



ORACLE[®]

Evaluated Configuration in Practice

Shaun Lee
Director, Security Evaluations
Oracle

Adam O'Brien
Senior Principal Program Manager
Oracle

Agenda

- **Evaluated Configurations**
- Management Tools
- Conclusion

Why an Evaluated Configuration?

- Many products have high degree of flexibility, so the evaluation needs to be constrained.
- The evaluators need to be able to set up the evaluated configuration themselves.
- The end user needs to be able to replicate the configuration that was evaluated.

Mechanisms for setting the Evaluated Configuration

- None
- Program settings / Switches
- Patches and Packages
- Scripts
- Installation options
- Evaluated Configuration Document (ECD)

Why does Oracle use the ECD?

- Some functional requirements are satisfied
- The instantiation of assumptions and environmental requirements
- Patching instructions
- Contact information

Issues with the concept

- The ability to tailor the evaluated configuration (by whatever mechanism) has led to the claim that they are unrealistic
- Is the Evaluated Configuration used in the Real World
 - Anecdotal evidence is that the Evaluated Configuration is not used in anger
- Size/complexity of ECD itself

Agenda

- Evaluated Configurations
- **Management Tools**
- Conclusion

Why Management Tools?

They could make it easier to:

- Apply specified configurations
- Audit installations against specified configurations

And do these across the enterprise.

Current Capability

Tools ensure that TOEs are configured in a certain state:

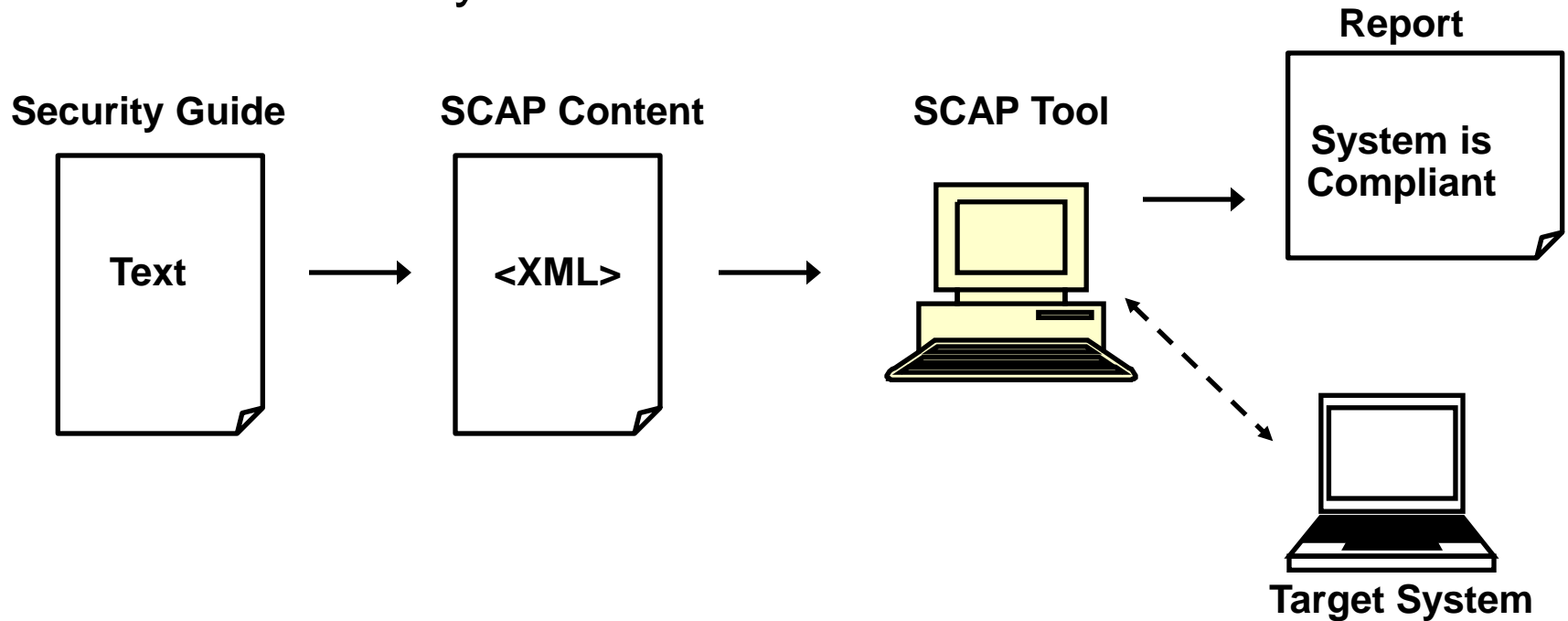
- Oracle's Enterprise Manager Grid Control has secure configuration rule checks
- The U.S. government Federal Desktop Core Configuration (FDCC) program mandates using tools to check that Windows systems are configured securely.

FDCC (a.k.a. USGCB)

- Specifies a minimal set of security configuration settings that all Windows desktops should use.
- Functionally very similar to an evaluated configuration (the difference is that this is, or should be, enforced.)
- US federal government is promoting an open configuration specification language, called Secure Content Automation Protocol (SCAP).

Security Content Automation Protocol (SCAP)

- Provide an open language to specify configuration and vulnerability information



The motivation for SCAP

- SCAP aims to become the primary protocol used to specify security management activities for all US Federal government agencies
- Allow better integration of security tools:
 - An IDS could provide a more detailed report of an intrusion to a firewall
 - A log server can better integrate audit information from multiple, disparate sources
- An element of this is a push to open, standard configurations.

SCAP and CC : Thoughts

- Could the Evaluated Configuration for any product or product type actually be expressed in SCAP form?
- If it can, Enterprise Management tools could scan systems and report on the configuration in that form
- This would allow analysis of the configuration without requiring significant change to the management tool
- Would this give the end user more confidence to use the Evaluated Configuration?

Barriers to SCAP adoption?

- Can the tool support this protocol?
- Can a standardized protocol adequately reflect the target product's feature set - especially when richly featured and/or has complex interdependencies?
- Is SCAP really going to be widely adopted?

Agenda

- Evaluated Configurations
- Management Tools
- **Conclusion**

Conclusions

- Large organisations increasingly have the power to tightly monitor system configuration with enterprise management tools.
- Providing CC evaluated product configurations in a machine readable form with appropriate tool support allows interested parties to more easily ensure that the products are deployed in the secure configuration, increasing the utility of the configuration information and hence:
- Encourage vendors to evaluate realistic configurations

For More Information

Oracle Security Evaluations:

<http://www.oracle.com/technetwork/topics/security/security-evaluations-087427.htm>

General Oracle Security information:

<http://www.oracle.com/technetwork/topics/security>



ORA



ORACLE IS THE INFORMATION COMPANY