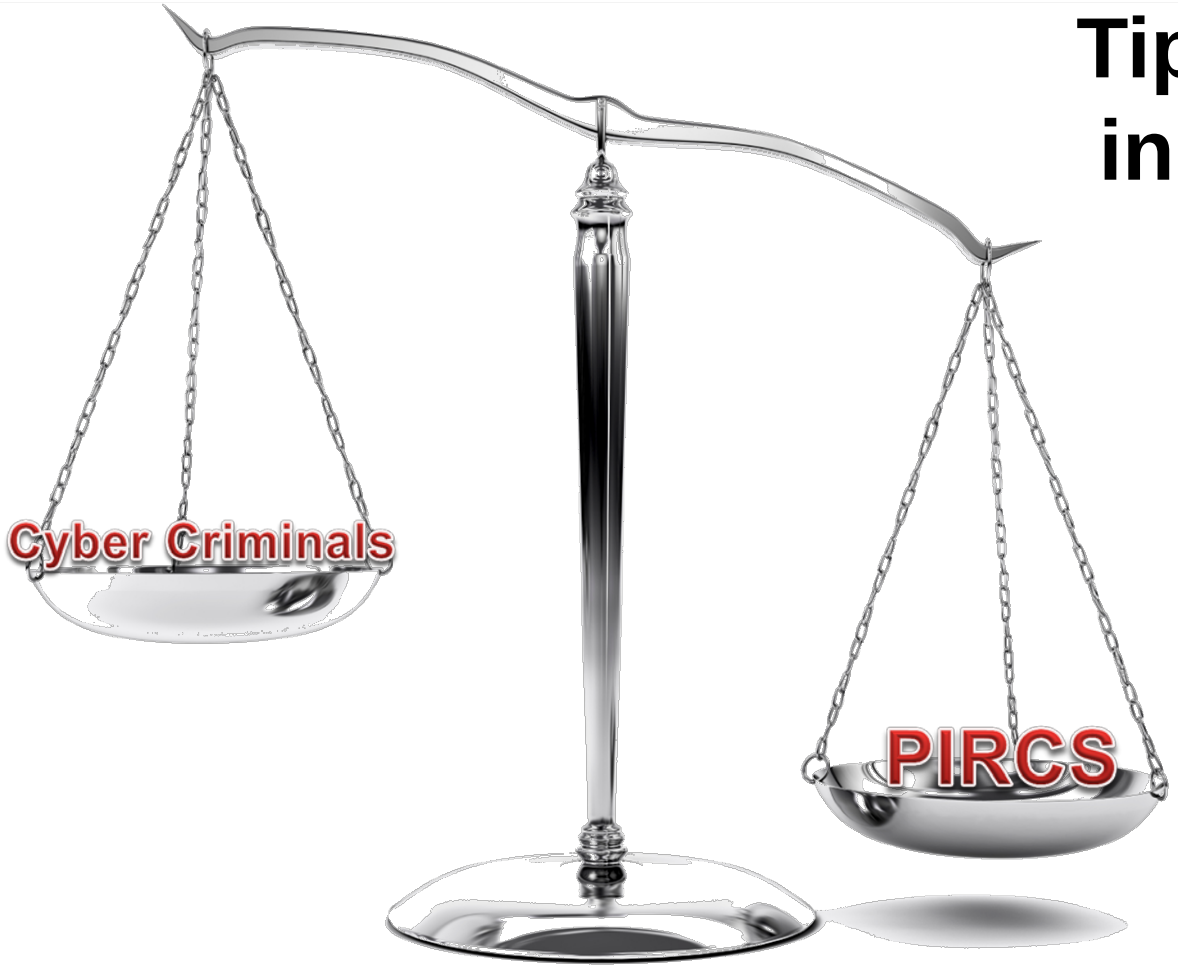
- Evidentiary Collection and Encapsulation
  - A custom file storage format that securely captures the entire stream of data flowing to and from the investigator and the target system.
  - Automates the persistent encoding of metadata about the circumstances and the individuals involved in an incident investigation directly within the forensic image file architecture.
  - Example of metadata fields include:
    - Name of the investigator (or other means of identification)
    - Validated date/time of the data collection
    - Suspect/target system details
    - Analysis/investigation host system details and other details relevant to incident investigations

Approach *(continued)*

- Secure Evidence Storage Repository
  - Stores all commands and their output in a "command database"
  - Downloaded attachments and evidence files are similarly stored in an attachment database, while investigator comments added to the investigation case file are stored in a comments database
  - All three sets of captures are hashed continuously and linked in the Master Hash Index
    - Master Hash Index is itself hashed and encrypted in the Hash Seal Locker
    - Use of 128 AES level encryption to protect the Hash Seal Locker will provide a level of non-repudiation and accountability



Benefits



Tipping the scales in your direction!

PIRCS gives organizations the "OPTION" to prosecute by increasing the ability of IT staff to ***accurately*** and ***defensibly*** collect digital evidence during a command line incident response

Competition

- Keystroke and/or output loggers
  - Typically simple command input or output redirection operators (“>>” or DOSkey)
  - Only capture the typed commands or the output but not both
  - Separate repositories of logs, none of them secure, no hashing
  - Reliant on the end user to remember to turn them on and off
- Scripts MIR-ROR, MSDOS Batch-Scripts, RAPIER
  - Rely upon natively installed applications (which may be compromised)
  - Do not encrypt gathered data
  - Do not allow for investigator interaction
  - Automatically gather data into a bundle blindly

Current Status

- Milestones:
  - Multiple meetings and demonstrations were conducted with the following agencies (potential consumers):
    - New York State (NYS) Police
    - NYS Information Security Office Enterprise Information Security Office
    - Computer Forensics Research and Development Center at Utica College
    - Exelis IT Cyber Incident Response Center
  - Presented and demonstrated the PIRCS capability at the 2013 NYS Cyber Security Conference
  - Nearing completion of a PIRCS prototype that includes the following features:
    - Network intrusion investigation plug-in
    - Command History Lookup
    - Review mode and Investigation mode
    - Import capability
    - Comment capability
    - Searchable interface
- Schedule
  - Beta testing is anticipated to begin the end of September/early October 2013
- Deliverables submitted include monthly financial status reports, quarterly technical status reports, design review meetings and presentations

Next Steps

- Transitioning PIRCS prototype to the following host organizations for beta testing:
  - New York State Police, Forensic Investigation Center, Albany, NY
  - New York State Information Security Office Enterprise Information Security Office, Albany, NY
  - Exelis IT Cyber Incident Response Center, Rome, NY
  - Computer Forensics Research and Development Center of Utica College
- Finalize development of PIRCS prototype based on feedback from beta testing
- Looking into various commercialization/transition options

Contact Information

EXELIS

Jeffrey Isherwood
Senior Cyber Security Analyst

Information & Cyber Solutions
474 Phoenix Drive
Rome, NY 13441
(315) 838-7064
Jeffrey.Isherwood@exelisinc.com
CISSP, CRISC, C|EH, Linux+, LIPC-1

EXELIS

Rosanne Pelli
EIIR Program Manager

Information & Cyber Solutions
474 Phoenix Drive
Rome, NY 13441
(315) 838-7068
Rosanne.Pelli@exelisinc.com
PMP, CompTIA Security+

References: Henry, P., Williams, J., and Wright, B. (2013) "The SANS Survey of Digital Forensics and Incident Response." Online. Available: https://blogs.sans.org/computer-forensics/files/2013/07/sans_dfir_survey_2013.pdf