*Practical Concerns:*

# Engineered Controls for Dealing with Big Data

1. Recognize that insecure systems can't defend privacy from serious attacks … and current systems are penetrable. Study the threats and vulnerabilities in your environment.

2. Plan from the start to employ available engineered controls to enforce policies. Add-on measures have a poorer track record than built-in.

3. Maintain the technical basis for accountability for data use to retain public trust when problems occur.

# Know Your Vulnerabilities and Threats

## Prepare for both accidents and attacks

Even large, well-supported systems can harbor undetected, exploitable vulnerabilities

- Example: April 16, 2014: Oracle distributes patches repairing 104 security vulnerabilities*

## Aim to prevent, but be able to detect, respond, and recover

## Consider what might motivate an attacker – fear, greed, lust, revenge – and consider how your particular data (or programs) might be abused

*Source: https://threatpost.com/oracle-fixes-104-security-vulnerabilities-in-quarterly-patch-update

# Plan from the start to employ available engineered controls to enforce policies

- Access controls (subject, object, permitted access) provides basic structure;
  - may be extended to take account of purpose of access: "usage-based" access control
  - Example: Accumulo – open source tool for big data – supports cell-level access controls
- Future: Information flow controls may mirror policies and provide a simpler way to enforce them
- Future: breakthroughs in cryptography may support computing with encrypted data

# To Build Public Trust, Maintain Technical Basis for Accountability for Data Use

- When bad things happen, be able to answer
  - How are users identified, authenticated?
  - How is access to data tracked, logged?
  - How are software versions tracked, logged?
  - How is data provenance maintained from inputs through outputs?
- Mechanisms that can help
  - Multi-factor authentication
  - Hardware root-of-trust (e.g. Trusted Platform Module)
  - Data tagging
  - Cryptographic mechanisms

*Practical Concerns:*

# Engineered Controls for Dealing with Big Data

1. Recognize that insecure systems can't defend privacy from serious attacks … and current systems are penetrable. Study the threats and vulnerabilities in your environment.

2. Plan from the start to employ available engineered controls to enforce policies. Add-on measures have a poorer track record than built-in.

3. Maintain the technical basis for accountability for data use to retain public trust when problems occur.