``Chaffing and Winnowing" & Crypto Policy Comments

Ronald L. Rivest

Cryptography and Information Security Group

MIT Lab for Computer Science

April 1998

Outline

- Confidentiality and Authentication
- Chaffing and Winnowing
- Comments on Crypto Policy

Confidentiality

- A message is *confidential* if it can only be understood by the intended recipient. (An eavesdropper does not get the message.
- There are two standard ways of achieving confidentiality:
  - *steganography:* hiding the real message inside a larger one
  - *encryption:* transforming the plaintext message into ciphertext, using cryptography
- We add a third: *chaffing and winnowing*.

Authentication

- A message has been *authenticated* if the recipient can reliably identify the sender and confirm that the message was received exactly as sent.
- There are two standard authentication techniques:
  - *Public-key Digital Signatures* (e.g. RSA, DSS)
  - *Message Authentication Codes* (or *MAC's,* e.g. HMAC), based on a secret key shared between sender and receiver.

Confidentiality vs Authentication

- These are traditionally viewed as separate goals, achievable by separate techniques.
- ``Key recovery'' advocates normally focus on encryption, and ignore escrow or recovery of authentication keys.
- The new chaffing technique demonstrates that you can obtain confidentiality using Message Authentication Codes.

How do MAC's work?

- Divide a message into blocks (packets).
- Append to each block a MAC computed from message block and secret key:

```
Message = "Hi Alice"      MAC = "89310"
Message = "See you soon"  MAC = "32451"
Message = "Love, Bob"     MAC = "24550"
```

- Receiver can re-compute, and check, each MAC using the same secret key. Blocks with bad MAC's can be discarded as damaged or forged.

MAC's are not encryption

- An eavesdropper still sees the message.
- There is no way to ``decrypt'' a MAC to obtain the message block. Indeed, the message block may be 1000 times as long as the MAC. The receiver recomputes the MAC from the message block and the secret key in the same way the sender did.
- Software that uses MAC's for authentication are routinely approved for export.

What is Chaffing?

- Chaffing is the process of adding bogus message blocks with bogus MAC's to an authenticated message:

```
"Hi Al", 74522                      <-- chaff
"Hi Alice", 89310
"See you soon", 32451
"4PM at Oval Office", 32316   <-- chaff
"Love, Bob", 24550
"Bill", 36799                       <-- chaff
```

Chaffing provides confidentiality

- Without knowing the secret MAC key, an eavesdropper can't tell the good packets (wheat) from the bogus (chaff):

```
"Hi Al", 74522                          ??
"Hi Alice", 89310                       ??
"See you soon", 32451                   ??
"4PM at Oval Office", 32316             ??
"Love, Bob", 24550                      ??
"Bill", 36799                           ??
```

Small packets give more confidentiality

- Imagine packets were only one letter long:

HABTUDVIXWTUQOPWEUEGECATHNEAN

(MACs not shown)

- But now we show letters with good MACs:

HABTUDVIXWTUQOPWEUEGECATHNEAN

==> HI PETE

- Bit-by-bit packets are even more secure.
- Other techniques can also yield high degree of security while using larger packets.

Third party can add chaff!

- Note that Alice and Bob may not even care for confidentiality; they just use MACs for authentication of message contents.
- A third party (Charles) can add chaff, *without knowing secret authentication key!*
- Alice and Bob are not encrypting.
- Charles has no secret key to give to recover.

Alice can be framed

- We note that since anyone can add chaff, Alice could be framed for violating a (hypothetical) anti-confidentiality law by a rogue LE agent who added chaff himself.

Alice can hide many messages

- By using several authentication keys, Alice can hide more than one message in the chaff.
- When challenged by LE to reveal her authentication key, she could yield one that discloses an innocuous message, while "real" message is still buried in the chaff.

Policy implications

- Any crypto policy that required recovery of encryption keys would also have to require recovery of message authentication keys.
- But: knowledge of message authentication keys allows impersonation! Why should LE be able to impersonate one Federal Reserve Bank to another???
- Authentication keys are foundation of integrity of information infrastructure; their compromise could be catastrophic.

Digital Signatures still OK

- Note that chaffing and winnowing only works for MACs, not digital signatures, since anyone can verify a digital signature using public key of signer.
- LE would not need access to signature keys.

Do CA's relate to policy?

- Certificate authorities must not escrow private signing keys; only signer herself should know her signing key.
- Certificate authorities should not know (or escrow) encryption or MAC keys, since these are usually ephemeral (per session).
- Trying to burden CA's with key escrow or recovery responsibility is likely to make them economically unviable.
- ==> CA's can not implement crypto policy.

A Metaphor: Crypto = Gloves

- Imagine that gloves just dropped in price from $10,000/pair to $10/pair.
- Gloves, like crypto, are *protective:*
  - Gardener, electrician, doctor, skier.
- Gloves, like crypto, are cheap, importable.
- Nearly everyone uses gloves.
- LE complains that gloves leave no fingerprints, and wants mfrs to make only "fingerprint-recovery'' gloves…(!?)

My recommendations

- No restrictions on domestic use of cryptography. (This is NRC recommendation.)
- Increase LE budget to compensate for increased difficulty crypto may cause them.
- Remove all export regs once GAO determines that there are more than 1,000 foreign crypto products for sale with "strong crypto" (56 bits or above), except to Iraq, etc. (Now are hundreds of products.)