

1996:
The Cryptography Year
in Review

Outline

- Research
 - Recent attacks on cryptosystems and their impact
 - Practice-oriented provable security
 - New infrastructures for public-key cryptography

Research

- !Recent cryptanalytic results
 - attacks on smart card security
 - factorization of RSA-130
 - attacks on hash functions
- Practice-oriented provable security
 - HMAC: a new secure MAC
 - PSS!: data formatting for RSA signature
 - DESX: its security against key search
- New public-key infrastructure

Attacks on Smart Card Security

- First announced by Bellcore in Sept. 1996
 - Boneh, DeMillo, Lipton
 - Form of attack: recover keys in smart cards by introducing errors into key-dependent crypto operations through physical intrusions
 - apply the attack to certain public-key systems
- Soon extended by several researchers
 - Biham, Shamir
 - “differential fault analysis” on block ciphers
 - Anderson, Kuhn; ISS of Singapore

Impact of the Attacks

- At the current stage, the Bellcore attack is mainly of theoretical interest
 - no successful implementation of the attack on actual crypto devices has been reported
- Importance and relevance to secure hardware design should not be overlooked
 - security involves !more than just good algorithms
 - good engineering is essential

How to Overcome the Attacks

- Do not produce an output if intrusion into the device is detected
- Verify the correctness of the result before outputting it
 - e.g., signature verification
 - may incur overhead; need further research
 - e.g., probabilistic signature scheme (PSS)
 - randomness needs to be concealed in the output

RSA-130 is Factored

- What is RSA-130?
 - a composite number of 130 decimal digits, listed as part of the RSADSI Factoring Challenge
 - factored in Apr. 1996 by a group of researchers
- Some big numbers factored in past years

Impact of the Factorization of RSA-130

- Confirmed that for very large general-purpose factorizations, g.n.f.s. is the algorithm of choice
- 512-bit RSA modulus (less than 160 digits) can be anticipated to offer marginal security
- Factoring a 768-bit RSA modulus would require about 10^8 MIPS-years with current techniques
 - this is the minimum length of modulus currently recommended by DSA Labs

Attacks on Hash Functions

- General design approach for hash functions
 - iterative structure based on a compression function
 - in particular, MD4 has been used as the basis for the design of many other hash functions
- Recent attacks
 - Mostly done by Dobbertin (1995, 1996)
 - collisions of the reduced-round RIPEMD
 - collisions of MD4
 - collisions of the MD5 compression function

Status of Hash Functions

- !inMD4
 - collisions found; should not be used
- MD5, MD2
 - collisions for the compression function found
 - existing signatures formed by them are not at risk
 - remain suitable for use as one-way hash functions
 - should not be used for future applications requiring collision-resistant property

Practice-Oriented Provable Security

Motivation

- What do we have?
 - concrete primitives (math operations)
 - DES:
 $(P, K) \rightarrow C!$
 - fs20
 - MD5:
 $M \rightarrow h(M)$
 - RSA:
 $x \rightarrow x^e \bmod n$
 - Usually, input and

Practice-Oriented Provable Security

General Approach

- Formalize definitions of primitives (e.g., a hash function)
- schemes (e.g., a MAC)
- Construct schemes based on primitives
- Prove security
 - assumption: primitives are good (e.g., RSA is a good trapdoor one-way function)
 - reduction in the proof:
if there is an attack on the scheme, then there

HMAC: A Secure MAC

- Bellare, Canetti, Krawczyk (Crypto'96)
- Construction is based a hash function H
- $\text{HMAC}(\text{text}, \text{key})$
- $= H(\text{key} \oplus \text{opad}, H(\text{key} \oplus \text{ipad}, \text{text}))$
 - opad, ipad are two fixed 64-byte strings
 -
- HMAC was recently chosen by the IPSEC workgroup of IETF

PSS: Probabilistic Signature Scheme

- Bellare, Rogaway (Eurocrypt'96)
- Data formatting for RSA signature: $S = M!ain^d \bmod N$
 - $w = H(M||r)$
 - formatted block = $w || (M|| 00...00) \oplus G(w)$
 - r is a random number; G is based on a hash function
 - counterpart to OAEP for RSA encryption
 - under consideration by IEEE P1363 standard
 - !ainfor PKCS #1:

DESX: Its Security against Key Search

- DESX (designed by Rivest)
 - $\text{DESX}_{k, k1, k2}(x) = \text{DES}_k(x \oplus k1) \oplus k2$
 - a DESX key has $56+64+64 = 184$ bits
- Security analysis of DESX
 - Killian, Rogaway (Crypto' 96)
 - effective key length of DESX at least $118 - \lg m$ bits
 - assume that the attacker sees m plaintext blocks and their encryption under DESX
 - DESX has proven stronger than DES against

New Public-Key Infrastructures

- Motivations
 - slow development of PK infrastructure
 - existing proposals are
 - too complex (ASN.1 encoding, for example)
 - inadequate for developing secure distributed systems
- Some new proposals in the area
 - SDSI (Rivest, Lampson)
 - SPKI (Ellison, Frantz, Thomas)
 - PolicyMaker (Blaze, Feigenbaum, Lacy)

SDSI: Simple distributed Secure Infrastructure

- Keys are “Principals”
 - a principal is the private key that signs statements, and it is identified with the corresponding public key
- Names are always local
 - a principal can use arbitrary local names
 - maintain a principal can export bindings of names to values (e.g., principals or group definitions) by issuing corresponding certificates

SDSI Certificates

- Certificates are signed statements
- Certificates may bind names to values, describe the owner of public key, or serve other functions
-
- !ard 2 (Cert:
 (Local-Name: “Lisa Yin”)
 (Value: (Principal: ...))
 (Signed:
 (...)))

SPKI: Simple Public Key Infrastructure

- Certificates have two primary characteristics
 - authorization and delegation of authority are explicit, never assumed as they traditionally are with identity certificates
 - designed to be simple to implement
- SPKI supports SDSI fully
 - in particular, it supports SDSI names

SPKI Certificates

- An SPKI certificate body consists of a 5-tuple: $\langle I, S, D, A, V \rangle$
 - I: Issuer (a principal which can speak)
 - S: Subject (a principal or object being spoken about)
 - D: An integer (the permission to delegate A)
 - A: A specific authorization (possibly parameterized)
 - V: Validity period or other conditions
- Every certificate format currently known

Standards Activities

- IEEE P1363
 - a comprehensive standard for public-key cryptography
- RSA Labs' PKCS series
 - preview of the next generation
- SET
 - !a standard for securing payment card transactions over open networks

What is P1363?

- Emerging IEEE standard for public-key cryptography
 - discrete logarithm systems
 - elliptic curve systems
 - integer factorization systems
- A set of tools from which implementations, other standards can be built

Highlights of P1363

- Comprehensive
 - key generation and representation
 - key agreement, encryption, and digital signatures
- Separation of primitives and schemes
 - implementation can be compliant to either

Status of P1363

- First meeting Jan. 1994
- Most recent meeting Nov. 1996
 - version 1
 - more established techniques
 - draft available for review
 - version 2
 - more advanced techniques
 - contributions available, more solicited
- Balloting of version 1 in 1997

What is PKCS ?

- RSA Labs' Public-Key Crypto Standards
 - a series of standards first published in 1993
 - basis for many other standards
 - very widely used
- Events after the genesis of PKCS
 - new crypto algorithms
 - “provably secure” schemes
 - emerging standards
 - !

PKCS: The Next Generation

- Changes and additions in consideration
 - #1 (RSA), #3 (DH), #7 (Crypto Message Syntax)
 - add P1363 support (e.g., OAEP, elliptic curve methods)
 - #5 (Password-Based Encryption)
 - #6 (Extended Certificate Syntax)
 - superseded by X.509 version 3
 - #12 (Personal Information Exchange Syntax)
 - a possible new document

PKCS #11 and PICA

- PKCS #11: Cryptographic Token API
 - emerging de facto standard for programming interface to tokens
 - v1.0 published in April 1995
 - v1.1 final spec under construction
- PICA
 - platform-independent cryptographic API
 - initiated by a consortium of companies
 - currently soliciting suggestions

SET: Secure Electronic Transaction

- A new and secure way of getting the most from the electronic commerce market
-

Status of SET

- Announced by Visa and MasterCard, with others in the industry, in Feb. 1996
- June 1996 SET spec includes
 - Card
 - s253business description
 - protocol description
 - programmer's guide
- Ongoing implementation effort
- Updated spec is expected by the end of

1997 Outlook

- DES replacement research continues
- More provable security
- Smart card security
- System cryptography
- TRUST

The Growth of RSA Laboratories

- RSA Labs is the research and consulting division of RSADSI / Security Dynamics
- !6 As of Sept. 1996, two locations
 - Redwood City, CA and Boston, MA
- Complementary and collaborative efforts
 - cryptographic technology
 - security technology
 - security assurance
- !270Contacting RSA Labs