

# Who's There?

## A Methodology for Selecting Authentication Credentials



VA-SCAN October 5, 2009

Mary Dunker

dunker@vt.edu

# Who's There?

Driving by your house

- Do you care?
- Probably not -- anyone can look

# Who's There?

Knocking at your door (on your property)

- Do you care?
- Probably so.
- What could happen if a person on your property is not who they say they are?

# Who's There?

Letting someone in

- Do you care?
- Very much so.
- What could happen if the “wrong person” enters your home?

# Who's There?

- Key concepts
- Methodology
- Credential selection
- Implementation

# Concepts

- Authentication helps prevent unauthorized access
- Identity authentication error - person using credential is not the one to whom it was issued
- Identity authentication error has consequences
- Negative consequences have impact

# Concepts

- Credentials represent identity to online process
- Personal digital identity – online representation of a real person's identity. Credentials + information about a person
- Personal digital identity has level of assurance (LOA)
- LOA - degree of confidence that a credential belongs to the person using it, and the person to whom the credential was issued is who they say they are
- Personal digital identity with appropriate LOA reduces likelihood of identity authentication error

# Methodology for selecting credentials

1. What is the potential impact if the wrong person gains access to a resource via this application?
2. How does the impact map to a level of assurance in a person's digital identity?
3. What kind of credentials satisfy the LOA? (Multiple factors?)
4. How will you implement the digital credentials in the application?
5. How do you know the authentication method chosen achieves the desired level of assurance?
6. Reassess annually.

# Methodology

## 1. What if the wrong person gains access?

### Types of consequences

- Inconvenience, distress, reputational damage
- Financial loss or liability
- Harm to university programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil, criminal, disciplinary violations

# Methodology

## 1. What if the wrong person gains access?

### Impacts

- **Low** impacts cause inconvenience without lasting effects.
- **Moderate** impacts are more serious short term or limited but long-term.
- **High** impacts have severe adverse effects, resulting in serious long-term damage.
- **Very high** impacts are catastrophic or life threatening, with very serious, irreversible long-term effects.

# Methodology

## 1. What if the wrong person gains access?

### Potential Impact Profile

Consequences	Potential Impact Profile Levels				
	1	2	3	4	5
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High	Very high
Financial loss or university liability	Low	Mod	Mod	High	Very high
Harm to university programs or public interests	N/A	Low	Mod	High	Very high
Unauthorized release of sensitive information	N/A	Low	Mod	High	Very high
Personal safety	N/A	N/A	Low	Mod (or) High	Very high
Civil or criminal violations	N/A	Low	Mod	High	Very high

# Methodology

## Example: Tree trimming in my yard Potential Impact Profile

Consequences	Potential Impact Profile Levels				
	1	2	3	4 ✓	5
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High	Very high
Financial loss or university liability	Low	Mod	Mod	High	Very high
Harm to university programs or public interests	N/A	Low	Mod	High	Very high
Unauthorized release of sensitive information	N/A	Low	Mod	High	Very high
Personal safety	N/A	N/A	Low	Mod (or) High	Very high
Civil or criminal violations	N/A	Low	Mod	High	Very high

# Methodology

2. How do you map the potential impact to a level of assurance in the person's digital identity?

Use a standard like NIST 800-63. A given LOA is backed by trust in identity proofing process and in credential.

## Methodology: Levels of assurance of personal digital identities

LOA	Identity assertion	Identity proofing requirements	Authentication factors	Digital credential examples
0	No identity is asserted.	None	None	No authentication is required . Site is open to public
1	Little or no confidence in the validity of the asserted identity	Some identity information is acquired. Little or no verification is performed.	Single-factor authentication with password	Guest accounts
2	Some confidence that the asserted identity is valid	Some identity information is acquired, with some level of verification.	Single-factor authentication with password or <i>biometric attribute</i>	PID and password; Active Directory ID and password; Oracle ID and password. Finger print reader. Hokie Passport card with photo
3	Moderate degree of confidence in validity of the asserted identity	Matching of the collected identity information is strengthened by additional identity verification from a trusted authority. Identity proofing may be in-person or in some circumstances, remote.	A minimum of two authentication factors is required; i.e., something you know and (something you have or something you are)	Personal digital certificates; finger print readers requiring passwords or PINs,
4	High degree of confidence in the validity of the asserted identity	In-person identity proofing is required, including referencing a biometric attribute.	A minimum of two authentication factors is required, including a cryptographic key stored on a <i>hardware token</i> that does not allow the export of authentication keys.	Personal digital certificate (PDC) on Aladdin eToken USB device protected with password
5	Very high degree of confidence in the validity of the asserted identity	In-person identity proofing is required, including recording a biometric attribute.	Three authentication factors are required, including a biometric attribute and a cryptographic key stored on a hardware token that meets certain technical specifications.	Fingerprint reader with PIN along with physical key

# Credential Selection

3. What credentials are available at your institution for each LOA?
  - ID and password -- most common. Microsoft Active Directory account, e-mail account, Oracle IDs, NetID, guest ID
  - Something you have – USB devices/tokens, smart cards, digital certificates
  - Biometrics

Multiple credential factors increase LOA. Seek guidance from your Identity Management office or Security Office

# Credential Implementation

4. How will you implement the digital credentials in the application? Application developers & integrators may need to learn new methods.
- What authentication methods are available at your institution?
    - Kerberos
    - NTLM
    - NTLMv2
    - LDAPS
    - Client SSL
    - Central Authentication Service (CAS)
    - Shibboleth

# Credential Implementation

4. How will you implement the digital credentials in the application?
  - Do you need single sign-on?
  - Do you need Federated identity management?
  - How will you know the LOA of the credential?

# Implementation

5. Will the authentication method achieve the desired level of assurance?
  - Security Review

# Implementation

## 6. Reassess annually

- Applications change
- Risk vectors change
- Technology changes

# References

## References

- National Institute of Standards and Technology Special Publication 800-63, Electronic Authentication Guideline;  
[http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1\\_Dec2008.pdf](http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf)
- Office of Management Budget M-04-04, E-Authentication Guidance for Federal Agencies;  
<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- University of Wisconsin, Madison, User Authentication and Levels of Assurance;  
<http://www.cio.wisc.edu/security/initiatives/levels.aspx>
- Virginia Tech, Standard for Use of Personal Digital Identities