AUTHENTICATION THEORY/CODING THEORY*

Gustavus J. Simmons

Sandia National Laboratories
Albuquerque, New Mexico 87185

ABSTRACT

We consider a communications scenario in which a transmitter attempts to inform a remote receiver of the state of a source by sending messages through an imperfect communications channel. There are two fundamentally different ways in which the receiver can end up being misinformed. The channel may be noisy so that symbols in the transmitted message can be received in error, or the channel may be under the control of an opponent who can either deliberately modify legitimate messages or else introduce fraudulent ones to deceive the receiver, i.e., what Wyner has called an "active wiretapper" [1]. The device by which the receiver improves his chances of detecting error (deception) is the same in either case: the deliberate introduction of redundant information into the transmitted message. The way in which this redundant information is introduced and used, though, is diametrically opposite in the two cases.

For a statistically described noisy channel, coding theory is concerned with schemes (codes) that introduce redundancy in such a way that the most likely alterations to the encoded messages are in some sense close to the code they derive from. The receiver can then use a maximum likelihood detector to decide which (acceptable) message he should infer as having been transmitted from the (possibly altered) code that was received. In other words, the object in coding theory is to cluster the most likely alterations of an acceptable code as closely as possible (in an appropriate metric) to the code itself, and disjoint from the corresponding clusters about other acceptable codes.

* This work performed at Sandia National Laboratories supported by the U. S. Department of Energy under Contract No. DE-AC04-76DP00789.

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 411-431, 1985.

In [1,2] the present author showed that the problem of detecting either the deliberate modification of legitimate messages or the introduction of fraudulent messages; i.e., of transmitter and digital message authentication, could be modeled in complete generality by replacing the classical noisy communications channel of coding theory with a game-theoretic noiseless channel in which an intelligent opponent, who knows the system and can observe the channel, plays so as to optimize his chances of deceiving the receiver. To provide some degree of immunity to deception (of the receiver), the transmitter also introduces redundancy in this case, but does so in such a way that, for any message the transmitter may send, the altered messages that the opponent would introduce using his optimal strategy are spread randomly, i.e., as uniformly as possible (again with respect to an appropriate metric) over the set of possible messages, $\mathbb{M}$. Authentication theory is concerned with devising and analyzing schemes (codes) to achieve this "spreading." It is in this sense that coding theory and authentication theory are dual theories: one is concerned with clustering the most likely alterations as closely about the original code as possible and the other with spreading the optimal (to the opponent) alterations as uniformly as possibly over $\mathbb{M}$.

The probability that the receiver will be deceived by the opponent, P_d, can be bounded below by any of several expressions involving the entropy of the source H(S), of the channel H(M), of the encoding rules used by the transmitter to assign messages to states of the source H(E), etc. For example:

$$\log P_d \geq H(MES) - H(E) - H(M) \tag{1}$$

The authentication system is said to be perfect if equality holds in (1), since in this case all of the information capacity of a transmitted message is used to either inform the receiver as to the state of the source or else to confound the opponent. In a sense, inequality (1) defines an authentication channel bound similar to the communication channel bounds of coding theory. Constructions for perfect authentication systems are consequently of great interest since they fully realize the capacity of the authentication channel. In the paper given at Crypto 84 we analyzed several infinite families of perfect systems and also extended the channel bounds to include cases in which the opponent knew the state of the source. Here we have the more modest goal of rigorously deriving the channel bound (1) and then using this result to derive a family of related bounds.

FUNDAMENTALS

In authentication, there are three participants: a transmitter who observes an information source $\mathbb{S}$ and wishes to communicate these observations to a remotely located receiver over a publicly exposed, noiseless, communications channel and a

receiver who wishes to not only learn what the transmitter has observed but also to assure himself that the communications (messages) that he receives actually came from the transmitter and that no alterations have been made in transit to the messages sent by the transmitter. The third participant, the opponent, wishes to deceive the receiver into accepting a message that will misinform him as to the state of the source. He can achieve this end in either of two ways: by impersonating the transmitter and sending a fraudulent message to the receiver when in fact none has been sent by the transmitter, or else by waiting and intercepting a message sent by the transmitter and substituting some other message. There are two possibilities to be considered; the opponent may either know or not know the state of the source; he does however know the message sent by the transmitter. Using this information, in either case, he can choose some other message to forward to the receiver. The opponent "wins" if the receiver accepts the fraudulent message in any of these situations as being a genuine (authentic) communication from the transmitter, and thereby ends up being misinformed about the state of the source. We have defined the authentication problem in its narrowest sense here; however, the model can be easily extended to include cases in which the source can he influenced (controlled) by either the transmitter or the opponent or in which the opponent's objectives are more restricted -- i.e., he may wish to deceive the receiver into believing the source is in some particular state(s) not merely an arbitrary deception of the receiver. It is beyond the scope of this paper to treat these other authentication concerns, however, it is essential that the reader appreciate the precise constraints on the model of authentication used here. One of the simplifying assumptions made is that the transmitter and receiver act with common purpose, i.e., that they trust each other completely and that neither acts (either alone or in collaboration with an opponent) to deceive the other. In general, especially in commercial applications, this is an unrealistic assumption, since in practice the transmitter may wish to disavow messages (authentic) that he originated, or the receiver may wish to falsely attribute messages to the transmitter -- or even disclaim having received an authentic message actually sent by the transmitter (and received by him). These questions get into areas of digital signatures, notarization, dating, certification (in the sense of certified mail), etc., which, while closely related to authentication, are primarily questions of systems protocol in which message authentication plays an essential part. We also assume (here) that only the receiver need be convinced of the authenticity of a message -- as opposed to either the transmitter or receiver having to convince a third party (arbiter). In addition, as already mentioned we assume that all successful deceptions of the receiver are of equal value to the opponent, i.e., that his objective is purely to misinform the receiver about the state of the source -- not to cause him to conclude that it is in any particular state. Even though the most interesting applications of digital message authentication made thus far [3,4] have been in situations in which the opponent knew the state of the source (message authentication without

secrecy) we shall mostly be concerned with message authentication in situations in which the opponent is ignorant of the information being communicated to the receiver by the transmitter. Subject to these constraints, we now describe the general authentication system model.

There is a source (set) $\mathcal{S}$ with a probability distribution S on its elements for which the binary entropy is H(S). H(S) is the average amount of information about the source communicated to the receiver by the transmitter in each message. There is also a message space $\mathcal{M}$ consisting of all of the possible messages that the transmitter can send to the receiver. Since an unstated assumption is that the transmitter can communicate to the receiver any observation he makes of the source, $|\mathcal{M}| \geq |\mathcal{S}|$ where $|\mathcal{S}|$ is interpreted to be the cardinality of states of $\mathcal{S}$ that have nonzero probability of occurrence. It should be obvious that authentication depends on the set of messages that the receiver may receive being partitioned into two nonempty parts: a collection of messages that the receiver will accept as authentic and another collection that he will reject as inauthentic. If $|\mathcal{M}| = |\mathcal{S}|$, all messages would have to be acceptable to the receiver, hence no authentication would be possible in this case. Therefore, $|\mathcal{M}| > |\mathcal{S}|$ and as we shall see later the even stronger inequality H(M) > H(S) holds as well. Figure 1 schematically shows the essential features of what has been described thus far

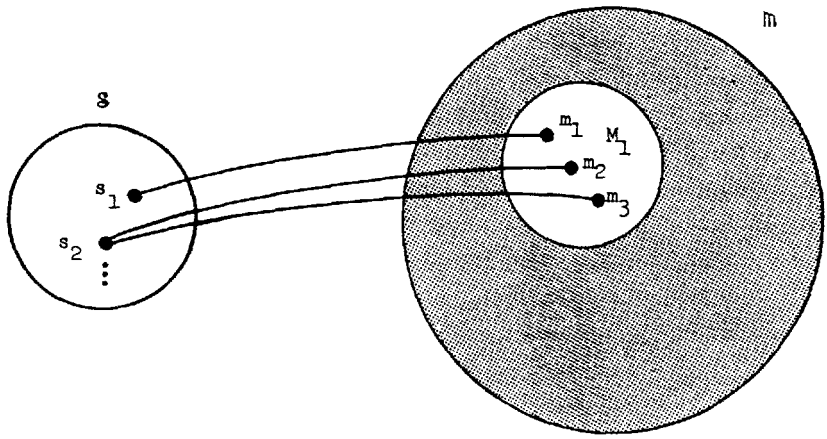

Figure 1.

Any message in the shaded region of $\mathcal{M}$ would be rejected by the receiver, while any message in the set M_1 would be accepted as authentic. Figure 1 also illustrates that it is possible for the opponent to fail to deceive the receiver, even though he succeeds in getting him to accept a message that was not sent by the transmitter. Assume that the state of the source is s_2 and that the transmitter chooses to encode this information by sending message m_2 to the receiver. If the opponent -- not

knowing the information shown in Figure 1 of course -- intercepts the message m_2 and replaces it with m_3, the receiver would accept m_3 as being authentic since it is one of the messages that the transmitter might have sent, even though it was not the message actually sent in this case. However the receiver would interpret m_3 to mean that the source state was s_2 -- as observed by the transmitter. The opponent would lose in this case, in spite of the fact that he succeeded in having the receiver accept a fraudulent message, since the receiver is not misinformed as to the state of the source.

There is a well known precept in cryptography, known as Kerckhoff's principle, that the opponent knows the system, i.e, the information contained in Figure 1. It is equally reasonable to assume the same for authentication. Consequently there would be no authentication possible for the receiver using the scheme shown in Figure 1 alone. What is done instead is to have many such encoding rules in an authentication system -- all of which are known to the opponent -- with the choice of the particular encoding rule in use being known only to the transmitter and receiver, similar in many respects to the "key" known only to the transmitter and receiver in a cryptosystem. Figure 2 suggests the general scheme:

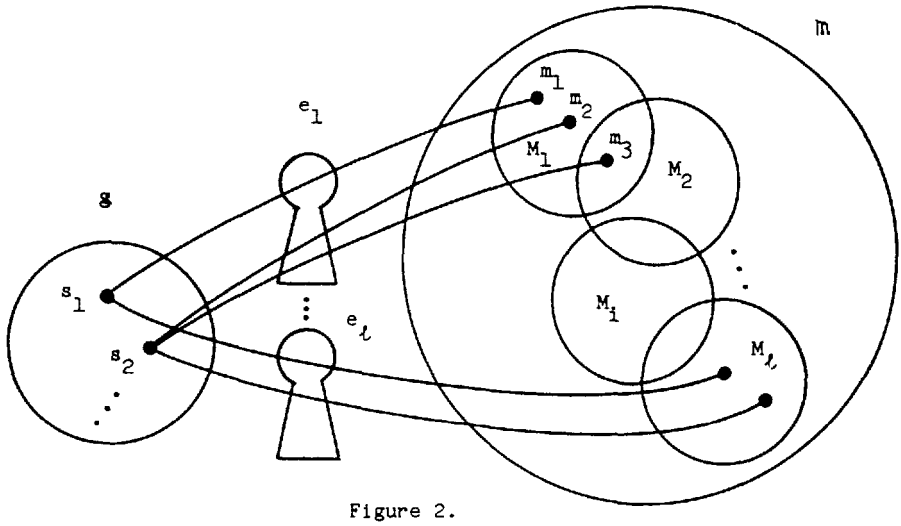

Figure 2.

Each encoding rule, e_i, determines a proper subset M_i of $\mathbb{M}$, $|M_i| \geq |\mathcal{S}|$, and a mapping -- perhaps one to many -- of $\mathcal{S}$ onto M_i. The inverse mapping D is a well defined function, i.e., for any $e \in \mathcal{E}$ and $m \in M_i$, the function $D(e,m)$ defines a unique state in $\mathcal{S} \cup \phi$, where ϕ is the null set.

Even this very intuitive description of authentication should make clear the reason for describing authentication as a problem in "spreading" messages in $\mathbb{M}$. If m_1 is an acceptable message only in set M_1, then the opponent, knowing the system, would be able to conclude that e_1 was the coding rule being used if he saw m_1 in the

channel and would then be able to substitute another message with certainty of deceiving the receiver. To avoid this it is necessary that each message occur in sufficiently many authenticating sets to (ideally) leave the opponent no more able to "guess" at an acceptable message after he has observed what the transmitter sent than he could have before the observation. This ideal can be achieved in infinitely many perfect authentication systems [5,6].

THE "GAME" MODEL OF AUTHENTICATION

A concise representation of the authentication system depicted in Figure 2 is possible in the form of an $|\mathcal{E}| \times |\mathbb{M}|$ matrix, **A**, where $\mathcal{E}$ is the set of encoding rules. The rows of **A** are indexed by encoding rules and the columns by messages. The entry in $a(e_i, m_j)$ is the element of $\mathcal{S}$ encoded by rule e_i into message m_j if such a source mapping exists under e_i and 0 otherwise. Every element of $\mathcal{S}$ appears in each row of **A** at least once and perhaps several times. We define an authentication system to be the triple $(\mathcal{S}, S, \mathbf{A})$. Earlier comments imply that each row and column contains at least one 0 entry. We now define another $|\mathcal{E}| \times |\mathbb{M}|$ matrix **X**, in which

$$\chi(e_i, m_j) = \begin{cases} 1 & \text{if} \quad a(e_i, m_j) \in \mathcal{S} \\ 0 & \text{otherwise} \end{cases} .$$

For example, for $|\mathcal{S}| = 2$, $|\mathbb{M}| = 4$, the "best" authentication system possible has:

$$\mathbf{A} = \begin{vmatrix} s_1 & s_2 & 0 & 0 \\ s_1 & 0 & s_2 & 0 \\ 0 & s_2 & 0 & s_1 \\ 0 & 0 & s_2 & s_1 \end{vmatrix} \quad \text{and} \quad \mathbf{X} = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{vmatrix} .$$

It is now easy to see the relationship of the impersonation "game" to the matrix **X**. If m_j is an acceptable (authentic) message to the receiver when encoding rule e_i has been agreed to by the transmitter and receiver then $\chi(e_i m_j) = 1$ and the opponent has a probability of success of $p = 1$ if he communicates m_j to the receiver. Conversely, whenever $\chi(e_i, m_j) = 0$ he is certain the message will be rejected. It is certainly plausible -- and in fact rigorously true -- that the opponents probability of success in impersonating the transmitter is the value, v_I, of the zero sum game whose payoff matrix is **X**. It is possible to define a companion payoff matrix **Y** for the substitution game, although it is considerably more complex. The value of this game, v_S, is the probability that the opponent will be successful in deceiving the receiver through intercepting a message sent by the transmitter and substituting one of his own devising. Given an authentication system the transmitter/receiver have

the freedom to choose among the encoding rules and if some state(s) of the source can be encoded into more than one message under some of the encoding rules, a choice of which messages to use, i.e., a splitting strategy. The opponent on the other hand can choose between impersonation and substitution with whatever probability distribution he wishes and then choose according to his optimal strategy which fraudulent message he will communicate to the receiver, either with no conditioning if he is impersonating the transmitter or else conditioned on the message he observed if he is substituting messages. Not surprisingly there exist authentication systems in which the optimal strategy for the opponent is either pure impersonation, pure substitution, immaterial mixes of the two, or most interesting -- essential mixing of both as well as examples in which splitting is essential in the transmitter/receiver's optimal strategies. The point of these remarks is that we have shown in earlier papers that an opponent's overall probability of success in deceiving the receiver, P_d, is simply the value of the game whose payoff matrix is the concatenation of **X** and **Y**, and hence that

$$P_d = v_G \geq \max(v_I, v_S) \tag{2}$$

It is not germane to this paper to develop the payoff matrix **Y**, since (2) is the only result pertaining to the substitution game that we shall need later.

With these preliminaries out of the way we survey the essential notation used in the authentication model.

Name	Set	Element	Variable
Source	$\mathcal{S}$	s_i	S
Message Space	$\mathcal{M}$	m_j	M
Encoding Rules	$\mathcal{E}$	e_k	E
Splitting Strategies		$\pi(m_j \mid s_i e_k)$	Π
Impersonation Strategy	Q	q_j	Q

$P(X = x)$ probability that the random variable X takes the value x, as for example $P(M = m)$, $P(S = s)$ or $P(E = e)$.

Name	Entropy
Source Distribution	H(S)
Message Distribution	H(M)
Coding Strategy	H(E)
Joint (message coding strategy source) Distribution	H(MES)

A	encoding matrix
X	impersonation payoff matrix
Y	substitution payoff matrix
XY	concatenated authentication payoff matrix
v_I	value of impersonation game on X (to opponent)
v_s	value of substitution game or Y (to opponent)
$P_d = v_G$	probability that opponent deceives the receiver: value of game on XY.

$|e_i| = \sum_{m \in \mathcal{M}} \chi(e_i, m)$ number of nonzero entries in the e_i row of either A or X.

$|m_j| = \sum_{e \in \mathcal{E}} \chi(e, m_j)$ number of nonzero entries in the m_j column of either A or X.

THE AUTHENTICATION CHANNEL BOUND

Our object in this paper is to derive channel bounds for the authentication channel. Several such bounds are easy.

Theorem 1.

$$P_d = v_G \geq \frac{\min_{\mathcal{E}} |e_i|}{|\mathcal{M}|} . \tag{3}$$

Proof:

As has already been noted, the opponent has available as part of his strategy the choice of whether to impersonate the transmitter or to substitute messages, hence the value of the concatenated game is at least as large as the value of either game alone. We actually prove that for the impersonation game:

$$v_I \geq \frac{\min_{\mathcal{E}} |e_i|}{|\mathcal{M}|} .$$

The payoff matrix for A is the $|\mathcal{E}| \times |\mathcal{M}|$ (0,1) matrix X in which $\chi(i,j) = 1$ if some state of $\mathcal{S}$ is encoded into m_j by the encoding rule e_i, and 0 otherwise. If the transmitter/receiver are playing an optimal strategy E (probability that encoding rule e_i is played is $P(E = e_i)$ and the opponent is impersonating the transmitter with an optimal strategy Q (probability that he sends m_j is q_j) then the expected value to the opponent of impersonating with message m_j is

$$r_j = \sum_{e \in \mathcal{E}} P(E = e)\chi(e, m_j)$$

and his expected payoff from playing strategy Q is simply the value of the game

$$v_I = \sum_{m \in \mathcal{M}} \left(q(m) \sum_{e \in \mathcal{E}} P(E = e)\chi(e,m)\right) \quad .$$

Since v_I is the value of the game for the opponent, realized playing an optimal strategy Q, it is at least as large as the value realized by his playing any other strategy -- in particular, the uniform probability distribution of $\mathcal{M}$. Therefore,

$$v_I = \sum_{m \in \mathcal{M}} \left(q(m) \sum_{e \in \mathcal{E}} P(E = e)\chi(e,m)\right) \geq \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} \sum_{e \in \mathcal{E}} P(E = e)\chi(e,m)\right)$$

(4)

$$= \frac{1}{|\mathcal{M}|} \sum_{e \in \mathcal{E}} P(E = e) \sum_{m \in \mathcal{M}} \chi(e,m) = \frac{1}{|\mathcal{M}|} \sum_{e \in \mathcal{E}} |e| P(E = e) \quad .$$

The inequality is only weakened by replacing $|e|$ by $\min_{\mathcal{E}} |e|$. Therefore,

$$v_G \geq v_I \geq \frac{\min_{\mathcal{E}} |e|}{|\mathcal{M}|}$$

as was to be shown. ∎

Corollary:

Since $\min_{\mathcal{E}} |e| \geq |\mathcal{S}|$

(5)
$$P_d = v_G \geq \frac{|\mathcal{S}|}{|\mathcal{M}|} \quad .$$

Theorem 2.

Given an authentication system ($\mathcal{S}$, S, A) for which

(6)
$$v_G = \frac{\min_{\mathcal{E}} |e|}{|\mathcal{M}|} \quad ;$$

in every optimal strategy, E, for the transmitter/receiver $P(E = e) = 0$ for any encoding rule for which $|e| > \min_{\mathcal{E}} |e|$.

Proof:

As in the proof of Theorem 1 we use the fact that $v_G \geq v_I$ and actually prove the conditions of the theorem for the impersonation game. From (4) we have

$$v_I = \sum_{m \in \mathcal{M}} q(m) \sum_{e \in \mathcal{E}} P(E = e)\chi(e,m) \quad .$$

Assume that there is some encoding rule, e_j, for which $|e_j| > \min_{\mathcal{E}}|e|$ and for which $P(E = e_j) > 0$. As noted before Q is an optimal strategy for the opponent and hence v_I is at least as great an expectation for him as he could achieve using any other strategy -- in particular the uniform probability distribution on $\mathcal{M}$.

$$v_I \geq v(\text{uniform}) = \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} \sum_{e \in \mathcal{E}} P(E = e)\chi(e,m)$$

$$= \sum_{e \in \mathcal{E}} P(E = e) \sum_{m \in \mathcal{M}} \frac{\chi(e,m)}{|\mathcal{M}|} = \sum_{e \in \mathcal{E}} P(E = e) \frac{|e|}{|\mathcal{M}|} > \frac{\min_{\mathcal{E}}|e|}{|\mathcal{M}|}$$

if $P(E = e) > 0$ for any $e \in \mathcal{E}$ for which $|e| > \min_{\mathcal{E}}|e|$. ∎

Corollary:

If for an authentication system $(\mathcal{S}, S, A)$

$$v_G = \frac{|\mathcal{S}|}{|\mathcal{M}|}$$

which by Theorem 1 can only happen if $\min_{\mathcal{E}}|e| = |\mathcal{S}|$, then every optimal strategy for the transmitter/receiver, E, has $P(E = e) = 0$ for any encoding rule for which $|e| > |\mathcal{S}|$.

Another way of stating the conclusion of the Corollary is that if $v_G = |\mathcal{S}|/|\mathcal{M}|$ no splitting occurs in any encoding rule occurring in an optimal strategy! It is worth remarking that

$$v_G = \frac{\min_{\mathcal{E}}|e|}{|\mathcal{M}|}$$

does not imply that splitting does not occur in any of the encoding rules that occur in $\mathcal{E}$. What is true, by Theorem 2, is that in this case all of the encoding rules that occur (with positive probability) in an optimal strategy use the same number of messages.

Several other channel capacity theorems of similar flavor can be proven, however we now turn to our primary object in this paper; establishing bounds on the authentication channel in terms of the various entropies on the primary variables. A trivial bound can be given in terms of H(E). Since H(E) is the total equivocation that the opponent has as to which encoding rule is being used by the transmitter/receiver, and since he could deceive the receiver with certainty if he only knew the rule they had chosen, we have

(7) $$\log P_d = \log v_G \geq -H(E)$$

(7) isn't a particularly useful result since as we shall see later there is a much stronger bound in terms of H(E). The bound of the following theorem is the main result on which the theory of authentication is based.

Theorem 3. (Authentication Channel Capacity)

(8) $$\log P_d \geq H(MES) - H(E) - H(M)$$

Proof:

Let $P(M = m)$ be the probability that message m will be observed in the channel when states of the source occur according to the probability distribution S and are encoded by the transmitter with an encoding rule chosen from $\mathcal{E}$ with probability distribution E, employing splitting strategies Π. $P(M = m)$ is formally

(9) $$P(M = m) = \sum_{(e,s)\in\mathcal{E}\times\mathcal{S}} P(M = m, E = e, S = s)$$

or equivalently by

(10) $$P(M = m) = \sum_{(e,s)\in\mathcal{E}\times\mathcal{S}} P(M = m, E = e, S = s)\chi(e,m)$$

$$\text{where } \chi(e,m) = \begin{cases} 1 \text{ if some state of the source can be encoded into m using encoding rule e} \\ 0 \text{ otherwise} \end{cases} .$$

The formal sum (10) has the same value as (9) since

$$P(M = m, E = e, S = s) \neq 0 \rightarrow \chi(e,m) = 1 \quad .$$

The converse need not be true, i.e., $\chi(e,m) = 1$ can hold while $P(M = m, E = e, S = s) = 0$, either because some s', other than the s in $P(M = m, E = e, S = s)$ is encoded into m by e, or else that the state occurring in $P(M = m, E = e, S = s)$ could be encoded into m and some other message(s) under m, but that the splitting rule used by the transmitter never uses m. $\chi(e,m)$ is the authentication function on $\mathcal{M}$ since the receiver will accept a message m when encoding rule e has been selected if and only if $\chi(e,m) = 1$.

The joint probability $P(M = m, E = e, S = s)$ can be represented as the product of the conditional probability that m will be sent given that state s occurred and that encoding rule e is being used $\Pi(m|e,s)$, times the independent probabilities that these events occur.

$$(11) \qquad P(M = m) = \sum_{(e,s)\in\mathcal{E}\times\mathcal{S}} P(E = e)\chi(e,m)P(S = s)\pi(m|e,s) \ .$$

We now wish to restrict the domain from the Cartesian product $\mathcal{E} \times \mathcal{S}$ to only $\mathcal{E}$ by using the inverse mapping to e; D(e,m), $\chi(e,m)$ was introduced in (2) to make this possible,

$$(12) \qquad P(M = m) = \sum_{e\in\mathcal{E}} P(E = e)\chi(e,m)P\big(S = D(e,m)\big)\pi\big(m|e,D(e,m)\big)$$

since

$$\chi(e,m)\ \pi(m|es) = 0 \quad \text{unless} \quad D(e,m) = s \ .$$

Define a probability distribution $W(m) = \{w_e(m)\}$ on $e \in \mathcal{E}$ for every $m \in \mathbb{M}$:

$$(13) \qquad w_e(m) = \frac{P(E = e)\ \chi(e,m)}{\sum_{e^*\in\mathcal{E}} P(E = e^*)\chi(e^*,m)}$$

$w_e(m)$ is well defined since every $m \in \mathbb{M}$ is acceptable to the receiver for at least one choice of an encoding rule. Also $\sum_{e\in\mathcal{E}} w_e(m)\chi(e,m) = 1$. Multiplying the summand in (12) by

$$\frac{\sum_{e^*\in\mathcal{E}} P(E = e^*)\chi(e^*,m)}{\sum_{e^*\in\mathcal{E}} P(E = e^*)\chi(e^*,m)}$$

we obtain

$$(14) \qquad P(M = m) = \sum_{e\in\mathcal{E}} w_e(m)\Big\{\Big[\sum_{e\in\mathcal{E}} P(E = e^*)\chi(e^*,m)\Big]P\big(S = D(e,m)\big)\pi\big(m|e,D(e,m)\big)\Big\} \ .$$

We now wish to form $-P(M = m) \log P(M = m)$ on both sides of (14) as a first step to calculating the entropy H(M) of the messages observed in the channel. Formally,

$$(15) \qquad -P(M = m)\log P(M = m) = -\Big[\sum_{e\in\mathcal{E}} w_e(m)\{\ldots\}\Big] \log \Big[\sum w_e(m)\{\ldots\}\Big] \ .$$

Noting that $-x \log x$ is concave downwards, we use Jensen's inequality -- which says that if g(x) is a concave function on (a,b), and if $\{x_i\}$ are arbitrary real arguments, $a < x_i < b$, then for any set of positive weights w_i where $\sum w_i = 1$;

$$g(\textstyle\sum w_i x_i) \geq \sum w_i g(x_i)$$

to replace the equality in (15) with an inequality.

Let $x = \{...\}$ in (7):

$$-P(M = m)\log P(M = m) \geq -\sum_{e\in\mathcal{E}} w_e(m)\{...\}\log\{...\} \quad . \tag{16}$$

By canceling the sum $\sum_{e\in} P(E = e)\chi(e,m)$ between the denominator of $w_e(m)$ and $\{...\}$, and by splitting the logarithm of the product in $\{...\}$ into the sum of three logarithms, we get

$$\begin{aligned} -P(M = m)\log P(M = m) \geq & -\sum_{e\in\mathcal{E}} P(E = e)\chi(e,m)P\big(S = D(e,m)\big)\pi(m)e,\ D(e,m)\big) \\ & \times \left[\log\Big(\sum_{e\in\mathcal{E}} P(E = e)\chi(e,m)\Big) + \log P\big(S = D(e,m)\big) + \log\pi\big(m|e,\ D(e,m)\big)\right] \end{aligned} \tag{17}$$

Now, we make use of the game model for the authentication channel to bound (17) below. The value of the impersonation game, v_I, is

$$v_I = \max_{m\in\mathcal{M}} \sum_{e\in\mathcal{E}} P(E^* = e)\chi(e,m) \geq \sum_{e\in\mathcal{E}} P(E = e)\chi(e,m) \tag{18}$$

where E^* is an optimal strategy for the transmitter/receiver and E is an arbitrary strategy. Inequality (18) is at worst weakened through replacing

$$\sum P(E = e)\chi(e,m)$$

in $[...]$ with the maximum value it can have for any choice of m. Summing both sides of (18) over all $m \in \mathcal{M}$, we get

$$H(M) = -\sum P(M = m)\log P(M = m)$$

on the left and the expression in (19) on the right:

$$\begin{aligned} H(M) \geq & -\sum_{m\in\mathcal{M}} \sum_{e\in\mathcal{E}} P(E = e)\chi(e,m)P\big(S = D(e,m)\big)\pi\big(m|e,D(e,m)\big) \\ & \times \left[\log v_I + \log P\big(S = D(e,m)\big) + \log \pi\big(m|e,\ D(e,m)\big)\right] \quad . \end{aligned} \tag{19}$$

Since $\log v_I$ is a constant it can be moved through the double summation to give

$$\log v_I \sum_{m\in\mathcal{M}} \sum_{e\in\mathcal{E}} P(E = e)\chi(e,m)P\big(S = D(e,m)\big)\pi\big(m|e,D(e,m)\big)$$

Using (12), the summand can be replaced by $P(M = m)$

$$\log v_I \sum_{m\in\mathfrak{M}} P(M = m) = \log v_I$$

so that (19) becomes

$$H(M) \geq -\log v_I - \sum_{m\in\mathfrak{M}} \sum_{e\in\mathcal{E}} P(E = e)\chi(e,m)P\{S = D(e,m)\}$$

(20)

$$\times \pi\{m|e,D(e,m)\}[\log P\{S = D(e,m)\} + \log\pi\{m|e,D(e,m)\}] \quad .$$

It has already been noted that

$$\chi(e,m)\pi(m|e,s) = 0$$

unless $D(e,m) = s$, therefore (20) can be rewritten in the form

$$H(M) \geq -\log v_I - \sum_{e\in\mathcal{E}} \sum_{s\in\mathcal{S}} \sum_{\substack{m\in\mathfrak{M} \\ D(e,m)=s}} P(E = e)P\{S = s)\pi(m|e,s)$$

(21)

$$\times \{\log P(S = s) + \log \pi(m|e,s)\}$$

or

$$= -\log v_I - \sum_{e\in\mathcal{E}} \sum_{s\in\mathcal{S}} P(E = e)P(S = s)\log P(S = s)$$

(22)

$$- \sum_{e\in\mathcal{E}} \sum_{s\in\mathcal{S}} P(E = e)P(S = s) \sum_{\substack{m\in\mathfrak{M} \\ D(e,m)=s}} \pi(m|e,s)\log\pi(m|e,s)$$

since

$$\sum_{\substack{m\in\mathfrak{M} \\ D(e,m)=s}} \pi(m|e,s) = 1 \quad .$$

Moving the summation over $\mathcal{S}$ through $P(E = e)$, we obtain

(23) $$H(M) \geq -\log v_I + \sum_{e\in\mathcal{E}} P(E = e)H(S) + \sum_{e\in\mathcal{E}} \sum_{s\in\mathcal{S}} P(E = e)P(S = s)H(M|ES)$$

(24) $$= -\log v_I + H(S) + H(M|ES) \quad .$$

Using the entropy identity

$$H(A|B) = H(AB) - H(B)$$

(16) becomes

$$\log v_I \geq H(S) + H(MES) - H(ES) - H(M) \quad . \tag{25}$$

But

$$H(ES) = H(E|S) + H(S) = H(E) + H(S)$$

since E and S are independent. Therefore

$$\log v_I \geq H(MES) - H(E) - H(M) \quad .$$

The conclusion of the theorem follows from the earlier result that $P_d = v_G \geq \max(v_I, v_S)$, so that

$$\log P_d = \log v_G \geq \log v_I \geq H(MES) - H(E) - H(M) \tag{26}$$

as was to be shown. ∎

The hard work is now completed. A variety of useful equivalent expressions can be derived from (26) using simple identities from information theory, for the cases of authentication either with or without secrecy. We illustrate the technique in Theorem (4) for the case of authentication with secrecy: i.e., the opponent does not know the state of the source observed by the transmitter. This, of course, only matters when the opponent elects to substitute messages rather than to impersonate the transmitter.

Theorem 4.

$H(MES) - H(E) - H(M)$ is equivalent to any of the following eight entropy expressions.

	X	Equivalent Form
(27)	ES	$H(M\|ES) + H(S) - H(M)$
(28)	MS	$H(E\|MS) - H(E) + H(MS) - H(M)$
		or
(29)		$H(E\|MS) - H(E) + H(S\|M)$
(30)	ME	$H(E\|M) - H(E)$
		or
(31)		$H(M\|E) - H(M)$
(32)	S	$H(ME\|S) + H(S) - H(E) - H(M)$
(33)	E	$H(MS\|E) - H(M)$
(34)	M	$H(ES\|M) - H(E)$

Proof:

The proof in each case proceeds by splitting the argument in the entropy H(MES) through conditioning the joint probability on X and then using simple identities to reduce the resulting expressions. The derivation of (27) is typical.

$$H(MES) = H(M|ES) + H(ES)$$

$$= H(M|ES) + H(E|S) + H(S)$$

$$= H(M|ES) + H(E) + H(S)$$

since E and S are independent random variables. Hence

$$H(MES) - H(E) = H(M) = H(M|ES) + H(S) = H(M)$$

as was to be shown, etc. ▌

Using the results of Theorem 4 it is possible to derive some (generally) weaker but enlightening channel bounds. We first note that the total effective equivocation to the opponent playing the substitution game but without knowledge of the source state, i.e., authentiction with secrecy is no greater than H(E|M) and as remarked earlier, the opponent's total effective equivocation if he knows the source state, i.e., authentication without secrecy, is at most H(E|MS).

Theorem 5.

For authentication with secrecy

$$\log v_G \geq -\frac{1}{2} H(E) \tag{35}$$

while for authentication without secrecy

$$\log v_G \geq -\frac{1}{2}\{H(E) - H(MS) + H(M)\} = -\frac{1}{2}\{H(E) - H(S|M)\} \tag{36}$$

Proof:

For authentication with secrecy

$$\log v_G \geq \min\{\log v_I, -H(E|M)\} \tag{37}$$

while for authentication without secrecy

$$\log v_G \geq \min\{\log v_I, -H(E|MS)\} \quad . \tag{38}$$

In either (37) or (38) the bounds derived in Theorems 3 and 4 on the value of the impersonation game can be substituted, since the opponent's impersonation strategy is independent of whether he plays substitution with or without secrecy. Replacing the minimum on the right-hand side of the inequality by the average of the two bracketed terms either weakens the inequality if the terms are not identical or leaves it unaffected if they are. Therefore for authentication with secrecy, replacing v_I with the bound (30) in (37) we get

$$\log v_G \geq \frac{1}{2}\{H(E|M) - H(E) - H(E|M)\} = -\frac{1}{2}H(E)$$

and similarly by replacing v_I with the bounds (28) or (29) in (38) we get

$$\log v_G \geq \frac{1}{2}\{H(E|MS) - H(E) + H(MS) - H(M) - H(E|MS)\}$$

$$= -\frac{1}{2}\{H(E) - H(MS) + H(M)\}$$

or

$$\log v_G \geq \frac{1}{2}\{H(E|MS) - H(E) + H(S|M) - H(E|MS)\}$$

$$= \frac{1}{2}\{H(E) - H(S|M)\}$$

as was to be shown. ∎

Corollary:

(39) $$P_d = v_G \geq \frac{1}{\sqrt{|\mathcal{E}|}}$$

Proof:

$$H(E) \geq \log|\mathcal{E}|$$

with equality if and only if the transmitter/receiver's optimal strategy E is the uniform probability distribution on $\mathcal{E}$. The conclusion follows by substituting (39) into (35). ∎

Bound (35) was first found by Gilbert, McWilliams and Sloan [7] under slightly more restrictive conditions and derived directly in the same generality used here by Simmons and Brickell in [6]. (35) is the bound based on H(E) promised earlier when the trivial bound in (7) was given.

FOR EXAMPLE

In this section, in order to show the effects of secrecy on both the strategies of the participants and on the game values as well as to illustrate parameters such as splitting, etc., we discuss two small examples. Earlier we described on authentication system for which $|\mathcal{E}| = |\mathcal{M}| = 4$, $|\mathcal{S}| = 2$ and for which the payoff matrix X was:

$$X = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{vmatrix} \tag{40}$$

X could also be the payoff matrix for many different authentication systems, one of which was exhibited before

$$A = \begin{vmatrix} s_1 & s_2 & 0 & 0 \\ s_1 & 0 & s_2 & 0 \\ 0 & s_2 & 0 & s_1 \\ 0 & 0 & s_2 & s_1 \end{vmatrix} . \tag{41}$$

One other such system is

$$A^* = \begin{vmatrix} s_1 & s_2 & 0 & 0 \\ s_2 & 0 & s_1 & 0 \\ 0 & s_1 & 0 & s_2 \\ 0 & 0 & s_2 & s_1 \end{vmatrix} . \tag{42}$$

In either case $v_I = 1/2$ with an optimal strategy for either player being the uniform probability strategy on rows (transmitter) and on columns (opponent). If we consider only substitution with secrecy, then it makes no difference to the opponent whether the transmitter/receiver are using the authentication system $(\mathcal{S}, S, A)$ or $(\mathcal{S}, S, A^*)$, since in either case when he sees a message he is faced with two possible encoding rules and hence with a choice between two equilikely messages to substitute -- one of which will be accepted and are rejected. His probability of success in either case is 1/2, which is precisely what his chances of success in impersonating the transmitter would have been had he not waited to observe a message. Hence for authentication with secrecy $P_d = 1/2$. The situation is different however for authentication without secrecy. In this case for the system $(\mathcal{S}, S, A)$ the same arguments given for the authentication with secrecy case hold and $P_d = v_G = v_I = v_s = 1/2$. For the system $(\mathcal{S}, S, A^*)$ however, if the opponent waits to observe a message he will know with certainty which encoding rule the transmitter/receiver

have chosen and hence can substitute another message with certainty that not only will it be accepted as authentic by the receiver but that the receiver will be misinformed as a result. Therefore in this case

$$P_d = v_G = v_s = 1 > v_I = \frac{1}{2} .$$

Incidentally the system ($\mathcal{S}$, S, A) is perfect and is also an instance in which equality holds in (39):

$$v_G = \frac{1}{2} = \frac{1}{\sqrt{|\mathcal{E}|}} .$$

We conclude by showing another example in which equality holds in (39) and in which, in addition, splitting is essential (for the transmitter/receiver) to hold the opponent to the game value $P_d = 1/\sqrt{|\mathcal{E}|}$. In order to have a concise description of ($\mathcal{S}$, S, A) we introduce a notation for A. $\mathcal{M}$ is partitioned into disjoint parts -- three in the example -- and the elements in each part indexed. The encoding rules will be of a special type (Cartesian) that encode a state of the source only into the messages in a particular part. In the example $|\mathcal{S}| = 3$, $|\mathcal{M}| = 12$ and $|\mathcal{E}| = 16$. The partition of $\mathcal{M}$ is into 4, 4 and 8 elements, indexed 1, 2, 3, 4; 1, 2, 3, 4 and 1, 2, 3, 4, 5, 6, 7, 8, respectively. The states of the source are assumed to be equiprobable.

$$A = \begin{array}{|c|c|c|} \hline s_1 & s_2 & s_3 \\ \hline 1 & 1 & 1,2 \\ 1 & 2 & 3,4 \\ 1 & 3 & 5,6 \\ 1 & 4 & 7,8 \\ 2 & 1 & 3,8 \\ 2 & 2 & 1,7 \\ 2 & 3 & 2,4 \\ 2 & 4 & 5,6 \\ 3 & 1 & 5,7 \\ 3 & 2 & 2,6 \\ 3 & 3 & 1,8 \\ 5 & 4 & 3,4 \\ 4 & 1 & 4,6 \\ 4 & 2 & 5,8 \\ 4 & 3 & 3,7 \\ 4 & 4 & 1,2 \\ \hline \end{array}$$

Encoding rule e_1 says that source state s_1 will be encoded into message 1 of part 1, state s_2 into message 1 of part 2 and state s_3 into either message 1 or message 2 of part 3, etc. The unique optimal strategy, E, for the transmitter/receiver is the uniform probability distribution $p(E = e_i) = 1/16$ with uniform splitting; i.e., if e_1 is being used and state s_3 occurs, then a fair coin would be tossed to decide

whether message 1 or 2 of part 3 was to be sent, etc. Against strategies S and Π, the value of the game is

$$P_d = v_G = \frac{1}{\sqrt{|\mathcal{E}|}} = \frac{|\mathcal{S}|}{|\mathcal{M}|} = \frac{3}{12} = \frac{1}{4}$$

and the game is perfect. Although it isn't quite obvious, it is easy to show that it doesn't matter to the opponent whether he chooses to impersonate the transmitter or to wait and observe a message and then substitute another message; in either case if he plays optimally his chance of success will be 1/4. Note that in this example while the opponent is faced with two bits of equivocation irrespective of whether he impersonates or substitutes, i.e., $v_I = v_S = 1/4$, that the equivocation about the source state is only $\log_2 3 = 1.585$ bits, or $P(S = s) = 1/3$ for any $s \in \mathcal{S}$. Thus while the opponent could guess the state of the source with a probability of success of 1/3 he could only guess at a message to communicate a state with probability 1/4. If one considers what the channel bound theorem says, this is no paradox and P_d can be made as small as desired, even for a one-bit source in which $P(S = s) = 1/2$. This example, incidentally, is one of the smallest illustrating an infinite class of perfect authentication systems [5] with essential splitting.

CONCLUSION

In this paper we have proven that the bounds on the authentication channel are precisely what one would intuitively expect (and hope for), namely that the difference between the amount of information transmitted through the channel and that needed by the receiver to resolve his equivocation about the source state can be used to authenticate the message, and conversely that no better result can be achieved. We also exhibited small examples demonstrating that it is possible to use all of this residual information to confound the opponent, i.e., that the channel bounds are sharp.

REFERENCES

1. A. D. Wyner, "The Wire-tap Channel," The Bell System Technical Journal, Vol. 54, No. 8 (Oct. 1975), pp. 1355-1387.

2. G. J. Simmons, "A Preliminary Report on a Theory of Authentication," Proceedings of the IEEE National Electronics Conf., Chicago, IL (Oct. 28-29, 1981), pp. 315-318.

3. G. J. Simmons, "Verification of Treaty Compliance -- Revisited," Proceedings of the IEEE 1983 Symposium on Security and Privacy, Oakland, CA (Apr. 25-27, 1983), pp. 61-66.

4. G. J. Simmons, "A System for Verifying User Identity and Authorization at the Point-of-Sale or Access," Cryptologia, Vol. 8, No. 1, January 1984, pp. 1-21.

5. G. J. Simmons, "Message Authentication: A Game on Hypergraphs," Proceedings of the 15th Southeastern Conference on Combinatorics, Graph Theory and Computing, Baton Rouge, LA, March 5-8, 1984, (to appear).

6. E. F. Brickell, "A Few Results in Message Authentication," Proceedings of the 15th Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, LA, March 5-8, 1984, (to appear).

7. E. N. Gilbert, Mrs. F. J. MacWilliams, and N. J. A. Sloane, "Codes which Detect Deception," The Bell System Technical Journal, Vol. 53, No. 3 (March 1974), pp. 405-414.