Theoretical bounds for human mediated data authentication protocols

T-79.7001 Postgraduate Course in Theoretical Computer Science, Fall 2006

3.11.2006 Vesa Vaskelainen

Background

- M. Naor, G. Segev and A. Smith, *Tight Bounds for Unconditional Protocols in the Manual Channel and Shared Key Models*, presented at CRYPTO '06.
- A. Mashatan and D. Stinson, *Noninteractive Two-channel Message Authentication Based on Hybrid-collision resistant Hash Functions*, Cryptology ePrint Archive, Report 2006/302.
- S. Laur and K. Nyberg, *Efficient Mutual Data Authentication Using Manually Authenticated Strings*, volume 4301 of Lecture Notes in Computer Science, Springer, 2006. To appear.

Overview

- Message authentication
- Manual channel communication model
- Cryptographic primitives
- Examples of protocols
- Theoretical results

Message authentication

- Message authentication is a security service for a message receiver to verify whether a message is from a specified legitimate source, even in the presence of an adversary who controls the communication channel.
- The first construction of an authentication protocol was suggested by Gilbert, MacWilliams and Sloane in 1974.
- In 1984, Rivest and Shamir were the first to incorporate human abilities into an authentication protocol.
- Manual channel model got the formal treatment in the literature by Vaudenay in 2005.

Manual channel communication model

- Example: A user who wishes to connect a new DVD player to her home wireless network reads a short message from the display of the DVD player and types it on a PC's keyboard. This constitutes a manual authentication from the DVD player to the PC.
- In this model the sender and the receiver are connected by a bidirectional insecure channel, and by a unidirectional low-bandwidth auxiliary channel, but do not share any secret information.
- It is assumed that the adversary has full control over the insecure channel. In particular, the adversary can read any message sent over this channel, prevent it from being delivered, and insert a new message at any point in time.

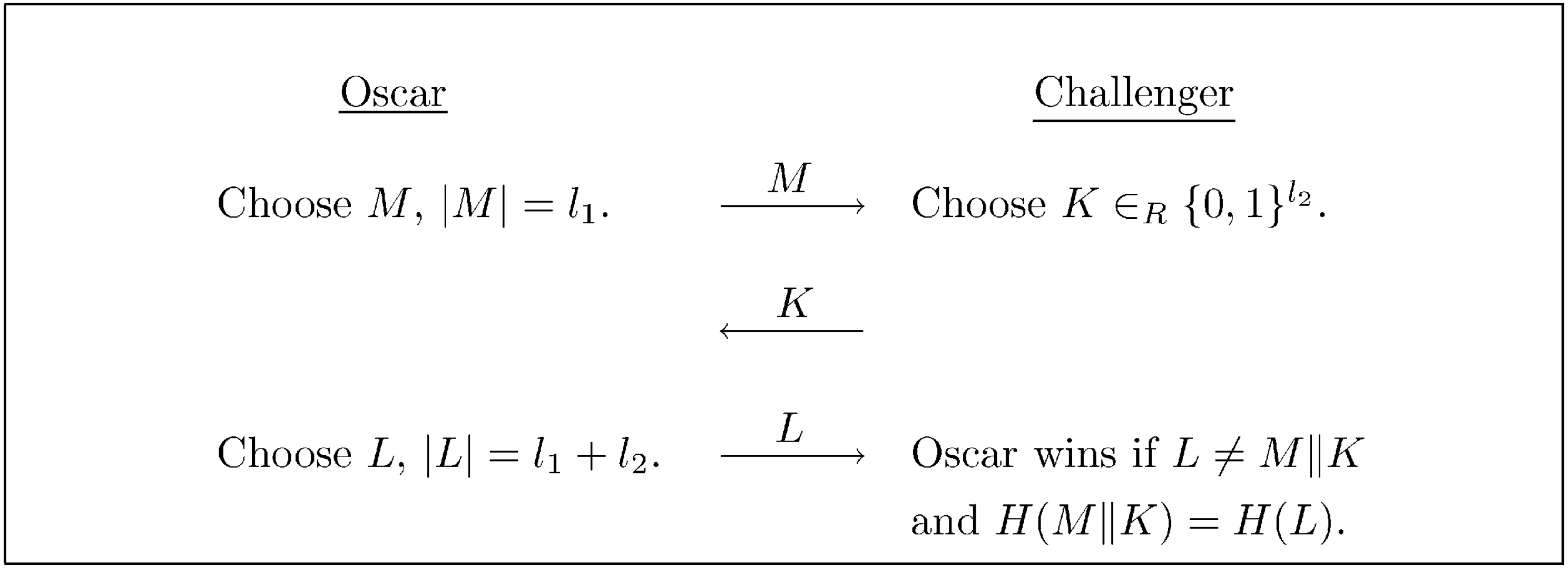
- The low-bandwidth auxiliary channel enables the sender to “manually” authenticate one short string to the receiver. For example, the sender can type a short string and send it to receiver through the auxiliary channel.
- The adversary cannot modify the short string, but can still read it, delay it, and remove it.
- Protocols in this model should provide authenticity of long messages while minimizing the length of the manually authenticated string. Short messages can be manually authenticated without the use of any authentication protocol.

Constants do matter

- The most significant constrait is the length of the manually authenticated string.
- While it is reasonable to expect user to manually authenticate 20 or 40 bits, it is not reasonable to expect a user to manually authenticate 160 bits.
- Consider an active adversary Charlie who can launch a man-in-the-middle attack. Namely, Charlie can replace a desired secure channel from Alice to Bob by a pair of secure channels, one from Alice to Charlie and one from Charlie to Bob. The attack is transparent to legitimate users without prior authenticated information.
- This motivates the study of determining the exact bounds on the required length of the manually authenticated string.

Cryptographic primitives

- **Keyed hash functions**: A keyed hash function $h : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{T}$ has two arguments: the first argument corresponds to a data and the second to a key.
- **Hybrid-collision resistant hash functions**: A hybrid-collision hash function H, is a hash function for which the following game is hard with fixed values l_1 and l_2.



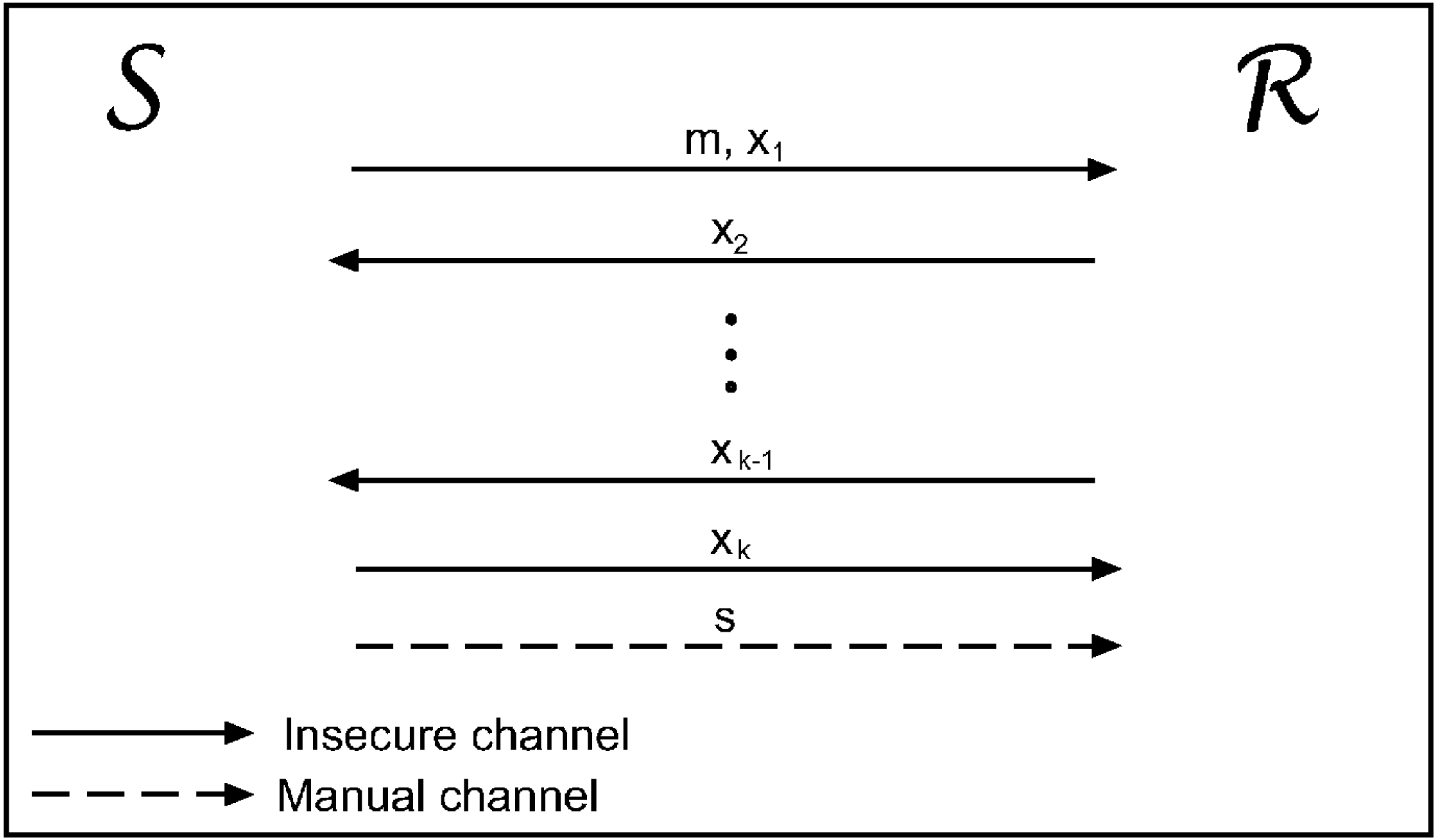
Oscar — Challenger

Choose M, $|M| = l_1$. $\xrightarrow{M}$ Choose $K \in_R \{0,1\}^{l_2}$.

$\xleftarrow{K}$

Choose L, $|L| = l_1 + l_2$. $\xrightarrow{L}$ Oscar wins if $L \neq M \| K$ and $H(M \| K) = H(L)$.

Generic protocol



A protocol P_k

$$\begin{tikzcd}
\mathcal{S} & \mathcal{R} \\
m^1_{\mathcal{S}} = m \arrow[r, "m^1_{\mathcal{S}}"] & m^1_{\mathcal{R}} = \widehat{m}^1_{\mathcal{S}} \\
i^1_{\mathcal{S}} \in_{\mathrm{R}} \mathrm{GF}[Q_1] \arrow[r, "i^1_{\mathcal{S}}"] & \widehat{i}^1_{\mathcal{S}} \\
\widehat{i}^1_{\mathcal{R}} & i^1_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_1] \arrow[l, "i^1_{\mathcal{R}}"'] \\
m^2_{\mathcal{S}} = \langle \widehat{i}^1_{\mathcal{R}}, C^1_{\widehat{i}^1_{\mathcal{R}}}(m^1_{\mathcal{S}}) + i^1_{\mathcal{S}} \rangle & m^2_{\mathcal{R}} = \langle i^1_{\mathcal{R}}, C^1_{i^1_{\mathcal{R}}}(m^1_{\mathcal{R}}) + \widehat{i}^1_{\mathcal{S}} \rangle
\end{tikzcd}$$

$$\widehat{i^2}_{\mathcal{R}} \xleftarrow{\qquad i^2_{\mathcal{R}} \qquad} i^2_{\mathcal{R}} \in_{\mathrm{R}} \mathrm{GF}[Q_2]$$

$$i^2_{\mathcal{S}} \in_{\mathrm{R}} \mathrm{GF}[Q_2] \xrightarrow{\qquad i^2_{\mathcal{S}} \qquad} \widehat{i^2}_{\mathcal{S}}$$

$$m^3_{\mathcal{S}} = \langle i^2_{\mathcal{S}}, C^2_{i^2_{\mathcal{S}}}(m^2_{\mathcal{S}}) + \widehat{i^2}_{\mathcal{R}} \rangle \qquad m^3_{\mathcal{R}} = \langle \widehat{i^2}_{\mathcal{S}}, C^2_{\widehat{i^2}_{\mathcal{S}}}(m^2_{\mathcal{R}}) + i^2_{\mathcal{R}} \rangle$$

$$\vdots$$

manually auth. $m^k_{\mathcal{S}} \xRightarrow{\qquad m^k_{\mathcal{S}} \qquad}$ accept if $m^k_{\mathcal{S}} = m^k_{\mathcal{R}}$.

Theoretical results for P_k

Theorem 1. *For any integer $k \geq 3$, and any integer n and $0 < \epsilon < 1$, there exists an unconditionally secure perfectly complete $(n, l = 2\log(1/\epsilon) + 2\log^{(k-1)} n + O(1), k, \epsilon)$ -authentication protocol in the manual channel model.*

Corollary. *For any integer n and $0 < \epsilon < 1$, the following unconditionally secure perfectly complete protocols exists in the manual channel model:*

1. A $log^* n$-round protocol in which at most $2\log(1/\epsilon) + O(1)$ bits are munually authenticated.

2. A 3-round protocol in which at most $2\log(1/\epsilon) + \log\log n + O(1)$ bits are manually authenticated.

Lower bound for P_k

Theorem 2. *For any unconditionally secure (n, l, k, ϵ)-authentication protocol in the manual channel model, it holds that if $n \geq 2\log(1/\epsilon) + 4$, then $l > 2\log(1/\epsilon) - 6$.*

Proof. Show first for $k = 3$ and use the same technique for general case.

NIMAP

- Naor, Segev and Smith investigated two-channel authentication in the interactive setting.
- NIMAP is an abbreviation for “noninteractive message authentication protocol”
- Mashatan and Stinson have constructed a NIMAP based on HCR hash functions

General Model

- an insecure broad-band channel, donoted by $\longrightarrow$, and an authenticated narrow-band channel, denoted by $\Rightarrow$.
- Adversary cannot modify the information transmitted over the authenticated channel and the channel is equipped with authenticating features such that the recipient of the information can be sure about who sent it. However, the adversary can replay a previous flow or remove it.

GNIMAP

Alice		Bob
Input (M, Bob)		
Compute $split(M) = (m_1, m_2)$	$\xrightarrow{m_2}$	Receive m_2'
	$\overset{m_1}{\Longrightarrow}$	Receive m_1' and compute $reconstruct(m_1', m_2') = M'$ Output (Alice, M') if $M' \in \mathcal{M}$, and reject otherwise.

The *split* and *reconstruct* functions satisfy:

(i) Correctness property: Any message $M \in \mathcal{M}$ can be uniquely recovered.

(ii) Binding property: It is computationally infeasible to find a message M s.t. given $(m_1, m_2) = split(M)$, one can efficiently find an another m_2' so that with non-negligible probability $reconstruct(m_1, m_2') \in \mathcal{M}$.

NIMAP based on HCR

<u>Alice</u>		<u>Bob</u>
Input (M, Bob), $\lvert M\rvert = l_1$,		
Choose $K \in_R \{0,1\}^{l_2}$.	$\xrightarrow{M,K}$	Receive M', K'.
Compute $h = H(M\|K)$.	$\overset{h}{\Longrightarrow}$	Receive h', accept if $h' = H(M'\|K')$, reject otherwise.

Corollary *Let H be a (T,ϵ)-HCRHF$^{(*}$. Any adversary against the above NIMAP, with online complexity q and offline complexity T, has a probability of success p at most $q\epsilon$.*

*) a pair (*split*, *reconstruct*) is (T,ϵ)-binding, if any adversary bounded by complexity T manages to find M and m_2' with probability at most ϵ.

Summary

- We saw examples of two-channel authentication in the interactive and non-interactive settings.
- Security was based on keyed hash functions or hybrid collision resitant hash functions.
- Generally theoretical results of manual channel protocols are difficult to compare since often each setting includes some specific parameters that are part of the theorems too.
- Practical relevance?