Thomas J. Watson Research Center

# Privacy and Security Threat Analysis of the Federal Employee Personal Identity Verification (PIV) Program

**Paul A. Karger**

**karger@watson.ibm.com**

# Outline

- **Identify specific problem with FIPS 201**
- **Problem of multiple authentication protocol options**
- **Recommend use of single, formally proven secure, standards-based authentication protocol**

# Homeland Security Presidential Directive 12

- **HSPD 12 – August 2004**
- **Government-wide standard for identification of**
  - Federal Employees and Contractors
  - Primarily for access to federal buildings, world-wide
- **Must be "secure and reliable"**
- **NIST developed**
  - Federal Information Processing Standard (FIPS) 201
    - Plus series of accompanying documents
  - Two kinds of cards – PIV I and PIV II
    - PIV I is for quick deployment for single agencies
    - PIV II is for inter-agency interoperability – focus of this talk

# What is “Secure and Reliable” Identification?

- **Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation**
- **Can be rapidly authenticated electronically**
- **Strong criteria for verifying employee’s identity**
- **Issued only by accredited providers**

# Contact and Contactless Smart Cards

- **FIPS 201 requires dual-interface smart cards**
  - Contact cards must be inserted into a reader – provide better security
  - Contactless cards communicate via radio frequencies and therefore could be intercepted
    - Contactless smart cards are similar to RFID tags, but use different standards and have more powerful computational abilities
- **Contactless smart cards receive broadcast power from the reader and have no batteries**
- **RF transmissions can be intercepted**
- **Reports of successful interceptions at distances from 9 to 50 meters. Interception is MUCH easier when the card is in use and powered by a legitimate reader**
- **Therefore, encryption is essential for security, but FIPS 201 does not require encryption over the contactless interface**

# Card Holder Unique ID (CHUID)

- **CHUID evolved from an earlier DoD working group (SEIWG-12) that included a social security account number (SSAN) as part of the unique ID of a card holder**
  - DoD puts the SSAN on all military IDs
  - Due to potential identity theft problems, the newer CHUID strongly discourages the use of SSAN
  - CHUID includes a number of other fields including an agency code that identifies for which federal agency the card holder works

# CHUID transmitted in cleartext

- **FIPS 201 explicitly declares that reading the CHUID is not a privileged operation, and therefore need not be encrypted**
- **Agency code (part of CHUID) is sensitive information**
  - Very fine grained code
    - 12K3 = Animal and Plant Health Inspection Service
    - 571A = Air Force Command and Control (C2) & Intelligence, Surveillance and Reconnaissance
  - This level of detail could be of great interest to an eavesdropper, and could put federal employees in danger

# Attack Scenarios Using Agency Code

- **Espionage agents**
  - Select individuals likely to have high security clearances to recruit as spies
- **Terrorists**
  - Select individuals to target for kidnapping or assassination
  - Encryption could NOT prevent identification if terrorist gets physical access to the ID card, as in TWA 847 hijacking
  - Encryption could interfere with attempt by terrorists to select particular targets off the street, as in the DC sniper case
- **Journalists**
  - Identify Valerie Plame as a CIA employee just by remotely reading her FIPS 201 card

# Outline

- **Identify specific problem with FIPS 201**
- **Problem of multiple authentication protocol options**
- **Recommend use of single, formally proven secure, standards-based authentication protocol**

# Usability Issues

- **For cardholder, usability is excellent**
  - Contactless smart cards merely need to be waved near the readers
- **For agency developers, usability is not good**
  - FIPS 201 is supposed to provide inter-agency interoperability, but it offers many options for authentication that will make interoperability difficult
  - Furthermore, it assumes that each agency can make good security choices, yet it is well-known that selecting appropriate wireless security protocols is very difficult
  - Each agency will choose its own card vendors

# Recommendation

- **Even if just one agency's cards are broken, there could be serious problems for the employees**
- **Require a single, proven to be secure, authentication protocol for ALL agencies**
  - Assures interoperability
  - Removes agency need to have in-house cryptographic experts
- **IBM has developed such a protocol and offered it to various standardization bodies**
  - Caernarvon authentication protocol

# Outline

- **Identify specific problem with FIPS 201**
- **Problem of multiple authentication protocol options**
- **Recommend use of single, formally proven secure, standards-based authentication protocol**

# Caernarvon Castle – North Wales

# Privacy Preserving Protocol

- **Based on SIGMA (SIGn and Mac) family of protocols, including IKE**
  - Part of IPSEC
  - Formally proven
- **SIGMA protocols better protect privacy**
  - Key is negotiated before any identities are exchanged
  - Once key is agreed upon, all further communications are encrypted
- **Caernarvon protocol**
  - Requires that the reader authenticate first, then the card
    - Underlying protocol is symmetric, but someone has to go first
    - Needs for privacy are NOT symmetric
  - Once the reader has authenticated, the card can make a security policy determination of whether to reveal the card holder's identify

# Non-Mathematical Summary of Protocol

- **First, the reader and the card negotiate a Diffie-Hellman session key**

  This provides cryptographic privacy for all subsequent messages

  No authentication has taken place yet – neither the reader nor the card knows who is on the other end – they only know that eavesdroppers have been excluded
- **Second, the reader authenticates itself to the card**
- **Third, to protect the privacy of the card holder, the card now decides whether this particular reader is authorized**
- **Only if the reader is authorized, the card finally reveals the card holder's identity, so that the reader can decide whether the card holder is to be allowed access.**

# Standards Process

- **IBM has submitted the Caernarvon Authentication Protocol for international standardization as part of the European Electronic Signature effort**
  - IBM has not asserted IP rights over the protocol
  - Based on existing IKE standards in IPSEC
- **Part of a draft CEN standard**
- **When completed, the CEN standard will be submitted to ISO**

# Conclusions

- **Problem: FIPS 201 has weaknesses**

  CHUID is transmitted unencrypted putting card holder safety at risk

  Inter-agency interoperability will be difficult to achieve

  Each agency has to make difficult security trade-offs without good guidance

- **Problem: Does this meet HSPD-12?**

  Is it “strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation”?

- **Solution: Fix the next version of FIPS 201 by mandating a formally proven, standards-compliant, privacy-preserving protocol for ALL cards**

- **Solution: Limit use to PIV I (no interagency authentication) for now**

# Backup Slides

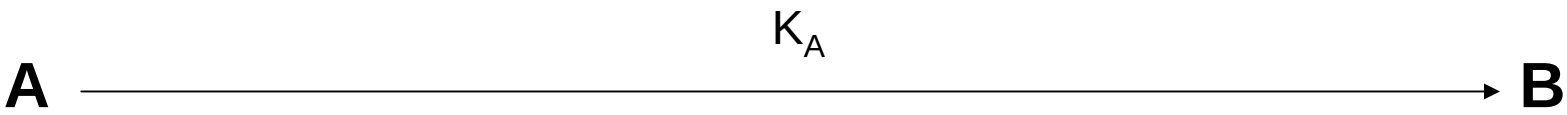
- **Mathematical summary of the protocol**

# Algorithms

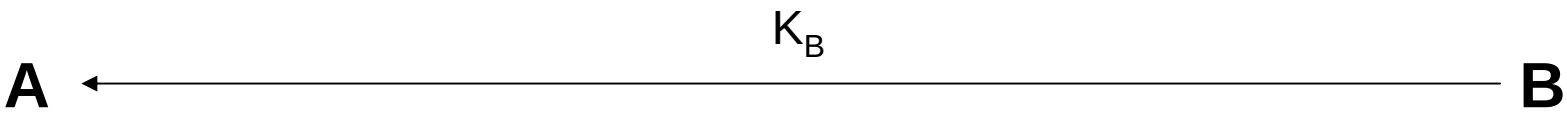
- **Protocol can use elliptic curves and AES algorithms**
- **Examples that follow use regular Diffie-Hellman, RSA signatures, and triple DES, because our first prototype smart card chip only supported those algorithms**

# Privacy Preserving Protocol 1
# Simple Diffie-Hellman

- A chooses a random number a with $1 \leq a \leq q-1$, computes a key token $K_A = g^a \bmod p$, and transmits it to B.




- B chooses a random number b with $1 \leq b \leq q-1$, computes a key token $K_B = g^b \bmod p$, and transmits it to A.




- Neither A nor B has revealed his identity. They now can compute a mutual key $K_{AB,}$ as in simple Diffie-Hellman, and then derive encrypting and message authentication keys, $K_{ENC}$ and $K_{MAC}$
- Since we have a session key, the rest of the protocol is protected from third-party eavesdroppers.

# Privacy Preserving Protocol 2
# Reader Proves Identity

- A sends its certificate to B by encrypting it with $K_{ENC}$.
  A computes: $E_{01} = 3DES_{K_{ENC}}(Cert(A))$


- B responds with a challenge


- A now computes:
  $E_1 = 3DES_{K_{ENC}}(A \mid Sig_{SK_A}[K_A \mid A \mid RND.B \mid K_B \mid DH(g \mid p \mid q)])$
  Diffie-Hellman key parameters are included to provide their authenticity

# Access Control Decisions

- **At this point, the smart card can check the reader's identity, and make a policy decision about the reader.**

- **Any security policy could be implemented here**

  Even no policy at all

# Privacy Preserving Protocol 3
# Card Proves Identity

- B sends its certificate to A by encrypting it with $K_{ENC}$.
  B computes: $E_{02} = 3DES_{K_{ENC}}(Cert(B))$


- A responds with a challenge


- B now computes:
  $E_2 = 3DES_{K_{ENC}}(B \mid Sig_{SK_B}[K_B \mid B \mid RND.A \mid K_A])$


- Finally, the reader can now verify the card's identity, make its own access control policy decisions and proceed.