Insecurity of Tweak Chain Hashing

ECS 227 (Fall 2003)

Thomas Ristenpart

Abstract

In [1], Liskov et al. present the idea of a tweakable block-cipher. A tweakable block-cipher accepts an extra input, called the tweak, that modifies the behavior of the permutation. Liskov et al. go on to introduce two tweakable block-ciphers and three constructions that utilize them as primitives. In this paper we will prove the insecurity of their Tweak Chain Hash mode of operation when the underlying tweakable block-cipher is either of the two they describe.

Update Feb 1, 2006: These attacks were known by Black, Cochran, and Shrimpton before I came up with them in December 2003. They subsequently published a paper in Eurocrypt 2005. One should reference their paper when citing these attacks. Check my web site http://www.cse.ucsd.edu/∼tristenp/ for more details.

1 Introduction

Tweakable block-ciphers are a new concept introduced by Liskov et al. These constructions provide variability: the observed behavior of the permutation is modified for each input tweak. This variability captures in a lower level primitive what most encryption and authentication schemes go at great lengths to introduce in higher-level modes of operation. Take, for example, the well known CBC$ encryption scheme, which utilizes previous blocks' output to provide variability in the output of each subsequent block.

Liskov et al. purport, and rightly so, that tweakable block-ciphers when used as a primitive in constructing schemes will allow for much easier proofs of security. They give two examples of tweakable block ciphers, an encryption scheme Tweak Block Chaining, a hash function construction Tweak Hash Chaining, and a tweakable block-cipher implementation of the OCB (Offset Codebook) mode of operation proposed by Rogaway et al. in [2].[1] They proved the security of their two tweakable block-ciphers and their modified OCB mode, but left the security of Tweak Block Chaining and Tweak Hash Chaining as open questions.

Our contribution includes an exploration of the (in)security of Tweak Hash Chaining. In the next section we briefly review Tweak Hash Chaining and definitions pertinent to our formalisms. In section 3 we prove Tweak Hash Chaining insecure when the first construction is used, in section 4 we prove it insecure using the second construction. We conclude in 5.

2 Definitions

Tweakable block-ciphers. A tweakable block-cipher is a function $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ such that each $\widetilde{E}_K(T, \cdot)$ is a permutation.

[1] A different implementation of OCB based on tweakable block-ciphers is given by Rogaway in [3].

Tweak Chain Hash (TCH). In TCH, a message M is split into n-bit blocks, where n is the block size of the underlying tweakable block-cipher. If necessary, M can be padded with a 1 followed by enough 0's to make the length of the input a multiple of n. The tweak for the first block is a public constant T_0, and the tweak of each subsequent block is the output of the previous block exclusive or'd with the input of the previous block. Thus for a message $M_1||M_2$, where $|M_1| = |M_2| = n$, $TCH(M_1||M_2) = \widetilde{E}_K(\widetilde{E}_K(T_0, M_1) \oplus M_1, M_2) \oplus M_2$. For a diagram of TCH, see [1].

Collision resistance. Let H be a hash function. Then the advantage an adversary A has in the collision-resistant sense against H is

$$\mathbf{Adv}^{\text{cr2-kk}}_{H}(A) = \Pr[K \xleftarrow{\$} \mathcal{K}; (M_1, M_2) \leftarrow A(K) : M_1 \neq M_2 \wedge H(M_1) = H(M_2)].$$

3 Insecurity of TCH with First Tweakable Block-Cipher

The first tweakable block-cipher described by Liskov et al. is $\widetilde{E}_K(T, M) = E_K(T \oplus E_K(M))$. We will now show that there is an adversary with advantage 1 that will break TCH when the underlying tweakable block-cipher is $\widetilde{E}$.

Proposition. Let $\widetilde{E}_K(T, M) = E_K(T \oplus E_K(M))$ and $TCH_{\widetilde{E}}$ be the tweak chain hash function that utilizes $\widetilde{E}$ as the underlying tweakable block-cipher. Then, there exists an adversary A such that

$$\mathbf{Adv}^{\text{cr2-kk}}_{\text{TCH}[\widetilde{E}]}(A) = 1$$

and A's running time is at most $O(t + \sigma)$, where t is the running time of $\widetilde{E}$ and σ is the length of four message blocks.

Proof. Let the adversary A be defined as follows.

Adversary $A(K)$
$M_1 = T_0$
$M_2 = T_0 \,||\, E_K(T_0) \oplus T_0 \,||\, T_0$
return (M_1, M_2)

Recall that T_0 is a publically known n-bit string. Then, we must show that $TCH_{\widetilde{E}}(M_1) = TCH_{\widetilde{E}}(M_2)$. We have that

$$\begin{aligned} TCH_{\widetilde{E}}(M_1) &= TCH_{\widetilde{E}}(T_0) \\ &= T_0 \oplus \widetilde{E}_K(T_0, T_0) \end{aligned}$$

and that

$$\begin{aligned} TCH_{\widetilde{E}}(M_2) &= TCH_{\widetilde{E}}(T_0 \,||\, E_K(T_0) \oplus T_0 \,||\, T_0) \\ &= \widetilde{E}_K(\widetilde{E}_K(TCH_{\widetilde{E}}(T_0), E_K(T_0) \oplus T_0) \oplus E_K(T_0) \oplus T_0, T_0) \oplus T_0 \\ &= \widetilde{E}_K(E_K(T_0 \oplus \widetilde{E}_K(T_0, T_0) \oplus E_K(E_K(T_0) \oplus T_0)) \oplus E_K(T_0) \oplus T_0, T_0) \oplus T_0 \\ &= \widetilde{E}_K(E_K(T_0) \oplus E_K(T_0) \oplus T_0, T_0) \oplus T_0 \\ &= \widetilde{E}_K(T_0, T_0) \oplus T_0. \end{aligned}$$

Therefore, $TCH_{\widetilde{E}}(M_1) = TCH_{\widetilde{E}}(M_2)$ and thus $\mathbf{Adv}^{\text{cr2-kk}}_{\text{TCH}[\widetilde{E}]}(A) = 1$. The resources used by A consist only of the time to compute one tweakable block-cipher, t, plus some string handling overhead. Thus, A's running time is $O(t + \sigma)$.□

4 Insecurity of TCH with Second Tweakable Block-Cipher

The second tweakable block-cipher given in [1] is $\widetilde{E}_{K,h}(T, M) = E_K(M \oplus h(T)) \oplus h(T)$. In this case $h \in \mathcal{H}$, where $\mathcal{H}$ is a family of ϵ-AXU$_2$ functions. For our purposes we do not care about the specifics of $\mathcal{H}$, refer to [1] for details about it. We will now prove that there is an adversary that shows that TCH is insecure in the cr2-kk sense when the underlying tweakable block cipher is $\widetilde{E}$.

Proposition. Let $\widetilde{E}_{K,h}(T, M) = E_K(M \oplus h(T)) \oplus h(T)$ and let $TCH_{\widetilde{E}}$ be the tweak hash chain function when $\widetilde{E}$ is used as the underlying block-cipher. Then there exists an adversary A such that

$$\mathbf{Adv}^{\text{cr2-kk}}_{\text{TCH}[\widetilde{E}]}(A) = 1$$

and A's running time is at most $O(t + \sigma)$, where t is the running time of $\widetilde{E}$ and σ is the length of three message blocks.

Proof. Adversary A behaves as follows.

Adversary A(K,h)
$M_1 = h(T_0)$
$M_2 = h(T_0) \,||\, h(E_K(0))$
return (M_1, M_2)

Now we must show that $TCH_{\widetilde{E}}(M_1) = TCH_{\widetilde{E}}(M_2)$. We have that

$$\begin{aligned} TCH_{\widetilde{E}}(M_1) &= TCH_{\widetilde{E}}(h(T_0)) \\ &= \widetilde{E}_{K,h}(T_0, h(T_0)) \oplus h(T_0) \\ &= E_K(h(T_0) \oplus h(T_0)) \oplus h(T_0) \oplus h(T_0) \\ &= E_K(0) \end{aligned}$$

and that

$$\begin{aligned} TCH_{\widetilde{E}}(M_2) &= TCH_{\widetilde{E}}(h(T_0) \,||\, h(E_K(0))) \\ &= \widetilde{E}_{K,h}(\widetilde{E}_{K,h}(T_0, h(T_0)) \oplus h(T_0), h(E_K(0))) \oplus h(E_K(0)) \\ &= \widetilde{E}_{K,h}(E_K(0), h(E_K(0))) \oplus h(E_K(0)) \\ &= E_K(h(E_K(0)) \oplus h(E_K(0))) \oplus h(E_K(0)) \oplus h(E_K(0)) \\ &= E_K(0) \oplus h(E_K(0)) \oplus h(E_K(0)) \\ &= E_K(0). \end{aligned}$$

Therefore, we have that $TCH_{\widetilde{E}}(M_1) = TCH_{\widetilde{E}}(M_2)$ and $\mathbf{Adv}^{\text{cr2-kk}}_{\text{TCH}[\widetilde{E}]}(A) = 1$. The resources that A uses are at most $O(t + \sigma)$. □

5 Conclusion

In this paper we have shown simple (albeit somewhat contrived) adversaries that can break TCH when the underlying tweakable block-cipher is either of the constructions given in [1]. This is true even though the security of those constructions has been proven. We have thus shown that the security of TCH is not ensured by the security of the underlying tweakable block-cipher. This is a serious weakness of TCH, and might imply that it has little value as a secure hash function.

References

[1] M. Liskov, R. Rivest, and D. Wagner. Tweakable Block Ciphers. *Advances in Cryptology - CRYPTO '02*. Lecture Notes in Computer Science, vol. 2442, pp. 31-46, 2002.

[2] P. Rogaway, M. Bellare, J. Black, and T. Krovetz. A block-cipher mode of operation for efficient authenticated encryption. *Eighth ACM Conference on Computer and Communications Security (CCS-8)*, pp. 196-205. ACM Press, Aug 16, 2001.

[3] P. Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. Manuscript, August, 2003. See http://www.cs.ucdavis.edu/~rogaway/papers/offsets.html.