Foundstone
Professional Services A DIVISION OF McAFEE


# Developers are from Mars, Compliance Auditors are from Venus

**Neelay S Shah**
**neelay.shah@foundstone.com**

**Rudolph Araujo**
**rudolph.araujo@foundstone.com**

**Foundstone Inc., A Division Of McAfee**

*November 25, 2010*

# Goal

- Provide guidance and best practices for software development from a regulatory compliance standpoint

# Agenda

- Background
  - Need for regulatory compliance
  - Intent of regulatory compliance
  - Approach of regulatory compliance
  - Disconnect between the regulatory compliance and the developer community
- Technology Recommendations
- People Recommendations
- Process Recommendations
- Questions

# Background

- The need for regulatory compliance
  - (In)Famous cases – Data Breaches
    - Heartland Payment Systems – Payment card data breach
      - Millions of payment card details compromised
    - Telstra – Personal account information data breach
      - Over 200,000 customers affected
    - Massachusetts community hospitals – Health information data breach
      - Over tens of thousands of patients impacted
    - Veteran Affairs Data Theft
      - Personal details of over 26.5 millions stolen
- Intent of regulatory compliance
  - Safeguard the sensitive data
    - Ensure confidentiality and integrity of the data

# Background

- Reason for disconnect between the regulatory compliance and the development community
  - Regulations most often indicate the end goal however they do not talk anything about how to achieve this end goal
  - Language and context of the regulatory compliance tend to be directed towards “legal” community rather than “technical” community
- Impact of non-compliance
  - Fines, Legal punishment, Public embarrassment, Lack of customer confidence
  - Etc…
- Approach of the regulatory compliance
  - Physical Security
  - Infrastructure Security
  - Operational Security
  - Application Development Security

# Background

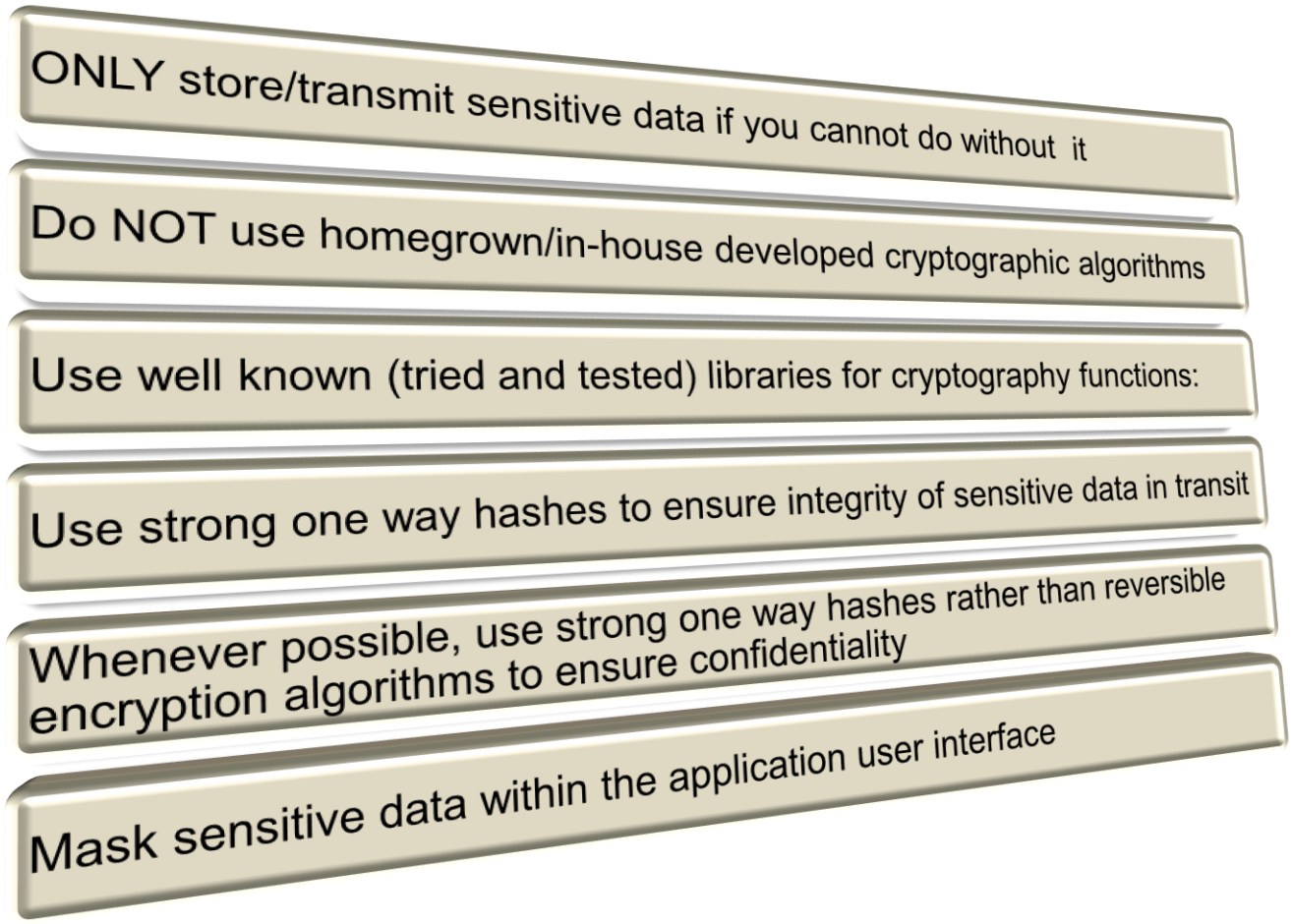
- Example regulatory compliance

| Name | Purpose / Scope |
|---|---|
| Payment Card Industry (PCI) | Applies to systems dealing with payment card data |
| European Union Data Protection Directive | Applies to systems collecting, processing and releasing personal data |
| Health Insurance Portability and Accountability Act (HIPAA) | Applies to systems dealing with personally identifiable health information |
| Sarbanes-Oxley (SOX) | Applies to all public companies and is concerned with the confidentiality and the integrity of financial reporting |
| Basel II | Applies to systems that deal with personal financial information |

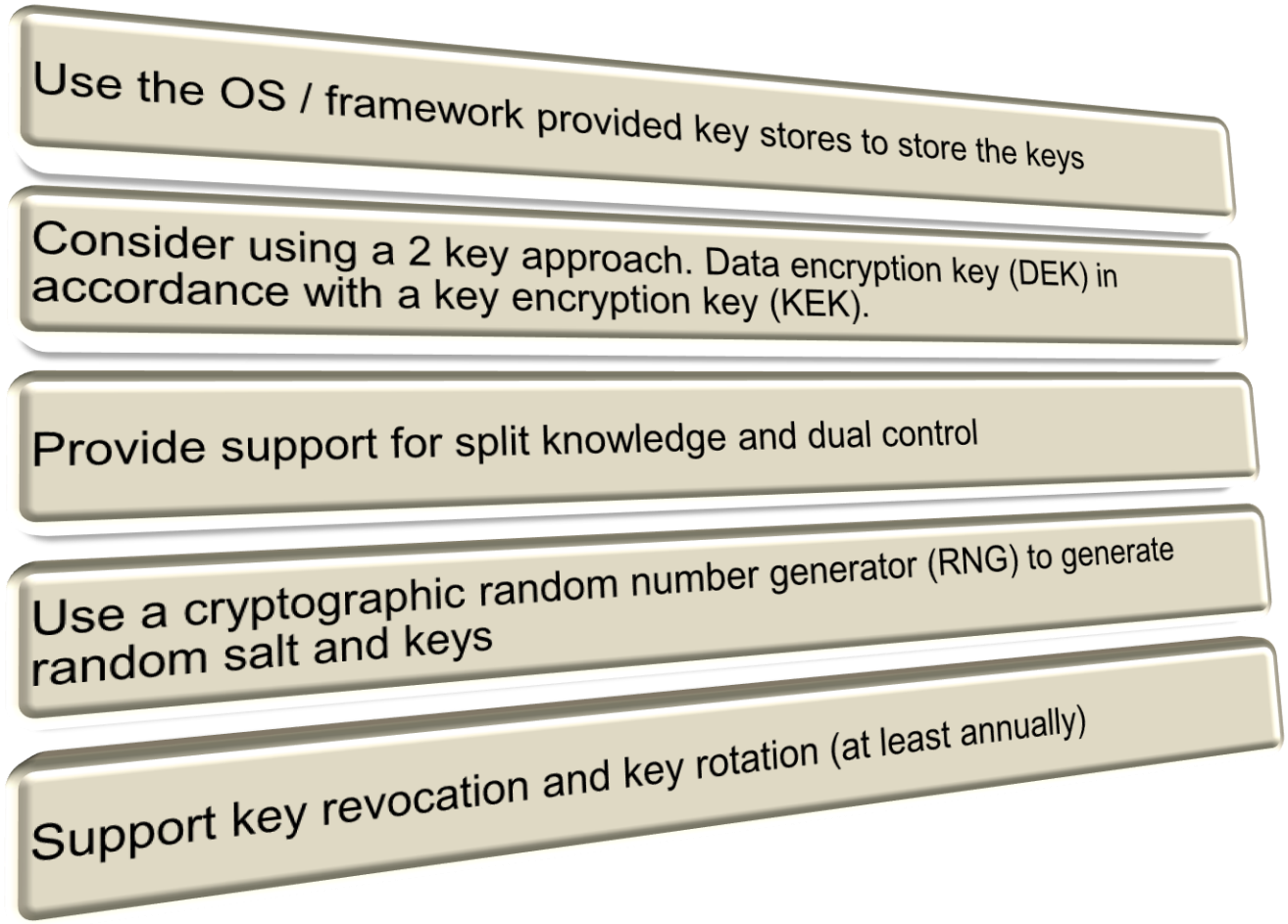
# Technology Recommendations

- Map the regulatory compliance requirements into developer technical categories
  - Data protection in storage and transit
  - Authentication
  - Authorization
  - User and session management
  - Data validation and exception handling
  - Auditing and logging
  - Configuration management

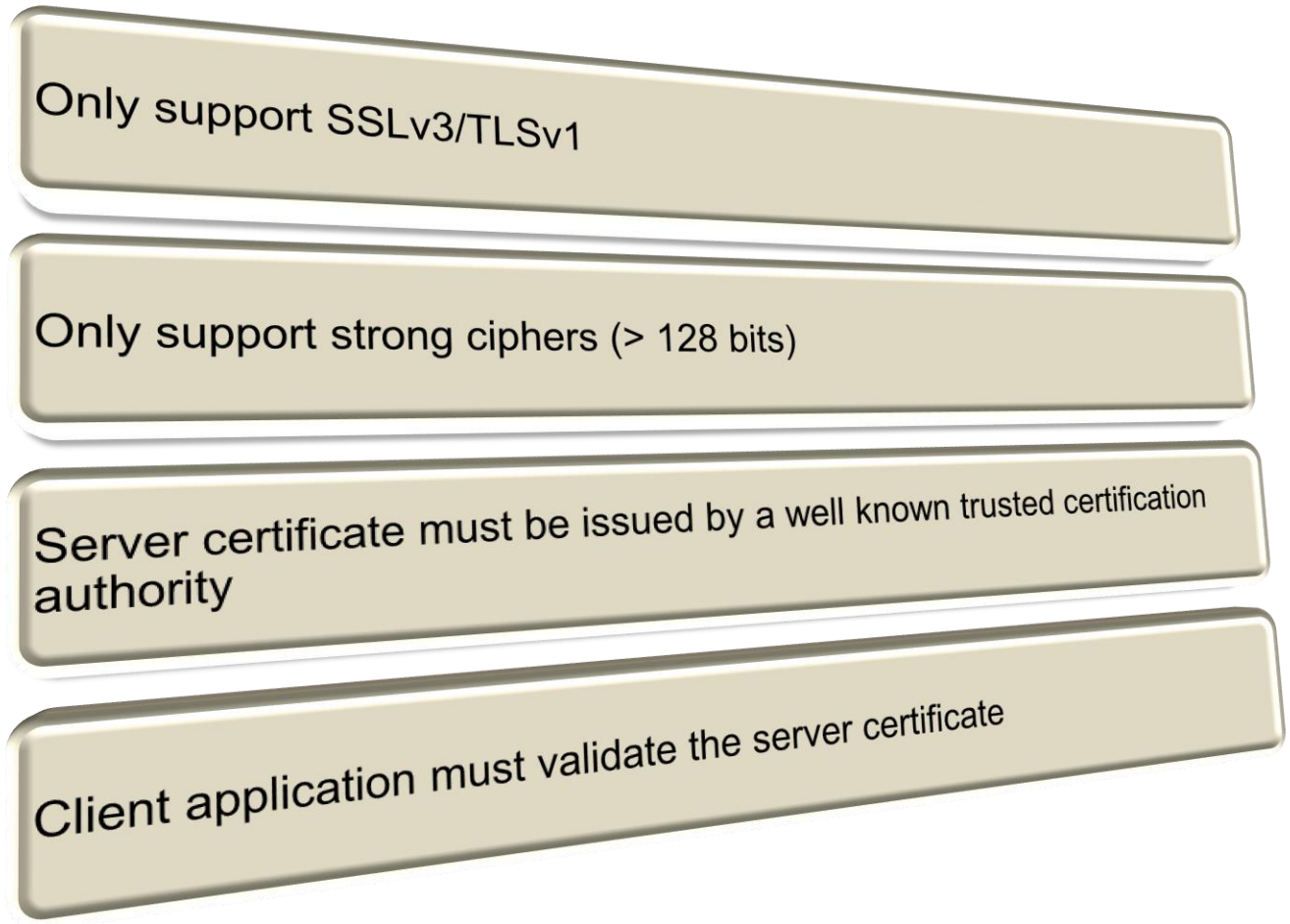
# Data Protection in Storage and Transit



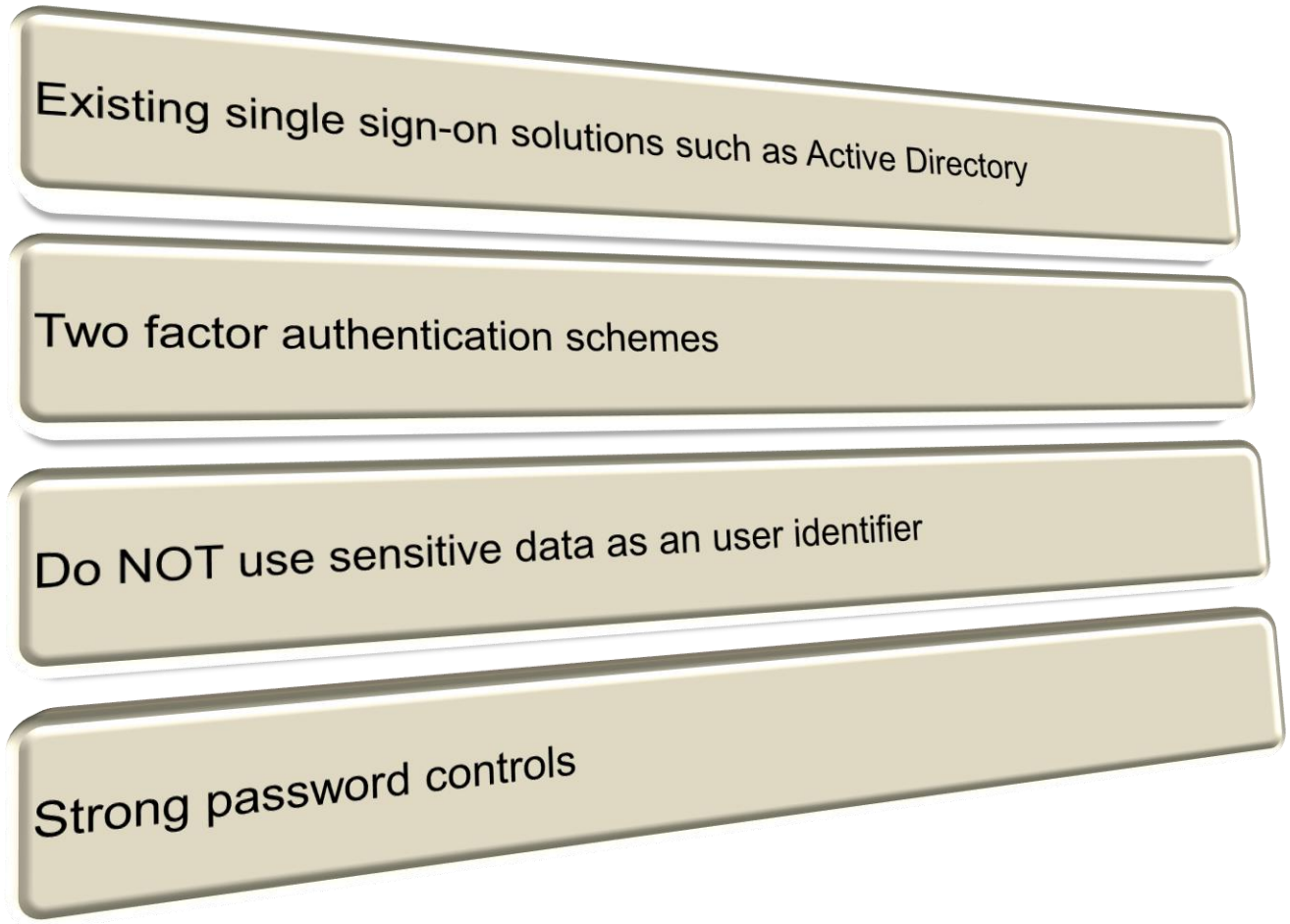
# Data Protection in Storage and Transit



# Data Protection in Storage and Transit



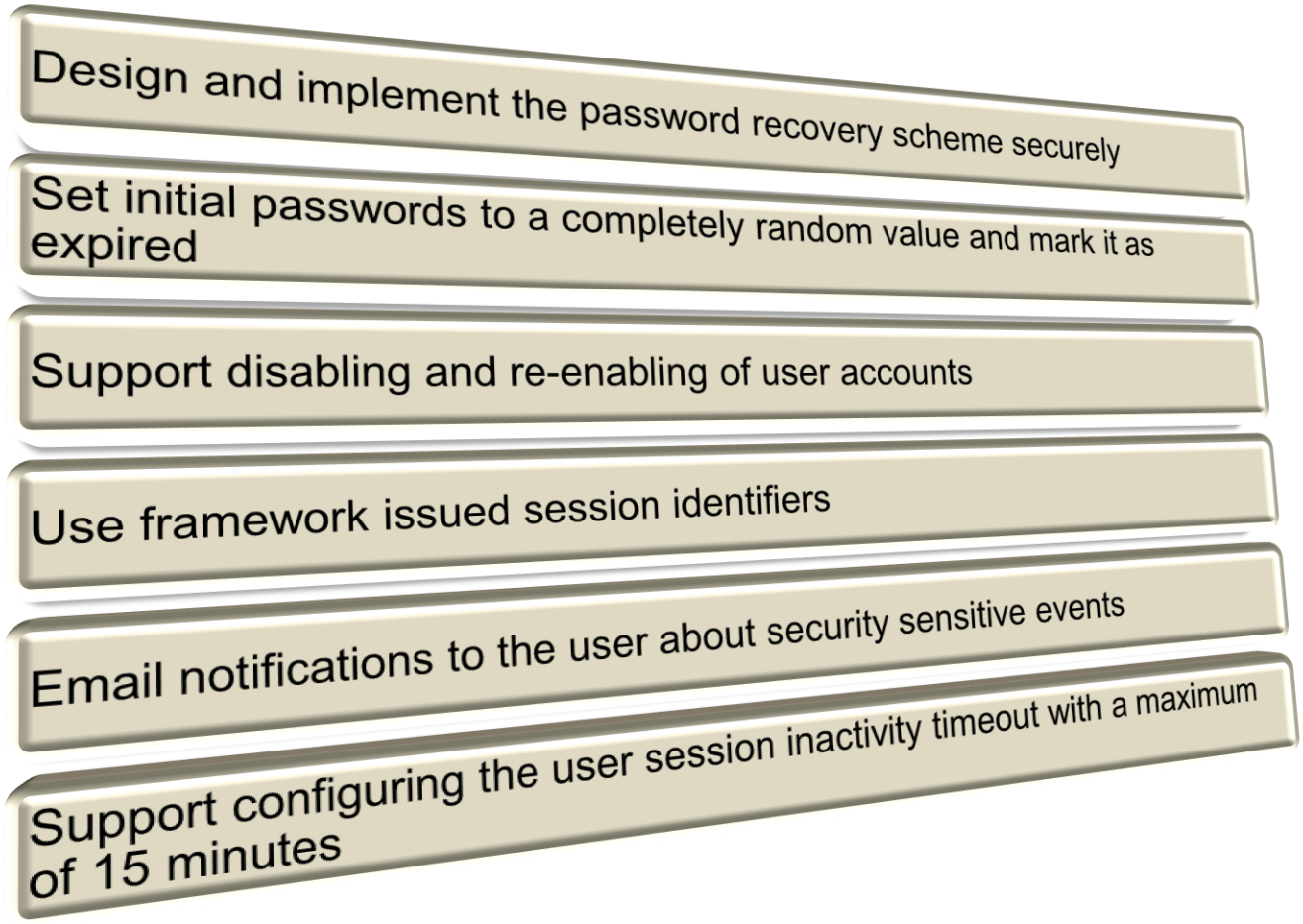
# Authentication



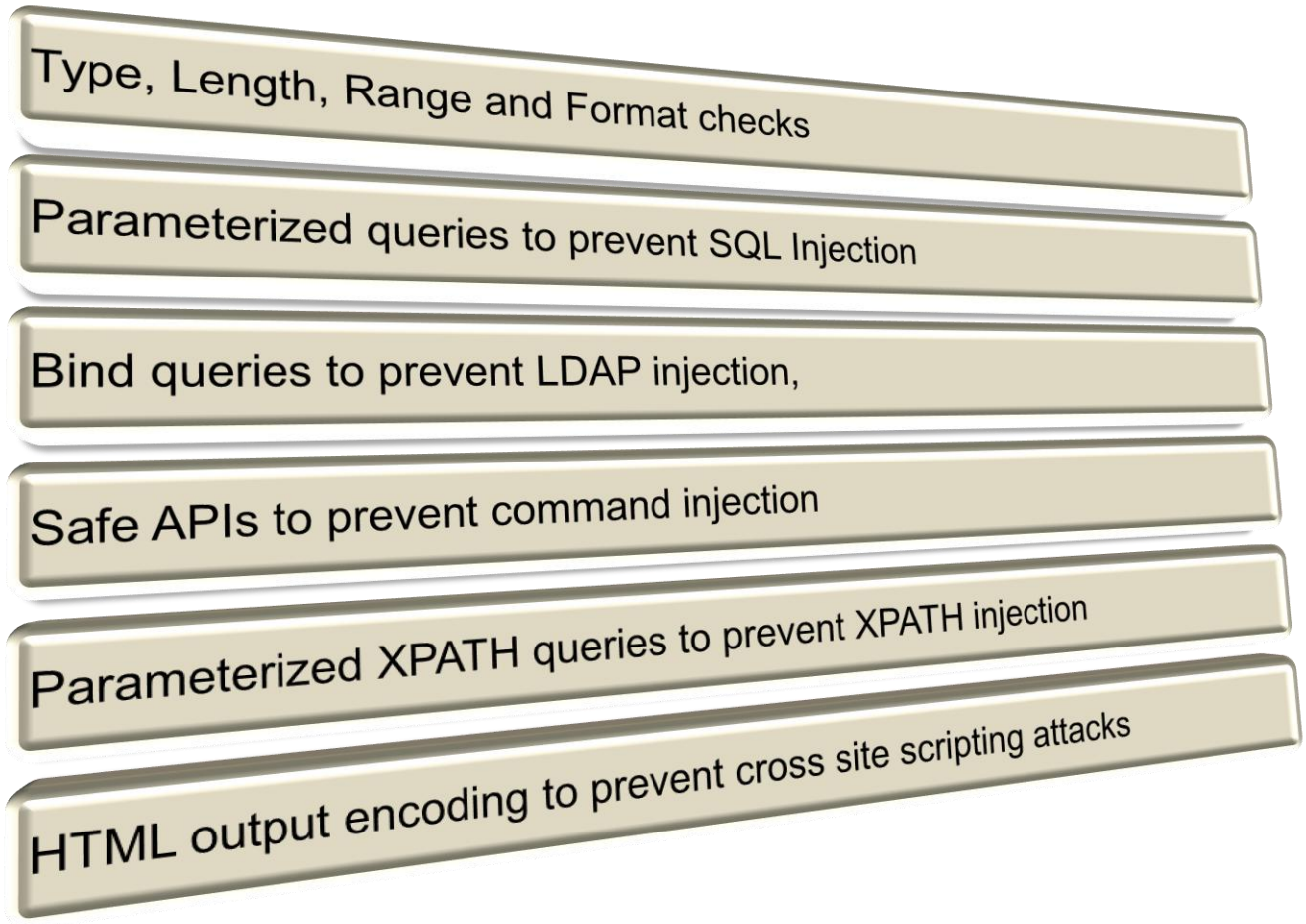
# Authorization

- Perform authorization checks for every request
- Check if the subject (for e.g. user) has the privilege to perform the action (CRUD – create, read, update and delete) on the object (for e.g. data element such as an account)
- Do not use hidden fields for user / role identifiers
- Do not use cookies for role identifiers

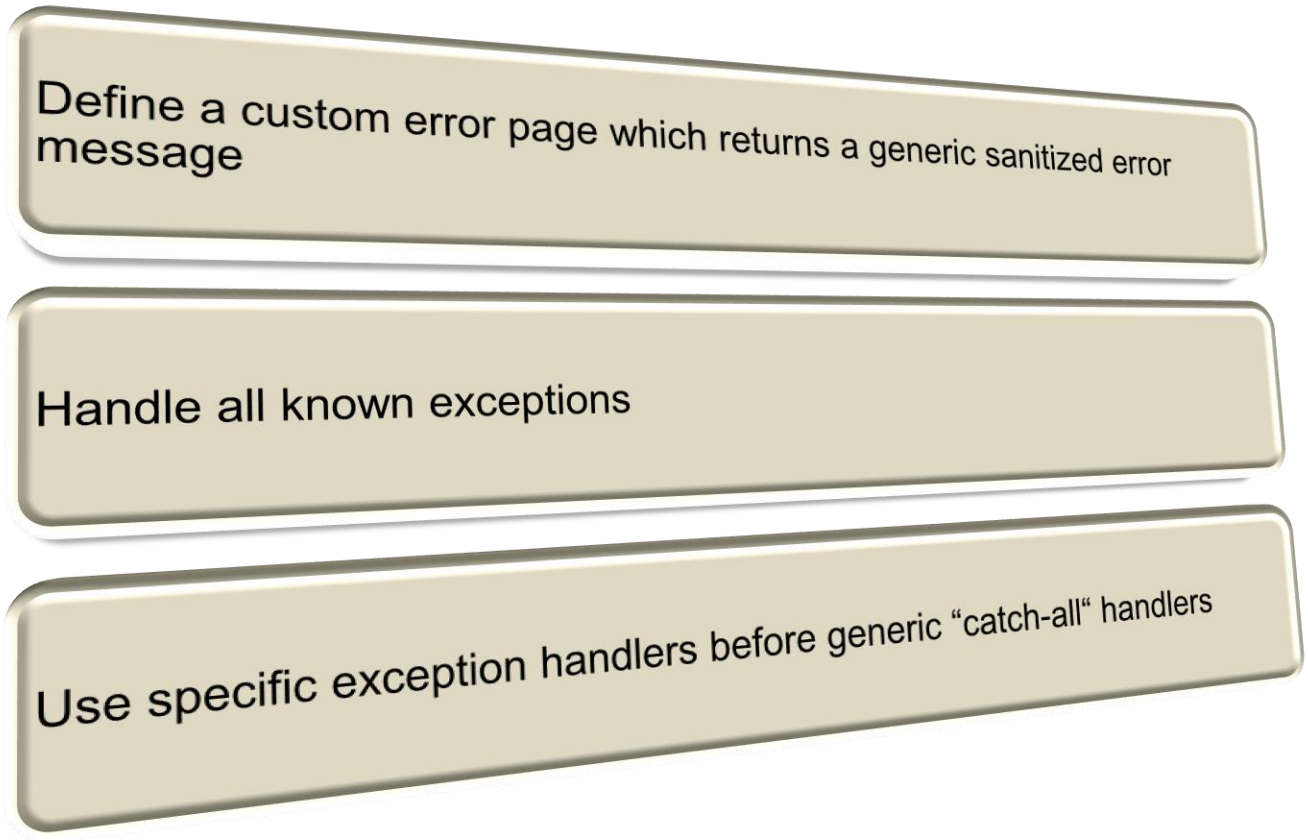
# User and Session Management



# Data Validation



# Error and Exception Handling



# Auditing and Logging

The audit log file should be able to answer the question "Who did what to whom and when".

The following actions must be logged:

- All attempts (failed or successful) to access (add, read, update, delete) objects
- All administrative actions
- All login attempts (failed or successful) to the application

In addition, the following metadata information must be logged for every event to ensure traceability:

- The date and time when the action was performed
- The source of the action e.g. the IP address
- The subject (user) requesting the action
- The result of the action - Success or Failure

The following data must NOT be logged

- Sensitive data such as credit card numbers, sensitive authentication data and application user passwords

# Configuration Management

**Support run-time configuration of the audit log**

- Log location – Database, File etc.
- Log level
- Log maximum size
- Log archival strategy – Log rotation, Log wrapping etc.

**Do NOT use default credentials for any third party / COTS component**

**For all new user / service accounts created as part of the application installer / runtime**

- Do NOT use default / fixed credentials

# Recommended Best Practices

- Cryptographic algorithms

| Type | Name |
|---|---|
| Symmetric cryptography | AES-512 |
| Asymmetric  cryptography | RSA-2048 |
| One way hash / MAC | SHA-512, HMAC-SHA512 |

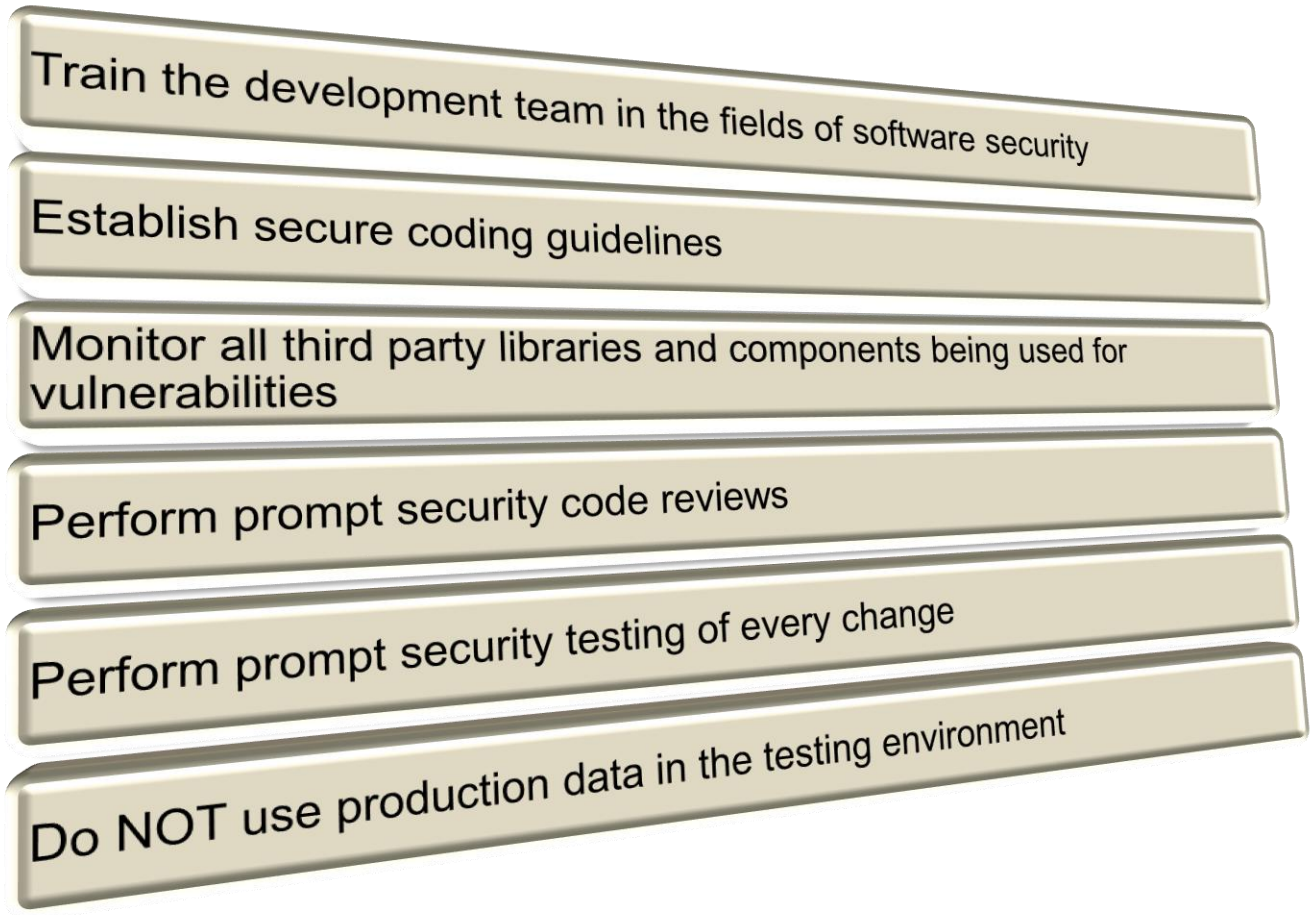
- Password controls

| | |
|---|---|
| Password Length | At least 8 characters |
| Password Complexity | 1 upper case, 1 lower case, 1 numeral and 1 special character |
| Password Expiry | 90 days at a maximum |
| Password History | Disallow at least the most recently used 4 passwords |
| Account Lockout | 5 consecutive failed attempts |

# The Macro View

- What we focused on so far were the technical aspects
- Most regulatory compliance laws will also focus and impact the software development lifecycle
- Let’s see those next

# People and Process Recommendations



# References


1. Defining the Developer's Role in achieving PCI-DSS compliance (Coming soon) - www.softwaremag.com
2. Regulatory Compliance Demystified: An Introduction to Compliance for Developers - http://msdn.microsoft.com/en-us/library/aa480484.aspx
3. Compliance: What Architects Must Know - http://msdn.microsoft.com/en-us/library/bb421526.aspx

# Questions

Foundstone
Professional Services A DIVISION OF McAFEE


# Developers are from Mars, Compliance Auditors are from Venus

**Neelay S Shah**
**neelay.shah@foundstone.com**

**Rudolph Araujo**
**rudolph.araujo@foundstone.com**

**Foundstone Inc., A Division Of McAfee**

*November 25, 2010*