New Approach to Security Event Management

Martin Hlaváček, Tomáš Konířˇ

SPI 2005 May 6, 2005

Our Job

- Security applications and devices management
- Network appliances logs and Syslog monitoring
- Security policy enforcement
- Defence and recovery from recognized incidents (virus removal, change of fw rules, ...)
- Unrecognized incident investigation

Methods We Use

- Remote terminal access
- Tools with log generating ability
- Central storage for logs
- Central monitoring and management

All the same as in 1980, still need specialist even for routine operations.

There Are Some Points to Improve ...

- Open interface for log retrieval and storage
- Interoperability between the log sources and the management server:
  - Active data retrieval
  - Control of sensor preprocessing
  - Configurable Level of Detail (LoD)
- Data-mining methods applied
- Integration of all security related information

Not Just Network Point of View

- Recent systems focus mainly on
  - Network layer (network IDS, firewalls, ...)
  - Hosts (syslog, host-based IDS, antivirus, ...)
- Weak and flat results of even advanced analysis methods
- Better level of understanding by adding:
  - Staff evidence
  - Property and rights assignment and distribution
  - Actual data from surveillance systems
- On-line import to appropriate layers

Layers

Designed according to analysis, not for easy input.

Types

- Networking layer
- Security layer
- Application layer
- Administration layer

Analysis: search for relations between the layers

Preprocessing and Control

- Preprocessing
  - Preliminary statistical operations shifted to the sensors
  - Value of the results importance relies on the source position/role
- Control
  - Ability to focus sensor
  - Data on demand ability
  - Level of Detail

Future Visions

- Design and develop central server and various sensors
- Verify the profit of our methods for basic analysis
- Apply advanced analytical methods
  - Design the metrics for method evaluation
  - Test the methods
  - Implement the suitable ones
- Validate the solution in real life environment

Conclusion

- New ways to improve the level of understanding and managing security events
- Validation of these methods in proof of concept
- Results at next SPI 2007 :-)

Thank You for Your attention