The HMAC brawl

Daniel J. Bernstein
University of Illinois at Chicago

2012.02.19 Koblitz–Menezes "Another look at HMAC":

"... Third, we describe a fundamental flaw in Bellare's 2006 security proof for HMAC, and show that with the flaw removed the proof gives a security guarantee that is of little value in practice."

2012.03.02: "Bellare contacted us and told us that he strongly objected to our language—especially the word 'flaw'—..."

Yehuda Lindell: "This time they really outdid themselves since there is actually no error. Rather the proof of security is in the non-uniform model, which they appear to not be familiar with. ... There is NO FLAW here whatsoever."

Jonathan Katz: "Many researchers are justifiably concerned about the fact that Alfred Menezes will be giving an invited talk at Eurocrypt 2012 related to his line of papers criticizing provable security. I share this concern."

2012.03.17 Koblitz–Menezes:
“. . . Third, we describe a fundamental defect from a practice-oriented standpoint in Bellare’s 2006 security result for HMAC, and show that with this defect removed his proof gives a security guarantee that is of little value in practice.”

2012.03.17 Koblitz–Menezes:
"... Third, we describe a fundamental defect from a practice-oriented standpoint in Bellare's 2006 security result for HMAC, and show that with this defect removed his proof gives a security guarantee that is of little value in practice."

What's going on here?

Classic Bellare–Kilian–Rogaway metric for cipher insecurity:

"The maximum,
over all adversaries
restricted to q' input-output
examples and execution time t',
of the 'advantage'
that the adversary has
in the game of distinguishing
[the cipher for a secret key]
from a random permutation."

2005 Bellare–Rogaway:

"For example we might conjecture something like [DES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{DES}}}{2^{55}} + c_2 \cdot \frac{q}{2^{40}}$$

... In other words,
we are conjecturing that the best attacks are either exhaustive key search or linear cryptanalysis.
We might be bolder with regard to AES and conjecture something like [AES insecurity]

$$\leq c_1 \cdot \frac{t/T_{\mathsf{AES}}}{2^{128}} + c_2 \cdot \frac{q}{2^{128}}."$$

2006 Bellare NMAC theorem:
(q, t) insecurity of NMAC-H
$\leq$ particular function of
(q', t') insecurity of the
compression function inside H.

Quantitative summary:
"Assume that the best attack
against h as a PRF
is exhaustive key search. . . .
The bound justifies NMAC
up to roughly $2^{c/2}/m$ queries."

HMAC: similar story, with
key-derivation complications.

Problem: The metric maximizes over *all* time-t algorithms, not just the algorithms we know.

Can spend a very long time precomputing the algorithm. t counts algorithm run time, not precomputation time.

Problem: The metric maximizes
over *all* time-t algorithms,
not just the algorithms we know.

Can spend a very long time
precomputing the algorithm.
t counts algorithm run time,
not precomputation time.

e.g. There *exists* an algorithm
finding AES key in time $\approx 2^{85}$
given a few known plaintexts.

e.g. There exists a *fast* algorithm
breaking AES, chance $\approx 2^{-64}$.

Inescapable conclusions:

The Bellare–Rogaway conjectures are false.

Inescapable conclusions:

The Bellare–Rogaway conjectures are false.

The Bellare assumption is false.

Inescapable conclusions:

The Bellare–Rogaway conjectures are false.

The Bellare assumption is false.

Koblitz–Menezes analysis: 2006 Bellare proof says nothing if you use HMAC-SHA-1 for 2^{30} medium-length messages; Bellare claim was 2^{60}.

Inescapable conclusions:

The Bellare–Rogaway conjectures are false.

The Bellare assumption is false.

Koblitz–Menezes analysis: 2006 Bellare proof says nothing if you use HMAC-SHA-1 for 2^{30} medium-length messages; Bellare claim was 2^{60}.

The classic metric is busted: massively inaccurate measure of actual cryptanalysis.

Fix metric by focusing on algorithms we know?
Kills non-constructive proofs, including 2006 Bellare proof and much more of literature.

Fix metric by switching from "time" to number of NANDs?
Kills many proofs in literature (e.g., repeated-query elimination becomes much more expensive), and still breaks all ciphers.

Fix metric by switching to circuit AT? Might save ciphers, but kills most proofs in literature.