Optimal Control Formulation of Query Model for Authentication Systems

Ferruh Özbudak, Ali D. Sezer and Üstün Yıldırım

***Abstract*—We give a stochastic optimal control representation of the N step adaptive attack on an authentication system using an authentication oracle described in [Safavi-Naini, Wild, IEEE Transactions on Information Theory, 54(6) (2008), 2426-2436]. The key quantity of interest in this attack is the maximum probability of a successful attack. We represent this quantity as the value function of an optimal control problem and derive the dynamic programming equation that this function satisfies. The same paper cited above proves that randomized queries in such an attack have the same probability of success as that of a deterministic attack. We rederive this fact using our control representation.**

***Index Terms*—Authentication system, query model, optimal control.**

I. Introduction

SUPPOSE that there are two parties called sender and receiver. The sender is to use an authentication algorithm to authenticate itself to the receiver. The authentication system consists of the set of keys K, the set of source states S (the actual text to be transmitted), the set of messages M, the authentication function $\text{Auth} : K \times S \to M$ and the verification function $\text{Ver} : K \times M \to \{0, 1\}$. The assumptions on these are as follows:

1) $\text{Ver}(e, \text{Auth}(e, s)) = 1$ for all $(e, s) \in K \times S$,
2) $\text{Ver}(e, m) = 1$ if and only if there is a source $s \in K$ such that $m = \text{Auth}(e, s)$,
3) $\text{Auth}(e, \cdot)$ is an injective function from S to M for all $e \in K$,
4) K, M and S are finite.

The authentication system works as follows. The sender and receiver chooses a random key E that takes values in K; only the sender and the reciever are assumed to know the key. If the sender is to transmit the source code k_0, it uses the authentication function $\text{Auth} : K \times S \to M$ to compute the authenticated message $m_0 = \text{Auth}(E, k_0)$ and sends this message to the receiver. The receiver, on the other hand, upon receiving a message $m_0' \in M$ checks whether $\text{Ver}(E, m_0')$ is equal to 1 to verify whether m_0' is a message authenticated using the key E.

Ferruh Özbudak is with the Institute of Applied Mathematics and Department of Mathematics, Middle East Technical University, 06800, Ankara, Turkey. Email:ozbudak@metu.edu.tr

Ali D. Sezer is with the Institute of Applied Mathematics and Department of Mathematics, Middle East Technical University, 06800, Ankara, Turkey. Email:devin@metu.edu.tr

Üstün Yıldırım is with the Institute of Applied Mathematics and Department of Mathematics, Middle East Technical University, 06800, Ankara, Turkey. Email:yildirim.ustun@gmail.com

Manuscript received March 1, 2012; revised April 14, 2012.

II. An N step attack using an authentication oracle

The paper [2] considers the following problem about this setup. Suppose that there is an attacker who has the capacity to have any source authenticated with key E, which is the key that has been fixed by the sender and the receiver and which is assumed to be known only by them. In [2] this capacity of the attacker is modeled using the concept of an "oracle." The attacker's having a message authenticated with the key E is referred to as "querying the authentication oracle;" we will also be using this terminology. The attack takes place as follows: the attacker chooses a source string s_1 and has it authenticated with key E; the result is the authenticated message $m_1 = \text{Auth}(s_1, E)$. Having observed m_1, the attacker chooses the source s_2 and has this authenticated and observes the response $m_2 \doteq \text{Auth}(s_2, E)$. This sequence of operations continues until the attacker has had a total of $N - 1$ sources authenticated and has observed the corresponding authenticated messages. In the N^{th} step the attacker sends a message m to the sender that has to be different from m_1, m_2,..., m_{N-1}. The goal of the attacker is to choose $(s_1, s_2, ..., s_{N-1}, m)$ so that the probability of $\text{Ver}(E, m) = 1$ is greatest.

A. Deterministic Queries

The sequence of source messages s_1, s_2,... s_{N-1} that the attacker gets authenticated are called "queries." Let us first consider the case when the attacker chooses s_i deterministically as a function of his first $i - 1$ queries and their results. Under this assumption, the only randomness in the problem arises from the randomness of the key E. Therefore, the sample space is merely $\Omega \doteq K$ itself; because K is finite one can use the power set $\mathscr{F} \doteq 2^K$ as the σ algebra and we will do so. P is a probability distribution on K, it is the distribution of the random key E. P is the sole probability measure in this formulation.

First define an expanded control problem with a general initial point. To motivate the definition we will describe a generalized attack associated with the expanded control problem. In the generalized attack, *before the attack begins* the attacker is assumed to have a collection $X_0 \in (S \times M)^l$ of source and authenticated message pairs. The attacker then queries the autentication oracle taking into account the results X_0 he has before the attack began. The source string message pairs he has at the end of the $k - 1^{st}$ step of his attack is

$$X_k = (X_{k-1}, (s_k, \text{Auth}(s_k, E)).$$

Note that if $X_{k-1} \in (S \times M)^l$ then $X_k \in (S \times M)^{l+1}$. Define the following filtration on $(\Omega, \mathscr{F})$:

$$\mathscr{F}_i \doteq \sigma(X_i).$$

$\mathscr{F}_i$ represents the information available to the attacker at step i of the attack. The control s_i of the attacker (the source code he chooses to send to the oracle at step i of his attack) is assumed to be $\mathscr{F}_i$ measurable. This means that the attacker makes use of all of the information available to him before step i to decide his next query.

Remark 1. Note that $\mathscr{F}_i \subset \mathscr{F} = 2^K$. Therefore, it is merely a collection of subsets of K. Being a finite σ algebra, it is defined by its atoms.

For $X = ((m_1, s_1), (m_2, s_2), ..., (m_k, s_k))$ let P_X denote P conditioned on the set

$$\{e : e \in E,\ \text{Auth}(e, s_i) = m_i, i = 1, 2, ..., k\}.$$

In particular, if X is the empty sequence, $P_X = P$.

Define

$$V(X_0, N) \doteq \max_{s_1, s_2, ..., s_{N-1}, M_N} P_{X_{N-1}}(\ \text{Ver}(M_N, E) = 1), \tag{1}$$

The value of our original problem is

$$V(\emptyset, N). \tag{2}$$

Now, by definition a $\sigma(X_{k-1})$ random variable s_k can be represented as $f_k(X_k)$ where f_k is a deterministic function from $(S \times M)^{k+l-1}$ to S, where l is the dimension of X_0. Thus we can write (1) as

$$V(X_0, N) \doteq \max_{f_1, f_2, ..., f_N} P_{X_0}(\ \text{Ver}(M_N, E) = 1),$$

where $f_i : (S \times M)^{l+i-1} \to S$ for $i < N$ and $f_N : (S \times M)^{l+N-1} \to M$.

For any $X_0 \in (S \times M)^l$ and an attack strategy defined by

$$\begin{aligned} g_1 &: (S \times M)^l \to S, \\ g_2 &: (S \times M)^{l+1} \to S, \\ &\vdots \\ g_k &: (S \times M)^{l+k-1} \to S, \\ g_{k+1}&(S \times M)^{l+k} \to M \end{aligned}$$

define

$$V(X_0, k, g_1^{k+1}) = P_{X_k}(\ \text{Ver}(g_{k+1}(X_k), E) = 1).$$

This is the probability that an attack using the strategy g_1^{k+1} is succesful. Note that

$$V(X_0, N) = \max_{g_1^N} V(X_0, N, g_1^N) \tag{3}$$

In (2), condition on the outcome M_1

$$V(\emptyset, N) = \max_{f_1, f_2, f_3, ..., f_n} \mathbb{E}[P(\ \text{Ver}(M_N, E) = 1 |\ \text{Auth}(q_1, E))]$$

By [1, Exercise 1.14, page 230] the conditional probability on the right side of this display is $V((q_1,\ \text{Auth}(q_1, E)), N - 1, f_2^N)$. This is less than or equal to $V(\{(q_1,\ \text{Auth}(q_1, E))\}, N - 1)$ by (3), which gives

$$V(\emptyset, N) \le \max_{f_1} \mathbb{E}[V(\{(q_1,\ \text{Auth}(q_1, E))\}, N - 1)].$$

On the other hand, if $f_2, f_3, ..., f_n$ are set to be the optimizers in the definition of $V(\{(s_1, m_1)\}, N - 1)$ for an arbitrary pair (s_1, m_1) we get

$$V(\emptyset, N) \ge \max_{f_1} \mathbb{E}[V(\{(q_1,\ \text{Auth}(q_1, E))\}, N - 1)].$$

These yield the dynamic programming equation for the present problem:

$$V(X, N) = \max_{f_1} \mathbb{E}[V(X \cup \{(q_1,\ \text{Auth}(q_1, E))\}, N - 1)].$$

B. Random queries

In this section we show that randomizing queries does not improve the optimal probability of success. There is no harm in assuming that the members of M and S are real numbers. Let O_M and O_S be the family of probability distributions on $\mathbb{R}$ that puts all of the probability mass on M and S respectively.

We are interested in an attack that will last N steps. The first $N - 1$ steps will be random authentication queries.

We use the following sample space to model this attack:

$$\Omega = K \times [0, 1]^N$$

The K part of Ω is the set of all keys and $[0, 1]^N$ correspond to the randomness in the first $N - 1$ queries and the spoof attack. Let $U_i : \Omega \to [0, 1]$,

$$U_i(e, (x_1, x_2, x_3, ..., x_n)) = x_i,$$

be the uniformly distributed random variable used in the i^{th} query (or the spoof attack if $i = N$). Note that these numbers are iid uniform and they are completely independent of the key, the authentication scheme and everything else.

Q_1 is a variable taking values in O_S. Q_1 is a distribution and its inverse is well defined. Define $S_1 = Q_1^{-1}(U_1)$. Under P, S_1 is a random variable taking values in S and has distribution Q_1. Define

$$M_1 = \ \text{Auth}(S_1, E)$$

For $i > 1$,

$$\mathscr{F}_{i-1} = \sigma(M_1, S_1, M_2, S_2, ..., M_{i-1}, S_{i-1}),$$

Q_i is an $\mathscr{F}_{i-1}$ measurable function taking values in O_M. Define

$$S_i = Q_i^{-1}(U_i), \quad M_i = \ \text{Auth}(S_i, E). \tag{4}$$

Finally, Q_N is an $\mathscr{F}_{N-1}$ measurable random variable taking values in O_M. Define

$$M_N = O_M^{-1}(U_N).$$

Our control problem is

$$\sup_{Q_1^N} P(\ \text{Ver}(M_N, E) = 1).$$

Now write this as

$$\sup_{Q_1^N} \mathbb{E}[P(\ \text{Ver}(M_N, E) = 1 | \mathscr{F}_0)].$$

Now note that conditioned on $\mathscr{F}_0$, U_i are constants and Q_i in (4) determines S_i as a deterministic function of $(S_1, M_1, S_2, M_2, ..., S_{i-1}, M_{i-1})$. Therefore, for each Q_1^N

$$P(\ \mathrm{Ver}(M_N, E) = 1 | \mathscr{F}_0) \leq V_N$$

It follows that

$$\sup_{U_1^N} \mathbb{E}[P(\ \mathrm{Ver}(M_N, E) = 1 | \mathscr{F}_0)] \leq V_N.$$

The reverse inequality is trivial because every deterministic control is also a random control.

ACKNOWLEDGMENT

Ferruh Özbudak and Ali Devin Sezer were partially supported by TUBITAK under the Grant No. TBAG-109T672.

REFERENCES

[1] Richard Durrett, *Probability: theory and examples*, second ed., Duxbury Press, Belmont, CA, 1996.
[2] R. Safavi-Naini and P.R. Wild, *Information theoretic bounds on authentication systems in query model*, Information Theory, IEEE Transactions on **54** (2008), no. 6, 2426–2436.