Knowledge Based Authentication (KBA) Metrics

Santosh Chokhani, Ph.D.

February, 2004

Orion
Security Solutions

Orion
SECURITY SOLUTIONS

Briefing Contents

- Background
- Model for KBA
- Issues and Considerations
- Practical Usage of KBA
- Metrics for KBA
- Applicability to U.S. Government e-authentication
- Summary

Orion
SECURITY SOLUTIONS

Background

- Context is U.S. Government e-authentication initiative as opposed to research or other applications of KBA
- Definition of KBA for this briefing, excludes
  - Password and PIN (addressed separately in NIST e-authentication)
  - Recognition oriented KBA (these systems require "training' the system during initial registration – a luxury that may not be affordable at the lower levels of U.S. Government e-authentication initiative; Note: KBA seen to be more useful at lower levels of U.S. Government e-authentication initiative)

Orion
SECURITY SOLUTIONS

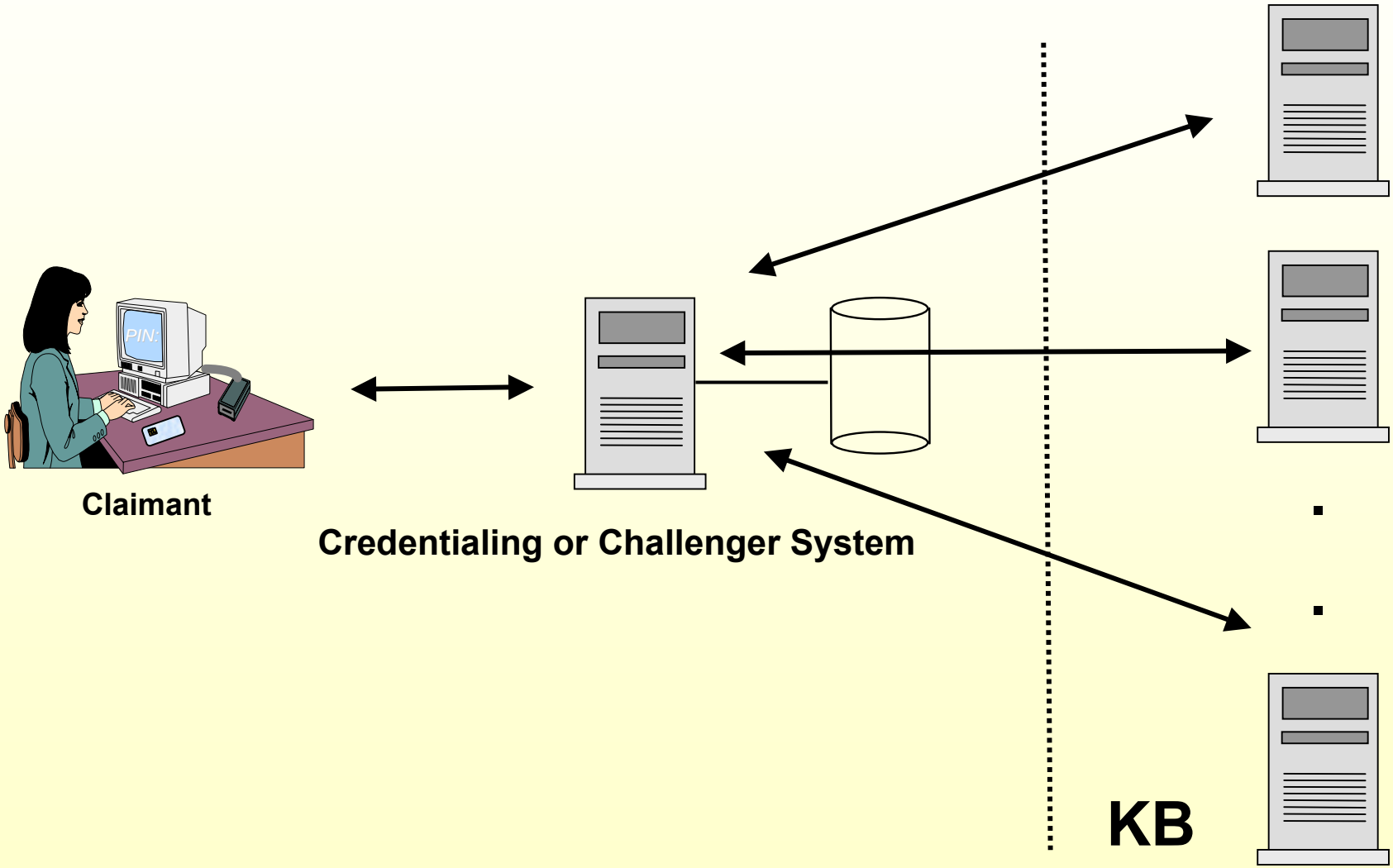
Background

- **Definition of KBA for this briefing, includes**
  - **Factoid recall (personal or otherwise, known to the subscriber, but not likely to be known to others, specially, potential masqueraders)**
  - **Examples: Date of birth, Place of birth, Adjusted Gross Income, Taxes paid, Mother's maiden name, Cell phone number, Credit card number, Favorite team, Favorite team record**
- **Claimant, verifier, relying party terms used in this briefing in accordance with NIST e-authentication guideline**

Purpose of KBA

- **Used for initial registration per e-authentication guideline**
- **e-authentication guideline would like to include KBA as a means for transaction/session authentication:**
  - **Useful for users who rarely authenticate to a system and do not like to register or do not like to manage passwords**
  - **Determine how KBA can provide security commensurate with the requirements of the various e-authentication levels**
  - **KBA will not be able to meet all the security requirements for higher levels**
    - **Level 3 unknown**
    - **Level 4 can not use KBA; it requires a hardware token**

Model for KBA



Considerations in Factoid Selection

- Impact on privacy
- Impact on identity theft
- Availability on other trusted systems for verification
  - Example: Information on pay stub may great candidate for factoids, but is not likely to be available to verifier
- Guessability
- Reliability/Accuracy
- Ease of recall or access to the subscriber/claimant

Orion Security Solutions

Considerations in KBA Design

- KBA factoids can impinge on personal privacy
- KBA factoids can be used by unauthorized persons to conduct identity theft
- To protect against these, KBA implementation requires
  - Strongly protected channel
  - User workstation security a la other authentication mechanisms, except the potential damage due to compromise is bigger
  - Server systems containing the factoids
  - Servers could store one-way hash of factoids in order to minimize insider threat
  - Distribute factoid databases across multiple servers

Considerations in KBA Design

- **KBA design needs to determine how much information to provide in case of authentication failure**
  - **User friendliness Vs providing information to imposter**
  - **Security consideration may mean collect all the data and only provide pass/fail response**
  - **Protected channel minimize off-line attacks except for insiders**
- **Response to authentication failures**
  - **Subscriber notification**
  - **Limited number of attempts**
  - **Account lock out**
  - **Auditing**
  - **Exponential delays**

Considerations in KBA Design

- Redundancy for availability and responsiveness
- Random selection of questions for each session to protect against script and manual threats
- Random ordering of questions for each session to protect against script
- Multiple forms of the same question to protect against script threats
- Providing claimant flexibility to select factoids to use depending on the subscriber's comfort level with verifier system
- Mix of static and dynamic factoids
  - Static factoid example: date of birth
  - Dynamic factoid example: bank balance
- Factoid aggregation impact on privacy
- Factoid aggregation impact on identity theft

Orion Security Solutions

Practical Usage of KBA

- **Basic Requirement**
  - **Strongly protected channel to protect against eavesdropping, replay, etc. to ensure individual privacy and protect against identity theft**
- **Initial registration by checking against existing databases**
- **KBA requires an on-line database or other mechanism to verify the factoids**

Orion Security Solutions

Practical Usage of KBA

- **Transaction authentication should use password or PIN established during initial registration, where initial registration is KBA based**

- **KBA is useful for transaction authentication for user with the following characteristics**
  - **Uses a system rarely; or**
  - **Does not like to register; or**
  - **Does not want to manage PIN or password**

Orion Security Solutions

Metrics for KBA

- **KBA Metrics**
  - **Guessability of factoid**
  - **Guessability of KBA**
  - **Cost of researching factoids**
  - **User acceptance (psychological)**
  - **Ease of use (ergonomics)**
  - **Ease of administration**
  - **Privacy protection**
  - **Identity theft protection**
  - **Commercial products**
  - **Interoperability**
  - **Cost of implementation**

Orion Security Solutions

Guessability of Factoid

- **Depends on the guesser**
  - Spouse/Significant Other/Cohabitant
  - Immediate Family
  - Extended Family
  - Friend
  - Acquaintance
  - Employer – Supervisor
  - Employer – HR
  - Employer – Coworker
  - Accountant
  - Attorney
  - Others
- **Depends on the factoid**
  - Date of birth, Place of birth, Credit card number, AGI, Tax, etc.
- **See table for actual values**

Guessability of KBA

$$P_{KBA,\,j} = \pi_i \, p_{i,\,j}$$

Where: $P_{KBA,\,j}$ **is probability of compromising KBA by j**

j is the claimant type

i is the i^{th} **factoid**

$p_{i,\,j}$ **is the probability of j to guess factoid I**

Assumption: Factoid are mutually independent , which may not be true for all factoids.

Applicability to U.S. Government e-authentication Initiative

- **e-authentication Goal of reducing the service time from weeks to minutes ➔ KBA can be a useful initial registration tool**

- **If KBA is used for transaction authentication, the following must be addressed:**
  - **Insider threat**
  - **Aggregation of data**
  - **Identity theft**
  - **Privacy act**
  - **Availability and response time concerns make validating KB from multiple sources impractical**

Orion Security Solutions

Applicability to U.S. Government e-authentication Initiative

- **Number of factoids used depend on the desired metric and assumptions regarding various types of claimants' desire to masquerade**
  - **Level 1 goal is 1 in 2048 (2^{-11})**
  - **Level 2 goal is 1 in 65K (2^{-16})**
  - **Level 3 goal is 1 in 1M (2^{-20})**

Orion Security Solutions

Sample Metric

- Assume "other" as adversary
- Level 1
  - Always: Name, Address
  - Random two of the following: Credit Card Number, Date of Birth, SSN, Credit Card Amount on Last statement (Probability = 2^{-24})
- Level 2
  - Always: Name, Address, Credit Card Number (2^{-24})
  - Random two of the following: Credit Card Amount on Last statement , AGI, Tax, Bank Balance (Probability = 2^{-20})
- Level 3 -- TBD

Applicability to U.S. Government e-authentication Initiative

- **Initial registration and credential renewal using KBA is acceptable at level 1 since level 1 has no requirements in these areas**
- **Initial registration and credential renewal using KBA is acceptable at level 2 since level 2 requires: verification of credit card number and home address**
- **Initial registration and credential renewal using KBA is acceptable at level 3 since level 3 requires: verification of credit card number and home address; and credit report**
- **KBA not recommended for Level 4 since it requires face to face authentication which provided opportunity to issue PKI or shared secret credentials**

Applicability to U.S. Government e-authentication Initiative

- **Transaction authentication using KBA in general is not recommended unless the subscriber prefers to KBA over credentials**
- **KBA can be used for transaction authentication for levels 1 and 2**
- **Acceptability of KBA for transaction authentication at level 3 requires further discussions with NIST and e-authentication guideline authors**

Orion
Security Solutions

Summary

- KBA metrics is an area of research
- KBA metric (i.e., probability of guessing a factoid) depend on the factoid
- KBA metric for each factoid depend on the personality of the subscriber (introvert, extrovert, other factors in terms of network and size of personal and professional relationships)
- KBA metrics will require assumptions or special considerations for threats from persons known to subscriber

Orion
SECURITY SOLUTIONS

Summary

- **KBA will require strongly protected channels (same as password and PIN, except in this case weak channel could lead to violation of privacy or identify theft)**
- **KBA will require strong assumptions regarding security of the user workstation (same as other authentication mechanisms, except in this case weak channel could lead to violation of privacy or identify theft)**
- **KBA can be deployed to protect against disclosure to verifier and relying party**
- **KBA more suited for initial registration**

Orion
SECURITY SOLUTIONS

Questions