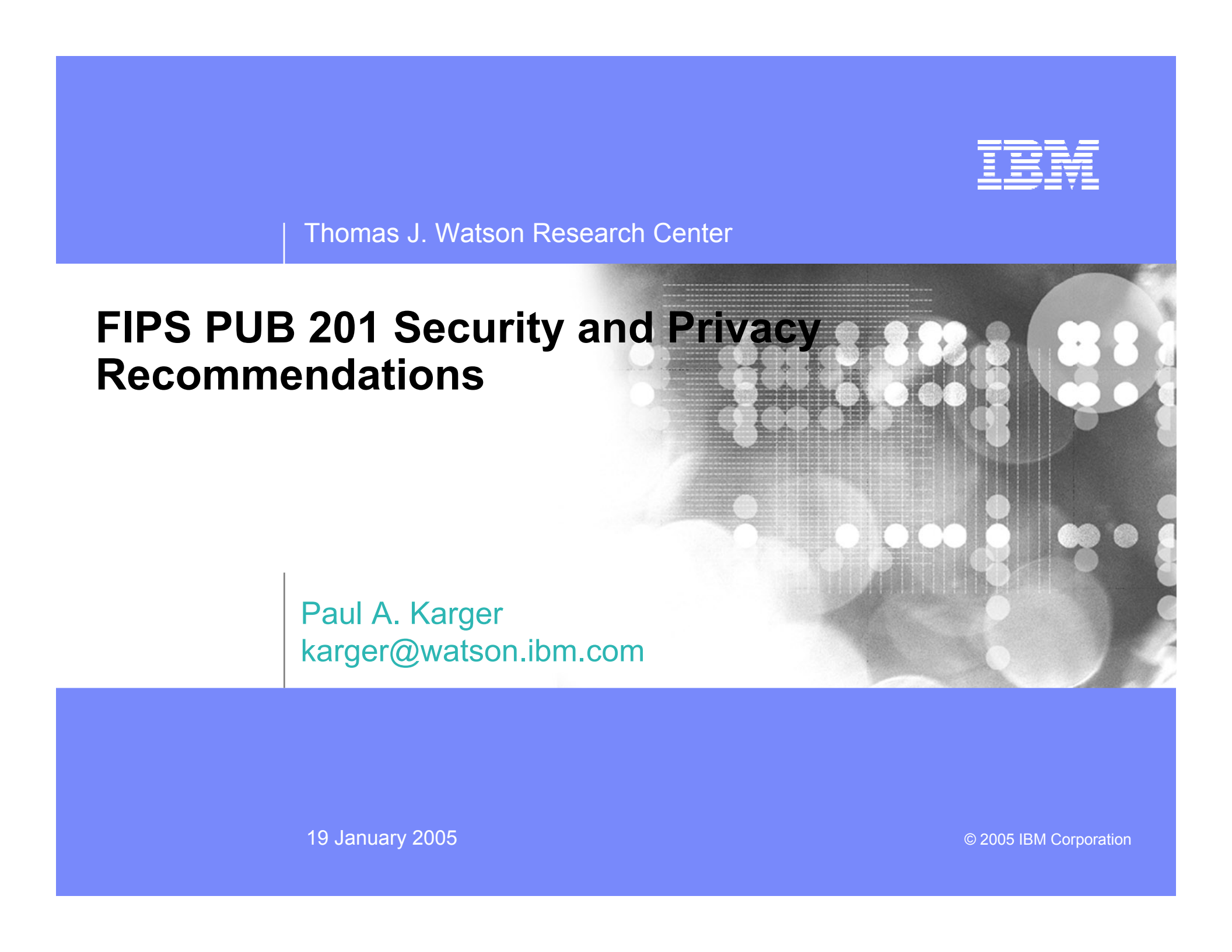
RC23871 (W0501-049) January 14, 2005
Computer Science

IBM Research Report

FIPS PUB 201 Security and Privacy Recommendations

Paul A. Karger
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich



Thomas J. Watson Research Center

FIPS PUB 201 Security and Privacy Recommendations

Paul A. Karger
karger@watson.ibm.com

19 January 2005

FIPS PUB 201

- Personal Identity Verification (PIV) for Federal Employees and Contractors
- Required by Homeland Security Presidential Directive 12
- Smart card-based identity cards
- Both contact and contactless
- Include biometric facial images and fingerprints

Security and Privacy Concerns

- Draft FIPS PUB 201 does a good job of identifying many security and privacy threats
- However, some threats are missing or are understated
- Purpose of this talk
  - Identify additional threats and vulnerabilities
  - Offer recommendations on how to deal with these on a practical basis with current smart card technology
    - Short time frame requirements of Homeland Security Presidential Directive 12 limit the kinds of technology that can be employed

General Principles behind our Recommendations

- Protect sensitive information from
  - Casual eavesdropping
  - Lost or stolen card
  - Active probing attacks
- Compromising one card should not compromise other cards
- Applications should not interfere with other applications

PACS Assurance Level Profiles

- Good: Recommended authentication techniques change, based on Physical Access Control System (PACS) Assurance Levels
  - Not all agencies and locations need the same level of security
- Problem: Same identity card may be used at different sites with different PACS assurance level profiles
  - Sensitive information could be revealed at one site with a low or medium assurance level profile that would have been better protected at a high assurance site

Contactless Smart Card Threats

- Contactless smart cards communicate via radio signals that can be picked up by unauthorized readers
  - Recent RISKS Digest 23.62 (21 Dec 2004) reports RFID transmissions unintentionally being picked up through hospital room walls
  - RFID is similar, but not identical to contactless smart cards
- Current draft wisely recommends biometrics data be encrypted over contactless, but…
- Recommendation: Extend encryption to CHUID data
  - Position sensitivity is allowed over the contactless interface
  - Reveals card holder's clearance level
  - Could make card holder a target for kidnapping by terrorists

Use of symmetric master keys

- PACS High Assurance profile requires a site-specific challenge-response keyed protocol
  - Good improvement
  - But the keyed protocol uses site-specific symmetric master keys
- Some smart cards may be vulnerable to a variety of physical attacks
  - Clock glitching, light attacks, etc.
  - Side channel cryptanalysis (both of power and of RF emanations)
- Physical attacks might reveal the site-specific symmetric master keys on a particular card
  - Next slide discusses why this is a problem

Scenario for attacking a master-key based protocol

- Attackers get access to one FIPS PUB 201 credential
  - Convince card holder to use card in a tampered reader
  - Acquire a lost or stolen card
- Carry out physical attack or side-channel cryptanalysis to learn the symmetric master key of that card
- Now use that symmetric master key to spoof other cards, possibly over contactless interface as card holder walks by with card in pocket
  - Once spoofed, the attacker could then extract the digitally signed biometrics or other sensitive information that could then be used for forgery or identity theft
- Better approach is to use asymmetric public-key algorithms – even if a particular card is successfully broken, nothing is revealed that could compromise other cards

Downloaded Applications

- NIST Special Publication 800-73 includes APDUs for downloading applications onto FIPS 201 identity cards
- While JavaCard has features to keep downloaded applications separate, these features have theoretical limitations and have not yet been proven to withstand sophisticated attacks
- It would be much safer, particularly given the short time frame requirements for FIPS 201, that downloading new applications not be permitted, particularly for cards intended for use in PACS High Assurance Profile locations

Privacy-Preserving Authentication Protocol

- IBM has developed a new smart card authentication protocol to address these kinds of threats
  - No other known smart card authentication protocol meets all these requirements
  - IBM has offered this for standardization on a royalty-free basis
- This authentication protocol could be implemented NOW in conventional smart card operating systems such as JavaCard
- Protocol was published at ESORICS 2003 conference

Goals of Authentication Protocol

- Privacy protection for the smart card holder
  - Existing standards for smart card authentication unnecessarily expose card holder's identity
- Protocol proven correct – useful for passing EAL6 or EAL7
  - Based on Sigma family of protocols used for IKE
  - Submitted to standards groups
    - E-Sign
    - Open Platform

Problems with ISO/IEC 11770-3 and DIN V66291

- Standards for Authenticated Diffie-Hellman
  - DIN V66291 is implementation standard for German Digital Signature Law
- Cardholder must reveal identity to unknown reader
  - Bogus smart card reader could track cardholder movements
  - Particularly a problem for contactless smart cards
  - Bogus reader could use illegally high power setting to reach cards carried by unsuspecting people
  - Analogous to RFID privacy issues
- Passive eavesdropper can determine both identities
  - Contactless environment
  - Internet tunneling

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
- Our 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
  - Examples use triple DES and RSA, but AES or elliptic curves could also be used

Standards

- IBM has not kept the authentication protocol proprietary
  - Based on IKE that is already a standard part of IPSEC
- We have submitted it to
  - E-Sign
  - Global Platform
- Proposal is for E-Sign and Global Platform to permit, but not require the use of this protocol
  - Existing smart card infrastructures remain standards compliant
  - New infrastructures can be deployed to better protect privacy and to support various security policies, including mandatory access controls
- E-Sign has incorporated the privacy-preserving protocol and is on fast track to become European standard, and then ISO standard

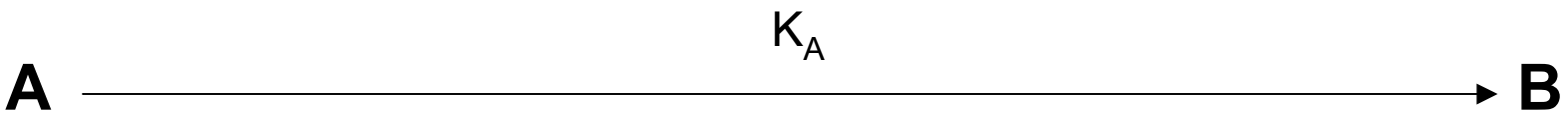
Summary of Recommendations

- FIPS PUB 201 needs to consider some additional privacy and security threats
  - Particularly for cards that may be used at multiple sites with DIFFERENT security requirements
  - Information flow over contactless should generally be encrypted
  - Cards need to be FIPS 140-2 evaluated to ensure adequate resistance to possible attacks
- IBM's privacy-preserving authentication protocol could be very helpful for this, and is on standards track for wide availability without IP restrictions
- Seriously consider restricting the ability to download new applications onto these cards until stronger smart card operating systems are available

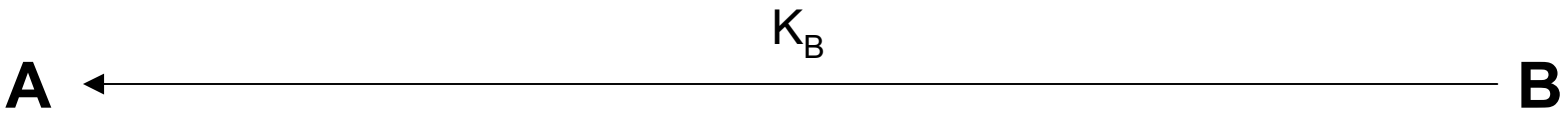
Backup Slides

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.



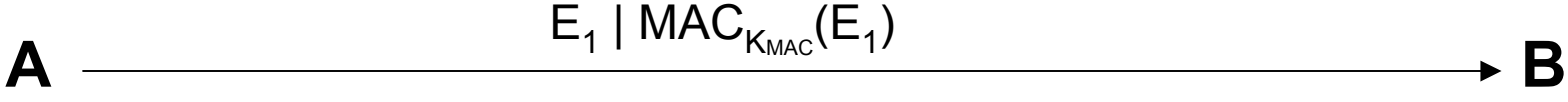
- Neither A nor B has revealed his identity. They now can compute a mutual key $K_{AB,}$ as in simple Diffie-Hellman, and then derive encrypting and message authentication keys, K_{ENC} and K_{MAC}
- Since we have a session key, the rest of the protocol is protected from third-party eavesdroppers.

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

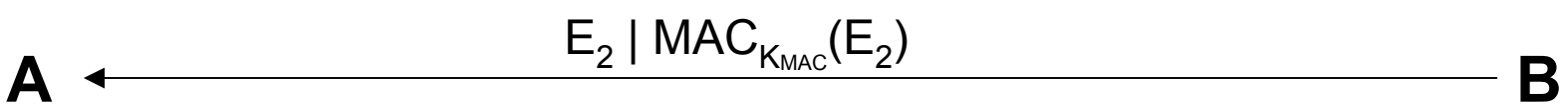
- At this point, smart card can check the reader's identity, and make an access control policy decision about the reader.
- Any security policy could be implemented here
  - Even no policy at all

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 mandatory access control policy decisions and proceed.