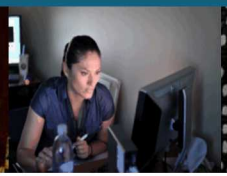
SAND2019-10579C

Lessons Learned from Eight Years of Need-to-Know



PRESENTED BY

Susan Byrnes, Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Background

Lessons Learned

Remaining Challenges

Where Does the Need-to-Know Concept Come From?

Executive Order 13526

- Prescribes a uniform system for classifying, safeguarding, and declassifying national security information

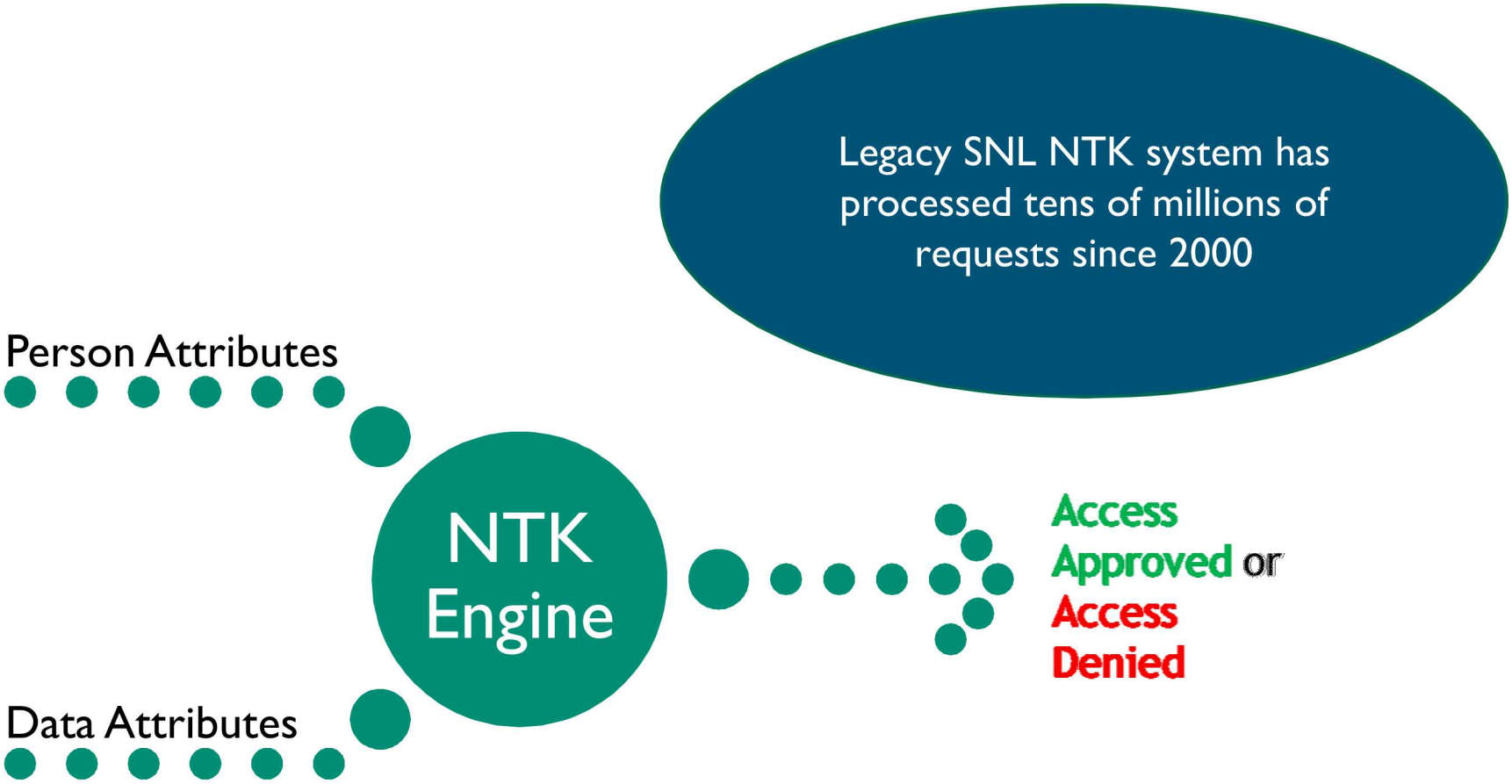
DOE Order 471.6

- Authorized access to classified information requires appropriate clearance, relevant access approval, and need to know

Federal Requirement R010

- Requirements relevant to the subject of this presentation

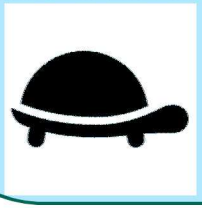
NTK via Attribute Based Access Control (ABAC)



User expectations have changed since 2000

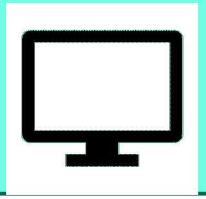
2000

- Still focused on providing access to physical documents
- Individuals access a handful of documents at a time
- New information takes days to be made available

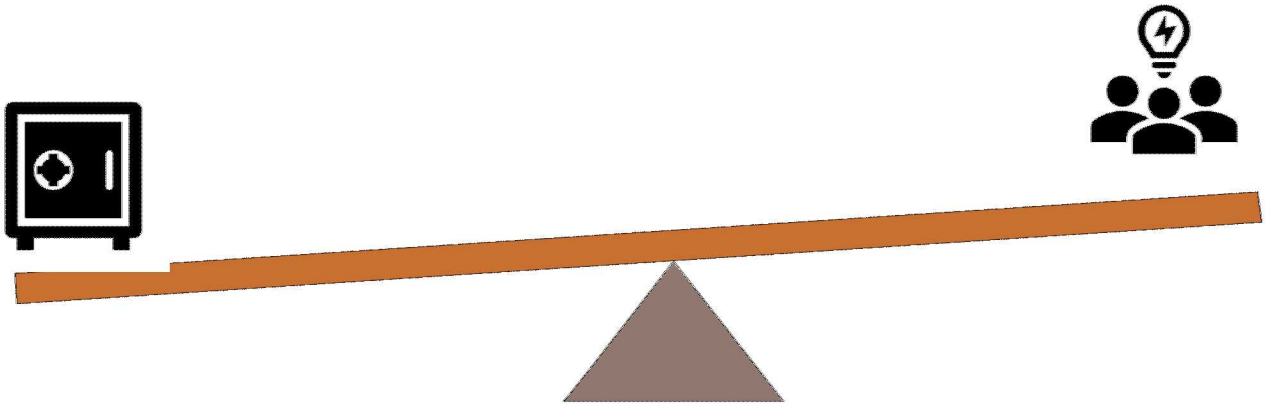


2019

- Electronic access to data across repositories
- Automated processing of large data sets for analysis and insights
- Instantaneous access to new information



Accessibility with Security



It's a delicate balance to make information accessible, yet protect it from unauthorized use

Lessons Learned

Clearly Define Attributes

Legacy system define attributes by:

- Name
- Required or Optional
- Whether Multiple Values Are Allowed
- Active or Inactive
- List of Valid Values

New system similarly defines all attributes, but attributes are defined and provided as master data so that:

- all consumers have access to the list of valid values and their intended use
- the meaning of the attributes and the list of valid values are governed

Common understanding of all attributes is essential to successful attribute based access control

Centralized vs Distributed Security Metadata

Legacy system relies a single repository for all security metadata. This improved performance but led to delays and inconsistencies :

- Accessibility to new data was delayed over night or longer initially and eventually reduced to only a few hours
- Security metadata could be changed in either system and discrepancies between the repositories increased over time

New system will rely on distributed security metadata :

- Person attributes are available in real-time
- Independent systems will provide their own metadata
- Reusable sources of data attributes will be provided as master data

Security metadata (for both persons and data) need to remain in the source system

Comprehensive Audit Logging

Legacy system provides excellent audit logging capability:

- enable tracking of all changes to attributes, rules and authorizations
- enable traceability of access authorizations providing the values of all attributes at the time of the NTK determinations

New system follows suit and will

- enable better reporting and analysis capability

All NTK determinations must be auditable and traceable

Streamline Rule Maintenance

Our NTK Rules are Boolean expressions that describe a set of data and associate that data with one or more authorized groups, example:

- If vehicle-make='FORD' and vehicle-type='TRUCK' then Ford-Truck-Group has access

Legacy system had a cumbersome process for "building" NTK Rules which led to IT personnel performing maintenance and eventually to assumption that IT "owned" the NTK rules

SNL is simplifying and consolidating existing NTK rules, but new system will support more complex NTK rules as needed

Provide text/YAML format or spreadsheet formats that can be configuration managed and deployed without requiring other code changes

Goal: Enable the business owner to maintain the rules

Ensure Scalability

Legacy system was built for individual access requests at low volume, and has evolved over the years:

- batch mode was added to provided overnight processing of large requests
- web service interface was added
- web service updated to accept 1000 requests per call – but responses could take several minutes

New system is based on scalable architecture that will enable multiple instances to be deployed for performance and availability

Goal: Enable the business owner to maintain the rules

Flexibility Leads to Complexity

Legacy system is very flexible, but this comes with a downside, including:

- the underlying database is abstract and difficult to work with – this makes programming changes difficult and risky
- creation of complex Boolean rules makes the outcome of rule processing difficult to explain, understand and maintain

New system's goal is simplicity and transparency

Just because we can, doesn't mean we should

Remaining Challenges

Remaining Challenges

- Enforce sufficient [and accurate] security metadata at time of data creation
- Lack of security metadata for legacy data
- Buy-in from the business: use governance to discourage data silos
- Aggregation of data from multiple sources is still a concern from a classification perspective as well as NTK
- Adoption by IT – for legacy and new applications
- Predictive / Estimated Access – still needed?
- Extend / integrate with role-based access control

Lessons Learned from Eight Years of Need-to-Know